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 (OAIC)

Prepared by

Assoc. Prof. Normann Witzleb and Prof. Moira Paterson

Faculty of Law, Monash University

Jordan Wilson-Otto, Gabby Tolkin-Rosen and Melanie Marks

elevenM Consulting

18 December 2020

Table of Contents

Recalling that the right to privacy is important for the exercise of freedom of expression, including the right to seek, receive and impart information, and contributes to the development of an individual's ability to participate in political, economic, social and cultural life and that digital technology has a considerable impact on the enjoyment of these rights'[1]

Executive Summary

The context for our report

Respect for privacy – or for one's private life – is a human right. Therefore, it is enjoyed by everyone regardless of age, ability or status. The international instruments which protect the right to privacy do not distinguish between adults, children or other groups as rights holders.[2] Yet, there is increasing international recognition that the privacy of vulnerable people, including children, is particularly at risk.

The Australian Competition and Consumer Commission's (ACCC) report on the Digital Platforms Inquiry acknowledged that 'extensive amount of data collected by digital platforms', combined with modern profiling techniques, may place vulnerable consumers 'at risk of being targeted with inappropriate products or scams, discriminated against, or inappropriately excluded from markets'.[3] The report also referred to the problem that '[c]ertain groups of consumers may lack the technical, critical and social skills to engage with the internet in a safe and beneficial manner'.[4] By way of example, the report specifically referred to the risks arising to children, older Australians and consumers from low socio-economic backgrounds.

When the Australian Government in 2019 announced a review the *Privacy Act 1988* ('Privacy Act'), it accepted the recommendation of the ACCC to task the Office of the Australian Information Commissioner (OAIC) with developing a binding 'online privacy code' that will apply to social media platforms and other online platforms that trade in personal information.[5] The Government stated that the privacy code will require these entities to:

- be more transparent about data sharing
- seek more specific consent from users when collecting, using and disclosing personal information
- implement mechanisms to stop using or disclosing personal information on request, and
- comply with stronger rules in relation to the above matters for children and vulnerable groups.

---

[1] UN General Assembly (2014), *Right to privacy in the digital age*, A/RES/71/199.
[2] Universal Declaration of Human Rights, Art 12; International Covenant on Civil and Political Rights, Art 17.
[3] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Final Report (December 2018), p 447 ('ACCC DPI Final Report').
[4] Ibid, 448.
[5] Australian Government, Attorney-General and Minister for Communications and Arts, 'Tougher penalties to keep Australians safe online', Joint Media Release (24 March 2019) <https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019>.

If enacted, this code will protect the personal information of all Australians, but it will also contain specific requirements to protect children and vulnerable people. The dual aim of the code should consist of protecting individuals from the risks and potential harms to their privacy, while facilitating access and participation in the full range of benefits of the online world.

At present, the Privacy Act neither contains any specific protections for children or other vulnerable groups nor any general requirement for fair dealing with personal information. Broadly speaking, it instead imposes limitations on data collection and processing based on notice, consent and consistency of purpose. In general terms, the Australian Privacy Principles (APPs) in the Privacy Act permit the collection and processing of personal information, including the personal information of children and other vulnerable persons, provided there is transparency by way of compliance with reasonable steps for notification of specified matters and the existence of an accessible privacy policy and a sufficient legal basis for the data collection and processing. Insofar as use and disclosure are concerned, the legal justification generally requires either consistency with the purpose of collection or consent. Consent is relevant primarily where the information qualifies as 'sensitive information', although it implicitly underlies the requirement that data must generally be collected directly from an individual. The APPs are premised on the assumption that individuals are able to provide informed consent and that the notification requirements are adequate to inform consent. These provisions therefore provide a logical starting point for addressing the protection of children and other vulnerable individuals.

The online privacy code will not replace the relevant provisions of the Privacy Act but will operate in addition to the requirements of the Privacy Act. Under the existing code-making framework in the Privacy Act, the purpose of a code is to set out how one or more of the APPs are to be applied, and how APP entities that are bound by the code should conduct their data processing. Codes are generally intended to be more concrete, and no less prescriptive, than the principles-based requirements contained in the APPs. It is envisaged that the same principles would also apply to the online privacy code, once the OAIC is provided with relevant code making power.

A limitation of a code that would give operational effect to the APPs is that it could not provide any regulation is inconsistent with the Privacy Act or the APPs. However, reliance on notice and consent has proven to be increasingly problematic for numerous reasons, in particular in the online environment. These reasons include that most privacy notices are long and difficult to understand, and that consumers are routinely asked to provide consent to a range of broadly defined purposes and often feel disempowered to withhold consent for data practices that they do not agree with. It follows therefore that further measures going beyond the current Privacy Act may be required to protect consumers and to ensure fairness in the processing of their personal information.

In recognition of this, the government's proposed privacy reforms include both the introduction of a privacy code for digital platforms, as recommended in the ACCC's Digital Platforms report, and broader reforms to the Privacy Act itself, as heralded in the recent Issues Paper[6] published by the Attorney-General's Department. We note that the latter

[6] Australian Government, Attorney-General's Department, *Privacy Act Review*, Issues Paper, Canberra (October 2020) ('Issues Paper').

includes specific mention of the notification and consent issues relating to children and other vulnerable persons. It also raises the possibility of other reforms relevant to these groups including additional controls over collection, use and disclosure and the introduction of right to require the erasure of information.

This report considers the factors that may create, influence, and mitigate vulnerability of children and other vulnerable groups in the online setting, and considers the risks for privacy arising from these vulnerabilities. In line with the brief, the report looks at children and other vulnerable groups separately, but we note that many considerations apply to both cohorts alike. The report considers international developments in the protection of privacy of children and vulnerable groups, as well as emerging examples of best practice in providing notice and consent. This discussion is intended to support the development of the online privacy code for digital platforms in Australia and inform the broader review of the Privacy Act.

The report primarily makes recommendations for specific requirements for the handling of personal information of children and other vulnerable groups that should be contained in a privacy code for social media platforms and other online platforms that trade in personal information. However, where reforms should go beyond the current Privacy Act or would apply better economy-wide, we will also make recommendations that would require changes to the Privacy Act itself.

Children's online privacy

(i) Privacy risks and harms arising for children online

Part 1 of this Report considers the privacy risks and harms that may arise when children's personal information is collected, used and disclosed online. It identifies the multiplicity of factors that make children vulnerable online from a privacy perspective and outlines the different types of privacy risks and harms they face in the online context. It also highlights the limited scope of existing restrictions or other measures currently adopted by digital platforms and other organisations to address these issues. This analysis suggests that there is clear case for reform to strengthen online privacy protections, while acknowledging that privacy is not the only right that is relevant in relation to online environments and that children also possess important participative rights.

Key findings:

- ***The factors that make children vulnerable online from a privacy perspective***

  Children are vulnerable online due to limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making. This vulnerability is particularly relevant in the privacy context due to the key role of notice and consent as a basis for current privacy protection. Children's ability to make rational decisions, like that of adults, is further affected by cognitive biases.

- ***The privacy risks and harms faced by children online***

  Despite the many benefits of children engaging in online activities, there are also a range of risks. The risks and harms that children face online arise primarily from the

monetisation of their personal information, from the social impacts of sharing personal information on their reputation and life opportunities, and from e-safety risks.

Loss of informational privacy can cause children dignitary and autonomy harms that include potential reduction in their capacity to freely develop their identity and to maintain anonymity. Apart from these intrinsic privacy harms, there is also the potential for consequential harms arising from increased exposure to online marketing and e-safety risks.

Some of these risks can lead to harm with immediate effects, whereas others may cause harm at an unspecified future time.

- ***Measures used by digital platforms or other organisations that operate online to mitigate risks/harms relating to the collection, use and disclosure of a child's personal information***

  All social media platforms evaluated (ie Facebook, Instagram, YouTube, Snapchat, Twitter, Apple and Google) have content moderations controls that specifically address risks to children, although these are not cohesive and are individual to the platform.

  All social media platforms and big tech companies evaluated have advertising controls for minors, although these are not cohesive and are individual to the platform or company.

  The majority of social media platforms evaluated (Facebook, Instagram, YouTube, Snapchat and Twitter) do not provide parental controls, however, several of them do offer a child-specific platform.

  Google and Apple have a range of parental controls.

(ii) Additional protections or requirements to address the children's online privacy risks and harms

Part 2 of the Report then explores what additional protections and requirements could be put in place to mitigate the risks and potential harms faced by children online. To inform the debate, this part also considers how international jurisdictions and data protection authorities have addressed privacy risks and harms faced by children online. As indicated above, our recommendations fall into two groups – some measures should be included in the proposed privacy code for digital platforms and additional reforms are worthy of consideration in the context of current review of the Privacy Act.

Key findings:

- ***Children's privacy protection in international jurisdictions***

  There is an international trend towards implementing additional privacy protections for children. The US (California in particular), and the EU are the most advanced in drafting and implementing these protections.

  In the US, the *Children's Online Privacy Protection Act 1998* imposes requirements to provide notice to parents of children under the age of 13, and to obtain verifiable parental consent, before personal information from these children can be collected, used or disclosed. These measures are now supplemented in California by the Consumer

Privacy Act, which also contains special protections for children. The General Data Protection Regulation (GDPR) in the EU has built on, and expanded, these protections, including by imposing stricter requirements on the use of children's personal data for the purposes of marketing or profiling, and by creating a right to erasure. On the basis of the GDPR, the UK Information Commissioner's Office has developed a path-breaking 'Age Appropriate Design Code' that is centred on the principle that the best interests of the child should be the primary consideration when designing and developing apps, games, connected toys/devices and websites that are likely to be accessed by children.

While the Californian Consumer Privacy Act, the GDPR and the UK 'Age Appropriate Design Code' currently provide some of the most substantial and forward-thinking protections, children are also given enhanced protections in the data privacy laws of Canada, China, India and South Korea.

- ***Obtaining meaningful consent from children***

  Children's ability to make informed choices is developing throughout the teenage years. It is important to adopt an approach that protects children's privacy rights against undue interference, yet also respects their increasing ability to make their own privacy choices.

  Despite a growing body of empirical evidence into the capacities of children and adolescents to make their own privacy decision, there is no consensus as to the most appropriate age of consent. Approaches in overseas jurisdictions are not evidence-based, and range from 13 to 18 years of age.

  Future Australian regulation should therefore aim to stipulate an age limit at which it would be safe to assume that a child of ordinary capacities and development will have capacity to make its own privacy decisions. Until further stakeholder engagement on this question is undertaken, this Report favours maintaining and codifying the current Australian threshold of 15 years of age.

- ***Obtaining parental consent***

  Using parental consent to enable children to access the online environment raises the same problems as the consent model more generally. Due to the complexities of the data environment, people are often not able to understand the conditions they are agreeing to, and this same problem applies equally to parents providing consent on behalf of their children.

- ***Transparency, notifications and privacy policies***

  Privacy transparency for children should aim for more than mere disclosure of material facts. It should aim to educate, empower and enable privacy self-management, accounting for a child's developing needs and capabilities.

  Children are not equipped to bear responsibility for reading and understanding disclosures (however simply drafted), nor is it reasonable to expect them to have the cognitive ability and background knowledge to understand how a disclosed act or practice is likely to impact them.

  The onus should be on platforms to help children to understand and contextualise privacy disclosures by:

- using the most effective tools and strategies for clear communication
- taking into account children's specific needs, vulnerabilities and contexts, and
- adopting design practices for privacy disclosures that involve children and ensure their effectiveness.

(iii) Our Recommendations for children's online privacy protection

In light of our findings, we make the following recommendation for additional children's online privacy protections.

Recommendations 1-8 can be incorporated into a privacy code consistently with the existing structure of the Privacy Act, as additional requirements linked to APPs 3, 6, 7 and 8. The others may require the inclusion in the Privacy Act of amendments specific to platforms and online web services to provide anchorage for them.

In the case of recommendations 2, 4, 14 and 16 we also recommend that they are worthy of consideration in the context of the current review of the Privacy Act for application on an economy-wide basis.

The age of digital consent

Recommendation 1

Subject to the results of further consultation with stakeholders, the existing standard under the Privacy Act and OAIC guidance should be maintained. That would apply:

- a cut-off age of 15 for a rebuttable presumption with respect to capacity, and
- the ordinary standard for the quality of consent, which requires that the individual must have capacity, and that consent must be informed, voluntary, current and specific.

Validity of consent

Recommendation 2

The Code should further clarify that consent is considered 'only valid if it is reasonable to expect that individuals to whom an organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.'

This is also recommended as an economy-wide measure.

Age assurance

Recommendation 3

The Code should require that digital platforms take a risk-based approach to age assurance; for example, by requiring reasonable steps proportionate to the nature and risks of the processing activities.

Strengthened notification requirements

Recommendation 4

The Code should adopt the ACCC recommendation 16(b) for strengthened notification requirements. This would include an expansion of the APP 5 matters to include clear statements of how the organisation will use and disclose the consumer's personal information. We also support the ACCC recommendation for further work to be done on standardised language, templates, icons or other tools for privacy transparency.

The adoption of ACCC recommendation 16(b) is also recommended as an economy-wide measure.

Recommendation 5

The Code should further expand the APP 5 matters to include how users can report concerns, exercise their rights, or use any other privacy self-management tools available to them (such as how to use account privacy settings or turn off profiling, targeted advertising or location tracking).

Recommendation 6

The Code should strengthen APP 5 by requiring digital platforms to take reasonable steps to ensure that their users are aware of APP 5 matters, in addition to providing notice per ACCC recommendation 16(b).

Recommendation 7

The Code should require organisations to collect evidence of the extent to which users engage with privacy notifications and use privacy features, and to be able to demonstrate the reasonableness of steps taken.

Recommendation 8

Guidance should make clear that certain steps are presumed to be reasonable with respect to ensuring awareness of the APP 5 matters, including:

- considering and designing for the needs, capabilities and behaviours of various user groups (such as children and other vulnerable groups);
- offering versions of notices appropriate for different groups, and
- embedding information and indicators within a service.

Fair, lawful and reasonable information handling

Recommendation 9

The Code should establish an overriding obligation to handle personal information in a manner that is lawful, fair and reasonable.

This obligation could be enacted in the Code as an additional requirement linked to APPs 3, 4, 6 and 7.

We recommend this also as an economy-wide measure.

Recommendation 10

The Code should set out a non-exhaustive list of factors to be considered in determining whether a collection, use or disclosure is fair and reasonable in the circumstances, including:

- where the personal information of a child is being processed, whether the processing is in the best interests of that child, and
- any foreseeable privacy harms that could result from processing and any measures that could be taken to prevent them.

Privacy Impact Assessments

Recommendation 11

The Code should require digital platforms to conduct a Privacy Impact Assessment (PIA) for all online products and services, and for all new products and services prior to launch.

High-privacy default settings

Recommendation 12

The Code should require that platforms and services are set to the highest privacy settings by default. High-privacy default settings should cover both user-to-user privacy settings (such as who can see activity or posts) and user-to-platform privacy settings (such as profiling, location tracking, or targeted advertising).

Nudging

Recommendation 13

The Code should prohibit the use of 'nudge' techniques which lead or encourage children to provide unnecessary personal data or turn off privacy protections.

Profiling

Recommendation 14

The Code should require that whenever a person is profiled, they must be provided with age appropriate information explaining the process and its implications for them and be able to express their point of view about their profile.

We recommend this also as an economy-wide measure.

Recommendation 15

The Code should establish a presumption that profiling of children for advertising or other commercial purposes is not fair or reasonable.

The right to erasure

Recommendation 16

The Code should provide for a right to withdraw consent for processing and set specific requirements for digital platforms to action such requests. For example, to cease any processing and to delete any information collected or retained on the basis of consent or reasonable expectation of the individual, unless another permissible purpose applies.

We recommend this or a full right to erasure also as an economy-wide measure.

Collection

Recommendation 17

The Code should prohibit collection of personal information about children beyond the minimum amount of personal data necessary to provide the elements of a service in which a child is actively and knowingly engaged, or as required by law or for a defined public interest. For younger children, consent should not be available as a basis for collection of personal information beyond the minimum necessary to provide the service. Collection of personal information for profiling and targeted advertising should be presumed to be unnecessary.

Geo-location data

Recommendation 18

The Code should require that location data is subject to additional protection. Unless necessary to provide elements of a service in which a child is actively and knowingly engaged and except as required by law or for a defined public interest:

- location tracking must be off by default, and
- options which make a child's location visible to others should default back to 'off' at the end of each session.

Recommendation 19

Services should also be required to provide an obvious indication when location tracking is active and every time the child's location is used or disclosed to others.

Recommendation 20

Consideration should be given to additional safeguards for services that allow for persistent monitoring of or access to a child's location, such as requiring that:

- younger children are only tracked with parental consent, and older children only with their own consent;
- children are aware and regularly reminded that they are being tracked; and
- a list of all persons authorised to monitor the child's location is readily available to both parent and child.

Data sharing

Recommendation 21

The Code should require that children's data must not be disclosed except as necessary to provide the elements of a service in which a child is actively and knowingly engaged, or as required by law or for a defined public interest. This restriction should apply the same standard to restrict information collection directly by third parties via cookies or other tracking technologies.

(iv) The protection of the online privacy of other vulnerable people

There are no groups of people other than children that are considered incapable of making decisions about privacy — vulnerability is not a fixed trait that can be associated with a specific group or an identifiable threshold. However, there are specific 'vulnerability factors' that can be used to identify people who are at higher risk of harm. It is important that these factors are used to define vulnerability as a state rather than a status, otherwise there is a high risk of marginalising individuals, or negatively impacting their autonomy. The ability to make decisions about privacy needs to be determined on an individual basis, and in light of the decision in question.

Digital platforms can pose a range of risks for people who may be vulnerable and their use can compound the risks these individuals are already experiencing.

All digital platforms have a range of policies and controls in place to help protect vulnerable people, and to facilitate independent access to products and services. These can help prevent discrimination, targeting and other potential harms, but only to a limited degree. The various digital platforms differ in their approaches towards these controls. There are also a broad range of regulatory protections for vulnerable people, including controls around consent and data handling, and requirements for accessibility.

One of the limitations for these controls (and one of the primary barriers to improving protections for vulnerable people) is that, unlike age, vulnerability cannot be easily identified and may vary over time and situation. Controls that restrict positive or negative targeting based on vulnerability factors do provide some protections. However, unless a person self-identifies as vulnerable, there are many situations where it is difficult to provide additional protections.

As with children's privacy, consent is one of the key issues for the balance between protection and facilitation. Decision-making capacity for privacy issues is often situation-specific and may depend on the complexity of the decision. It may also vary from time to time, depending on what causes the vulnerability and how it affects the individual in question (for example, someone with severe mental illness may have fluctuating capacity). Ultimately, it is essential to ensure that individuals are supported to make decisions and provide consent, as much as possible. Undue reliance on the guardian-consent model runs the risk of infringing on people's autonomy and right to make decisions that affect their lives.

Again, as with children, one of the best ways to improve consent process for people who have limited or varying capacity is to improve the transparency, complexity and accessibility of all privacy notices/policies. Some of the styles of communication that suit very young children may not be appropriate for adults, however, simplification and providing different levels of complexity based on reading age/decision-making age can also be applied in this context.

Key findings:

- ***Existence of other groups who are physically or legally incapable of making their own privacy decisions***

  There are no groups of people other than children that are considered physically or legally incapable of making decisions about privacy. The ability to make decisions about

privacy needs to be assessed on an individual basis. It is decision-specific and may fluctuate depending on the individual's circumstances.

While some state legislation expressly sets out when a person is considered incapacitated and how incapacity to make privacy decisions should be dealt with, the Privacy Act does not contain equivalent provisions. There is a case for giving the OAIC guidance on these matters statutory effect or otherwise to reform the law to ensure its conformity with the National Decision-Making Principles recommended by the Australian Law Reform Commission.

- ***Vulnerability is a state rather than a status***

  Vulnerability can be defined as heightened susceptibility to harm. It is preferable that any definition of 'vulnerable groups' engages with vulnerability as a state rather than a status.

  Vulnerability is dynamic and relative, rather than a fixed trait that is associated with belonging to a specific group. The causes of vulnerability are complex and can intersect with one another. Both individual characteristics and situational factors shape our susceptibility to harm.

  The preferred approach in other areas of consumer protection is to consider 'vulnerability factors' that put people at higher risk of suffering harm or detriment.

- ***The factors that make individuals vulnerable***

  Vulnerability in an online context can arise where an individual faces greater difficulty than others in protecting themselves from harm. This can be the technical or cognitive skills and experience to use digital platforms and other applications safely.

  Individuals can also be vulnerable because they have particular characteristics that expose them to greater or different harm than other people. Such harm can arise from being exposed to or targeted with inappropriate products or services, from unlawful discrimination, or inappropriate exclusion from a market.

  Digital platforms can exacerbate the risks for people with a range of 'vulnerability factors', and can compound the risks that are experienced by these individuals.

  The approaches of other agencies and organisations suggest that is advisable to engage in detailed qualitative and quantitative research into the vulnerability experience of specific customer groups and to adopt a multi-stage approach to identifying and addressing vulnerability.

- ***Existing restrictions or other measures designed to mitigate risks/harms relating to the collection, use and disclosure of the personal information of individuals physically or legally incapable of providing consent or other vulnerable groups/individuals***

  All the digital platforms reviewed have a range of policies and controls in place to help protect vulnerable people, and to facilitate independent access to products and services.

  The major platforms have detailed advertising policies that are intended to protect users from harm by imposing restrictions and prohibitions on advertising various types of potentially harmful products or services, and on certain advertising content.

In addition to restricting advertising content that may be potentially harmful to users, the major platforms further protect vulnerable users by imposing restrictions in relation to their personalisation and targeting tools.

Some platforms also impose restrictions on the collection of data relating to vulnerable groups through their advertising products.

Community guidelines and accessibility aids also operate to enhance the participation of vulnerable groups.

These policies can improve the experience and protection from discrimination and targeting. But they currently only operate on a voluntary basis through the platforms' terms and conditions of use.

- ***Privacy protection of vulnerable individuals in international jurisdictions***

  Overseas jurisdictions have adopted a broad range of regulatory measures that directly or indirectly protect vulnerable individuals.

  These include requirements for accessibility to respond to vulnerabilities that affect individuals' ability to access and interact with content.

  The consent requirements are modified where a data subject lacks capacity to provide consent.

  In the EU, the requirement for free consent operates to protect individuals whose vulnerabilities put them at risk of coercion, such as where there is an imbalance of power.

  Many jurisdictions, including Canada, the EU, Brazil and South Korea, adopt special restrictions on data handling where individuals are particularly exposed to harmful effects. These restrictions, which include fairness and non-discrimination requirements, purpose limitations and restrictions on the use of sensitive data, have special relevance for people in vulnerable positions.

- ***Obtaining meaningful consent on behalf of individuals who are physically or legally incapable of making their own privacy decisions***

  The capacity to provide consent needs to be assessed issue-by-issue. Capacity to make one's own privacy decisions may depend on the complexity of the practice in question and the risk involved in the data collection, use and disclosure.

  It is essential to ensure that individuals who have difficulty making their own privacy decisions are supported as much as possible.

  Overreliance on guardian-consent models runs the risk of infringing on vulnerable persons' autonomy and their right to make decisions that affect their lives.

  Before changes to the current requirements are proposed, there should be further consultation with stakeholders and further research to ascertain the extent to which inability to provide meaningful consent presents issues for data processing by platforms and commercial websites.

- ***Whether particular measures or requirements should apply to privacy policies and notification practices in relation to individuals physically or legally incapable of providing consent***

  The best way to improve consent process for individuals who have limited capacity to provide consent is to improve the transparency and accessibility of privacy notices/policies and to reduce their complexity.

  Where an individual is supported or represented in their decision-making, it should be a requirement that notice is also to be provided to the supporter or decision make.

- ***Additional protections that could be imposed to mitigate the privacy risks and harms faced by individuals physically or legally incapable of providing consent in the online environment***

  Individuals who lack capacity or require support in their privacy decision-making would benefit from any protections introduced to protect vulnerable individuals more broadly.

- ***Additional requirements or protections necessary to ensure the privacy of vulnerable groups is protected online***

  Implementing requirements that protect people's privacy generally will help protect vulnerable people. There is also a close relationship between the particular measures for children and measures for other vulnerable individuals.

  There would be significant benefits in introducing a 'fair, lawful and reasonable information handling' requirement, requiring mandatory PIAs, privacy-default settings, and transparency about profiling, banning nudge techniques, and introducing the right to erasure.

  There would also be benefits in mandating complete or partial compliance with accepted standards for accessibility, such as currently the Web Content Accessibility Guidelines 2.0 (WCAG).

(v) Our Recommendations for the online privacy protection of other vulnerable people

In light of our findings, we make the following recommendation for additional online privacy protections for vulnerable people.

Recommendations 24, 25 and 27 can be incorporated into a privacy code consistent with the existing structure of the Privacy Act. Recommendation 26 may require the inclusion in the Privacy Act of an amendment specific to platforms and online web services to provide anchorage for it.

In the case of recommendations 22 and 25 we recommend that it is worthy of consideration in the context of the current review of the Privacy Act for application on an economy-wide basis.

Factor-based definition of vulnerability

Recommendation 22

The Code should adopt a factor-based definition of vulnerability that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020.

We support this also as an economy-wide measure.

Further engagement and analysis

Recommendation 23

We recommend that the OAIC engage in further engagement and analysis to ensure that its protective measures are appropriately targeted, have the buy-in and support of affected groups and are tested for effectiveness.

Consent

Recommendation 24

Before any specific measures are considered for decision-making arrangements for individuals lacking capacity to give meaningful consent, there should be:

- consultation with both disability support groups and industry representatives, and
- further research to ascertain the extent to which inability to provide meaningful consent presents issues in the context of processing by platforms and commercial websites.

Notice

Recommendation 25

The Code should extend APP 5 to require that any privacy notices required to be provided to an individual also be provided to a nominated supporter or decision maker, where one exists.

We recommend this also as an economy-wide measure.

Processing restrictions

Recommendation 26

In addition to the matters listed under Recommendation 10, the Code should include the following factors to be considered in determining whether a collection, use or disclosure is fair and reasonable in the circumstances:

- Any information the APP entity has, or ought to have, about the likely vulnerabilities of their users.
- The appropriateness in the circumstances of enquiring about or verifying whether a user is vulnerable in a particular way before processing their information.
- Any privacy harms that could result from processing and any measures that could be taken to prevent them.

Accessibility of privacy policies and controls

Recommendation 27

The Code should require that privacy policies and privacy controls be provided in formats that are accessible, according to current, generally accepted accessibility standards or guidelines.

The scope and context of this report

The Office of the Australian Information Commissioner (OAIC) has commissioned this research paper about the privacy risks and harms that may arise for children and other vulnerable groups in relation to the handling of their personal information in the online environment.

In accordance with the OAIC's consultant brief, the research paper considers the following issues:

1. What privacy risks and harms may arise when children's personal information is collected, used and disclosed online?
2. What additional privacy protections or requirements could be put in place to address the privacy risks and harms faced by children online?
3. What other groups are vulnerable in relation to the collection, use and disclosure of their personal information online?
4. What additional protections or requirements could be put in place to address the privacy risks and harms faced by vulnerable groups online?

This research is intended to assist the OAIC undertake its guidance and advice functions. In particular, it is anticipated that the OAIC may draw on this research to provide input into the Government's recently announced reforms to the Privacy Act. These reforms have been announced to include the development of a binding online privacy code that will require, amongst other things, specific safeguards for children and other vulnerable groups in the online environment.

We note that the recent issues paper published by the Attorney-General's Department includes specific mention of the possibility notification and consent issues relating to children and other vulnerable persons. It also raises the possibility of other reforms relevant to these groups including additional controls over collection, use and disclosure and the introduction of right to require the erasure of information.

Question 1 — What privacy risks and harms may arise when children's personal information is collected, used and disclosed online?

Question 1a — What are the factors that make children vulnerable online from a privacy perspective?

Key findings:

Children are vulnerable online due to limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making. This vulnerability is particularly relevant in the privacy context due to the key role of notice and consent as a basis for current privacy protection. Children's ability to make rational decisions, like that of adults, is further affected by cognitive biases.

Children's privacy vulnerability online needs to be considered having regard to the existing context for privacy protection, which depends significantly on notice and consent. The factors relevant to children that increase their vulnerability in this context relate to deficits in literacy, including digital literacy, cognitive capacity and maturity of judgement. These vulnerabilities are enhanced by cognitive biases.

(i) Basic and digital literacy

Basic literacy involves the ability to read and presents issues for younger children to the extent that any information provided to them (for example, via privacy notices) involves vocabulary and sentence structures that make it difficult for them to read and understand the language used.

While simple and clearly comprehensible language is important, especially for younger children, the nature and extent of the background knowledge necessary to understand online dealings with personal information requires greater comprehension than simply the ability to read. As stated by a team of researchers in the context of advergames,[7] 'to a large extent the online world is not designed to be understood by children'.[8] This makes it important also to consider 'digital literacy', which is concerned with the knowledge and skills required to

[7] The expression 'advergames' refers to online video games that contain some form of advertising.
[8] Valerie Verdoodt, Damian Clifford and Eva Lievens, 'Toying with children's emotions, the new game in town? The legality of advergames in the EU' (2016) 32 *Computer Law & Security Review* 599, 609.

'[enable] youth to participate in digital media in wise, safe and ethical ways'[9] and therefore 'encompasses issues of privacy, safety and ethical use of technology'.[10]

The ability to make informed decisions in an online context requires awareness of a range of background matters including:

- that filling out an online registration form or other forms of participation in online activities involves the provision of personal information to the site owner and that such information is usually collected to further the site owner's commercial interests; and
- that the provision of personal information to a website may have both immediate consequences and also more distant consequences for them in their future lives.

There is evidence that children's lack of awareness of the commercial practices leaves them ignorant of the fact that providing their personal information, or participating in contexts where it can be gathered, raises potential privacy risks. For example, it may not necessarily be apparent to a younger child that completing an online form amounts to providing personal information for use by the site (as opposed being collected simply for the purposes of registration).

Because minors do not understand the business model of many internet services, such as social network sites and online communities, they tend to 'regard safeguarding personal information as a safety, rather than commercial, consideration'.[11] Young users are often not aware of the commercial value of their personal data and the fact that internet services do business on the basis of users' personal information.[12]

This lack of awareness means that children tend to understand privacy in the online context mainly in interpersonal terms. They appreciate that sharing sensitive personal data with others can have consequences for their personal relationships (e.g. increases trust, causes embarrassment or can lead to bullying) or that unauthorised access of personal data by, or disclosure to, a stranger can create safety risks. However, the intricacies and impact of data processing practices tend to be beyond their comprehension. This is not only because these data uses are technologically, economically, and socially complex, but also because industry often has little interest in creating greater transparency and making their consequences

---

[9] Media Smarts, 'The Intersection of Digital and Media Literacy', Web Page <https://mediasmarts.ca/digital-media-literacy/general-information/digital-media-literacy-fundamentals/intersection-digital-media-literacy>.

[10] Luci Pangrazio, Anna-Lena Godhe and Alejo González Lopez Ledesma, 'What is digital literacy? A comparative review of publications across three language contexts' (2020) 17(6) *E-Learning and Digital Media* 442, 444.

[11] Anna Fielder et al, *Fair game? Assessing commercial activity on children's favourite Web sites and online environments*, Report (National Consumer Council UK and Childnet International, December 2007) <http://www.agnesnairn.co.uk/policy_reports/fair_game_final.pdf> 2.

[12] Youth Protection Roundtable, Youth Protection Toolkit (2009), Stiftung Digitale Chancen, <www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf>.

more apparent.[13] In consequence, children rarely consider the commercial or institutional use of their data.[14]

As a result, the vulnerability that arises from this lack of awareness is also associated with relative naivety about the risks involved. Research suggests that 'children can be quite trusting of online platforms, choosing to accept the default privacy settings based on the belief that the site designers and developers have already considered privacy issues, and built adequate privacy protections into the site's architecture'.[15]

An evidence review conducted in the United Kingdom (UK) as part of a broader project exploring children's privacy in the online environment noted evidence that:

> commercial privacy is related to different behaviours than interpersonal privacy resulting from the different type of follow-up engagement: while individuals examine the reaction of friends towards their posts on social media, they do not often deliberately communicate with commercial entities, so the consequences of their data being used may remain unknown to them, making them less concerned about commercial than interpersonal privacy...[16]

The barriers to children's understanding of commercial privacy risks result from the fact that it is extremely difficult for them to understand concepts such as:

- how their online data is being collected and used;[17]
- how it flows and transforms – being stored, shared and profiled;[18] and
- to what effect and future consequence.[19]

---

[13] Simone Van der Hof, 'I Agree …. Or Do I? — A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) *Wisconsin International Law Journal* 409, 436.
[14] Sonia Livingstone, Maria Stoilova and Rishita Nandagiri, *Children's data and privacy online: Growing up in a digital age – An evidence review* (London School of Economics and Political Science, January 2019) 20 ('An Evidence Review'), citing Katie Davis and Carrie James, 'Tweens' conceptions of privacy online: Implications for educators' (2013) 38(1) *Learning, Media and Technology* 4-25; Wouter MP Steijn and Anton Vedder, 'Privacy under construction: a developmental perspective on privacy perception' (2015) 40(4) *Science Technology & Human Values* 615-37; Maria Stoilova, Rishita Nandagiri and Sonia Livingstone, 'Children's data and privacy online: a systematic evidence mapping (2019) *Information, Communication & Society*, DOI: 10.1080/1369118X.2019.1657164 ('Systematic Evidence Mapping').
[15] Livingstone et al, Evidence Review (ibid), citing Davis and James (ibid).
[16] Ibid, citing Gry Hasselbalch Lapenta and Rikke Frank Jørgensen, 'Youth, privacy and online media: Framing the right to privacy in public policy-making' (2015) *First Monday* 20(3) <https://doi.org/10.5210/fm.v20i3.5568>.
[17] Ibid, citing Lia Emanuel and Danaë Stanton Fraser, 'Exploring physical and digital identity with a teenage cohort' *IDC (*2014) *Proceedings of the 2014 Conference on Interaction Design and Children.* New York: Association for Computing Machinery, 67–76; Amelia Acker and Leanne Bowler, 'What is your Data Silhouette? Raising teen awareness of their data traces in social media' (2017) *Proceedings of the 8th international conference on social media and society* (Association for Computing Machinery: Toronto, Canada) 1–5.
[18] Ibid, citing Leanne Bowler et al. ''It lives all around us': Aspects of data literacy in teen's lives' *80th Annual Meeting of the Association for Information Science & Technology* (2017) Washington DC, USA, 27–35.
[19] Ibid, citing Maria Murumaa-Mengel, 'Drawing the threat: a study on perceptions of the online pervert among Estonian high school students' (2015) 23(1) *Young* 1–18; Bowler et al. (ibid); Luci Pangrazio

A research study of teenagers in the United States (US) has found that most had difficulty in connecting with data at a concrete and personal level. In particular, they were either unfamiliar with the concept of an information dossier or found it too abstract to engage with. Moreover, even to the extent that they were able to see the connection between data and 'digital traces', they seemed to imagine data as static and lacked knowledge of data flows and infrastructure.[20] These findings suggested that 'data – what it is, where it lives, who has access to it and how it might be controlled – is not yet part of the thought processes of young people'.[21] This study also found that the teenagers had spent very limited time thinking about their own digital dossiers in terms of their future lives.[22]

(ii) Cognitive capacity

As stated by the Australian Law Reform Commission, '[t]here is a general consensus in the literature on child development that the capacity of children to make voluntary and rational decisions increases with both age and the development of cognitive skills'.[23] The latter includes the capacity to think logically, understand cause and effect, and analyse the consequences of decisions.[24]

It follows that a child or young person is vulnerable if they lack the capacity to reason about risks, benefits and possible consequences of providing the information and to understand implications for them personally. This will be the case if the child's brain has not achieved a level of maturity to provide the 'processing speed, voluntary response suppression, and working memory' that are essential for cognitive control of behaviour.[25] The evidence suggests that these faculties do not mature until middle to late adolescence.[26] This makes children especially vulnerable online because of the specific tactics that are commonly used to persuade children to volunteer or make available their personal data.

A feature of the online environment which increases the vulnerability of children is that its complexity reduces their ability to objectively analyse the consequences of disclosing their personal information. This issue is exacerbated by the strategies used to influence them. As noted by Kennedy, Jones and Williams, 'a child, as an online consumer, is enveloped by specific interactive marketer-generated strategies that are only possible online' and that '[t]hese vehicles influence them in ways that exploit their vulnerable/powerless developmental status'.[27] Interactive marketing, which uses embedded and personalised advertising content,

---

and Neil Selwyn, ''It's not like it's life or death or whatever': young people's understandings of social media data' (2018) 4(3) *Social Media and Society* 41–49.

[20] Bowler et al (n 18).

[21] Ibid.

[22] Murumaa-Mengel (n 18); Bowler et al (n 18); Pangrazio and Selwyn (n 18).

[23] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report 108 (May 2008) [68.26] ('ALRC Privacy Report 108').

[24] Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview*, Discussion Paper 72, (2007), [60.27] referring to Dorothy G Singer and Tracey A Revenson, *A Piaget Primer: How A Child Thinks* (revised ed, 1996), 20–26.

[25] Beatriz Luna et al, 'Maturation of Cognitive Processes from Late Childhood to Adulthood' (2004) 75(5) *Child Development* 1357, 1368.

[26] Ibid, 1366.

[27] Ann-Marie Kennedy, Katharine Jones and Janine Williams, 'Children as Vulnerable Consumers in Online Environments' (2019) 53(4) *Journal of Consumer Affairs* 1478, 1494.

particularly exploits the difficulties of children with low levels of marketing literacy, in identifying the persuasive intent of the interactions.[28]

(iii) **Maturity of judgment**

While adolescents having a more developed ability to reason than younger children, they nonetheless remain vulnerable due to an increased propensity for risk taking. Neuroscience has established that adolescents undergo significant changes to the structure of the frontal lobe of the brain, which is responsible for functions such as organising thoughts, setting priorities, planning and making judgments, and therefore rely more heavily on parts of the brain that regulate emotion.[29] In its review of the relevant literature, the ALRC notes, in particular, research which suggests that adolescents allow their emotional responses to situations to determine their course of action and do not fully evaluate the consequences of a particular course of action before commencing it.[30] This emotive element can pose greater risks in the online environment due to the increased psychosocial factors that can come into play.

What is relevant to note in this regard is that there is a difference between possessing cognitive skills and being able to exercise them in a mature manner. The ability to control impulses and exercise good judgment, in particular in emotionally charged situations, does not fully develop until children are approaching adulthood. As identified by Caufman and Steinberg, maturity of judgment depends on three specific sets of psychosocial factors; i.e.'responsibility (autonomy, identity, and self-reliance), perspective (sense of morality and context), and temperance (regulation of emotion, avoidance of extremes, non-impulsivity)'.[31] Neurological research suggests that the behavioural immaturity of adolescents 'mirrors the anatomical immaturity of their brains'.[32]

> First, adolescents rely for certain tasks, more than adults, on the amygdala, the area of the brain associated with primitive impulses of aggression, anger, and fear. Adults, on the other hand, tend to process similar information through the frontal cortex, a cerebral area associated with impulse control and good judgment. Second, the regions of the brain associated with impulse control, risk assessment, and moral reasoning develop last, after late adolescence.[33]

---

[28] Ibid, 1488.
[29] Alexandra O Cohen and BJ Casey, 'Rewiring juvenile justice: the intersection of developmental neuroscience and legal policy' (2014) 18(2) *Trends in Cognitive Sciences* 63, 63–64.
[30] ALRC Privacy Report 108 (n 23) [68.34] referring to Adam Ortiz, *Adolescence, Brain Development and Legal Culpability* (2004) Juvenile Justice Center – American Bar Association, 2; Jeffrey Fagan, 'Adolescents, Maturity, and the Law', *The American Prospect* (14 August 2005) <https://prospect.org/special-report/adolescents-maturity-law/>. See also Grace Icenogle et al, 'Adolescents' cognitive capacity reaches adult levels prior to their psychosocial maturity: Evidence for a 'maturity gap' in a multinational, cross-sectional sample' (2019) 43(1) *Law and Human Behavior* 69 <https://doi.org/10.1037/lhb0000315>.
[31] Elizabeth Cauffman and Laurence Steinberg, 'The Cognitive and Affective Influences on Adolescent Decision-Making' (1995) 68(4) *Temple Law Review* 1763, 1774.
[32] American Medical Association and Others, *Amicus curiae brief for Roper v Simmons*, 10 <https://www.aacap.org/App_Themes/AACAP/docs/Advocacy/amicus_curiae/Roper_v_Simmons.pdf>.
[33] Ibid, 11.

Perspective is very relevant to adolescents' privacy decision-making online, especially as it relates to the ability to frame a decision within a 'bigger picture'[34]. This dimension of perspective, referred to as future time perspective, is concerned with taking into account long-term as well as short-term consequences of a decision. This longitudinal perspective is very relevant to online disclosures because the majority of potential harms are likely to occur at some future unknown time.

Temperance involves the ability to limit impulsivity and emotion in decision making and to evaluate situations thoroughly before acting. Disclosure of personal information online has inherent risks that are not all equally apparent. A tendency to risk-taking is therefore problematic, especially in relation to personal information that is likely to expose an adolescent to personalised marketing, manipulation or online profiling. Significantly, Canadian empirical research suggests that this risk-taking dimension peaks during adolescence.[35] This arises both from an increased willingness to disclose personal information and from less importance being placed on privacy-protective behaviour. Coupled with progressively greater internet use, and less parental supervision, this significantly increases the risk to personal privacy as children move through adolescence.[36]

(iv) The complication of cognitive biases

Models of consent tend to presume fully rational decision-making; they assume that decisions concerning disclosure of personal information are based on a rational weighing up of the potential benefits and risks involved. However, research in behavioural economics suggests this process is in reality affected by cognitive biases.[37] These biases arise because of the use of heuristics (mental short cuts) to assist in complex decision-making. Three specific forms of bias identified by Kokakalis that are likely to be especially relevant in an online context are the 'availability bias', 'affective bias' and 'immediate gratification bias'.

'Availability bias' refers to the tendency of people to make judgments about the likelihood of an event based on how easily examples of it come to mind. Its relevance to privacy has been explained as follows:

> Most people have not personally suffered from privacy invasions, or if they have, are unaware of that fact. Therefore, they are likely to recall only positive experiences associated with the disclosure of personal information, disassociated from negative consequences.[38]

This is likely to apply to a greater degree in the case of children, especially younger children, who are very unlikely to have been aware of any negative consequences associated with them interacting with websites.

---

[34] Cauffman and Steinberg (n 31), 1783.
[35] Valerie Steeves and Cheryl Webster, 'Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy' (2008) 28(1) *Bulletin of Science, Technology and Society* 4–19.
[36] Ibid.
[37] Spyros Kokolakis, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon' (2017) 64(1) *Computers & Security* 122.
[38] Matthias Schorer 'Regulating to Support Privacy Disclosures: The First Step Towards Avoiding an Internet of Things Dystopia' (Dissertation, Faculty of Law, University of Otago, October 2018) <https://www.otago.ac.nz/law/research/journals/otago710902.html> 29.

‘Affective bias’ refers the tendency of people to make judgements based on their emotional response when forced to decide something quickly. Its relevance in relation to privacy is that it tends to lead individuals to underestimate the risks, including the potential privacy risks, associated with things they like. This issue is of heightened importance for adolescents because of the extent to which emotions affect their decision-making.

Many applications and objects in the online environment, including objects such as smart home devices which form part of the Internet of Things (the linked network of objects embedded with sensors and other connective technologies which enable them transfer information via the internet) are ‘designed to elicit enjoyment from individuals’.[39] The risks recognised by an individual deciding whether or not to permit the collection of their personal information ‘are likely to be discounted by the haze of convenience and enjoyment these novel internet-connected devices cast’.[40]

Affective bias is significant because initial emotions generated by an individual’s overall impression of the website may have a lasting effect on later stage cognitive processing. Specifically, joy significantly enhances privacy protection belief and reduces privacy risk belief.[41] Positive affect such as enjoyment is positively related to an individual’s intention to disclose personal information.[42] Therefore ‘users tend to underestimate the risks of information disclosure when confronted with a user interface that elicits positive affect’.[43]

Finally, ‘immediate gratification bias’ arises from people’s desire to experience pleasure or fulfilment without delay. This has the consequence that they experience difficulties in assessing the trade-offs between certain, immediate gains and speculative, long-term disadvantages.[44] This form of bias is highly likely to arise online where disclosing personal information is commonly presented as something that needs to be done to access some benefit – approve the terms and conditions to begin tracking your step count and heart rate in real time – thus the benefit always appears immediate, tangible, and highly valuable. This bias is made worse by the fact that the potential risks of disclosure are largely abstract, unknown and likely to arise only at some time in the future.

---

[39] Ibid.
[40] Ibid.
[41] Han Li, Rathindra Sarathy and Heng Xu, ‘The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors’ (2011) 51(3) *Decision Support Systems* 434, 44.
[42] Kokolakis (n 37), citing Robin Wakefield, ‘The influence of user affect in online information disclosure’ (2013) 22(2) *The Journal of Strategic Information Systems* 157.
[43] Ibid, citing Flavius Kehr et al, ‘Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus’ (2015) 25(6) *Information Systems Journal Special Issue on: Privacy in a Networked World* 607.
[44] Christophe Lazar and Daniel Le Métayer, ‘Control over Personal Data: True Remedy or Fairy Tale?’ (2015) 12(1) *SCRIPT-ed*, 1, 11–12, citing Matthew Rabin and Ted O’Donoghue, ‘The economics of immediate gratification’ (2000) 13 *Journal of Behavioral Decision Making* 233–250.

Question 1b — What are the privacy risks and harms that children face online?

Key findings:

Despite the many benefits of children engaging in online activities, there are also a range of risks. The risks and harms that children face online arise primarily from the monetisation of their personal information, from the social impacts of sharing on their reputation and life opportunities, and from e-safety risks.

Loss of informational privacy can cause children dignitary and autonomy harms that include potential reduction in their capacity to freely develop their identity and to maintain anonymity. Apart from these intrinsic privacy harms, there is also the potential for consequential harms arising from increased exposure to online marketing and e-safety risks.

Some of these risks can lead to harm with immediate effects, whereas others may cause harm at an unspecified future time.

This section of the report seeks to identify the different types of harm that children face online. However, it should not be taken as suggesting that online participation is inherently negative or that it does not also result in considerable benefits for children. As noted in a recent UK study, 'excessive risk aversion based on privacy concerns can restrict children's play, development and agency, and constrains their exploration of physical, social and virtual worlds'.[45]

(i) Current and future harms

The risks and harms that children face online fall into two main groups. The first are the risks and harms that arise for them as children and possibly at their specific stage of childhood and which may be associated with their particular vulnerability at that time. The second are longer term risks that affect their future opportunities, either as they progress through childhood or when they have transitioned into adulthood.

Risks and harms from different groups

Harms for children arise from different uses of personal information by various entities and persons involved in the collection and processing of their data. These include the operators of websites which collect their information and others to whom that information is accessible or on-sold.

[45] Livingstone, Stoilova and Nandagiri, *An Evidence Review* (n 14).

A key purpose for which data is collected by websites is for monetisation via its use or on-sale for marketing. Direct marketing to children can result in a range of harms including economic and decisional harms.

A second category of users are entities which make use of the information for their decision-making purposes. These practices may be potentially harmful to the extent that they result in discrimination or reduced opportunities for the individual concerned.

Finally, there are the individuals and entities who use the internet for harmful and problematic practices that pose a range of potential hazards for children of the type commonly identified in e-safety initiatives.

Broader contexts

Potential risks and harms also need to be considered in the broader context of Big Data. Big Data is most commonly defined with reference to its key common characteristics, which are frequently described as 'volume, velocity, and variety'.[46] However, what is especially significant about the world of Big Data are the sophisticated analytical techniques to which it has given rise and their use in a myriad of decisions that impact on individuals. Big Data is also relevant insofar as it facilitates manipulation and reduces the effectiveness of processes used to de-identify personal data.

The use of personal data for both marketing and decision-making is increasingly affected by processes of automation that arise in the context of Big Data. The commercial practices that underpin websites are largely based on the monetisation of personal information and the collection and processing of information in the context, undermine personal privacy as well as raising potential risks of discrimination and manipulation, as further discussed below. Intrinsic privacy-related risks and harms.

The harms that arise from children's loss of informational privacy include the dignitary and autonomy harms that result from loss of control over one's personal information and the potential reduction in their capacity to maintain anonymity.

Developmental harms

The process of datafication,[47] and the quantified self, raise developmental risks for children because it affects important processes of identity formation that take place during childhood and adolescence.

Privacy plays a vital role in self-development and self-definition. It has long been understood as playing an important role in the creation of the self, i.e. a person who regards their existence, thoughts, body and actions as their own.[48] Informational privacy is a significant

---

[46] Doug Laney, '3D Data Management: Controlling Data Volume, Velocity, and Variety', *Gartner Blog Network* (6 February 2001) <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.
[47] Deborah Lupton and Ben Williamson, 'The datafied child: The dataveillance of children and implications for their rights' (2017) 19(5) *New Media & Society* 780-794.
[48] Jeffrey H Reiman, 'Privacy, Intimacy, and Personhood' (1976) 6(1) *Philosophy & Public Affairs* 26, 39.

ingredient in this process because it provides 'breathing room to engage in the processes of boundary management that enable and constitute self-development'.[49]

Children and adolescents are engaged in the construction of their identity while they are 'in the process of developing physically and mentally to become an adult'.[50] Privacy has been identified as having a constitutive role in the formation of identity; i.e. the person whom the child becomes.[51]

> [L]ack of control over personal information can impact upon self-esteem, something that is often considered key to the construction of identity: one of the key developmental goals of adolescence. This is because the inability to control personal information not only impacts on the way others judge a person, or use the information, but can have consequences for the way in which that person sees themselves. Making an unfavourable impression on others, or simply believing that one has done so (a so-called 'self-presentation predicament'), can impact upon a person's overall level of self-esteem.[52]

This is further reinforced in the comment by Westin that what is written about an individual becomes part of their estimate of themselves as it reflects how they are evaluated by others wiser and more powerful.[53] He notes that it takes a very strong personality, especially among children being recorded in the new information-worshipping society, to reject or fight the recorded judgment of who he or she 'is'.[54]

Reduced ability to benefit from anonymity

The Big Data environment also poses novel risks to processes of anonymisation which have previously been relied upon as a safe basis for the dissemination of aggregate information about individuals.[55] The risk of reidentification has been explained as follows:

---

[49] Julie Cohen, 'What is Privacy For?' (2013) 126 *Harvard Law Review* 1904.
[50] Hans Buitelaar, 'Child's best interest and informational self-determination: what the GDPR can learn from children's rights' (2018) 8(4) *International Data Privacy Law* 293, 298.
[51] Anna Bunn, 'Children and the "Right to be Forgotten": what the right to erasure means for European children, and why Australian children should be afforded a similar right' (2019) 170(1) *Media International Australia* 37, 41, citing Erik H Erikson, *Identity: Youth and Crisis* (London: Faber & Faber, 1968) 161; Jane Kroger, *Identity in Adolescence* (Hoboken, HJ: Taylor and Francis, 2004) 96; Jochen Peter and Patti M Valkenburg, 'Adolescent's online privacy: towards a developmental perspective' in Sabine Trepte and Leonard Reinecke (eds), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Heidelberg: Springer, 2011, 600.
[52] Bunn (ibid), citing Susan Harter and Nancy R Whitesell (2003), 'Beyond the debate: why some adolescents report stable self-worth over time and situation, whereas others report changes in self-worth' (2003) 71(6) *Journal of Personality* 1027, 1035; Mark R Leary and Robin M Kowalski, 'Impression management: a literature review and two-component model' (1990) 107(1) *Psychological Bulletin* 34; Laura Smart Richman and Mark R Leary 'Reactions to discrimination, stigmatization, ostracism, and other forms of interpersonal rejection: a multi-motive model' (2009) 166(2) *Psychological Review* 365.
[53] Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1968), 23, cited in Valerie Steeves, 'It's Not Child's Play: The Online Invasion of Children's Privacy' (2006) 3 *University of Ottawa Law & Technology Journal* 169, 187.
[54] Ibid.
[55] OVIC, *Protecting unit-record level personal information: The limitations of de-identification and the implications for the Privacy and Data Protection Act 2014*, Report (2018) <https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf>.

> Re-identification works by identifying a 'digital fingerprint' in the data, meaning a combination of features that uniquely identify a person. If two datasets have related records, one person's digital fingerprint should be the same in both. This allows linking of a person's data from the two datasets – if one dataset has names then the other dataset can be re-identified.[56]

As noted by data sources that have been identified as sources of reidentification include social network connections[57] and mobility data.[58] It has also been found that '[s]imply linking with online information can work'.[59]

(ii) Consequential risks and harms

Increased exposure to online marketing

Marketing activities are a key driver for the collection of personal information. In the absence of regulation, it is highly likely therefore that a child or young person whose information is collected will receive marketing materials that are specifically targeted at them. Marketing is designed to encourage the purchase of products and may pose financial risks if a child increases their spending by making impulse purchases or spends money on products that they cannot afford and would not otherwise have purchased.

If the products advertised are unhealthy this may contribute to problems such as obesity, early alcohol consumption or smoking cigarettes or e-cigarettes.[60] Depending on the messages used, marketing to children may also result in modified psychological or mental health changes such as negative body image.[61]

Further concerns about the influence of online marketing include sexualisation of children, entrenchment of gender stereotypes, stigmatisation of poverty and reductions in parents' authority and influence.[62] Finally, there is the issue that 'marketer-controlled outputs may be able to monopolize the sources of online information', thereby having a disproportionate impact on identity development.[63]

---

[56] Ibid p 7.
[57] Arvind Narayanan, Elaine Shi & Benjamin Rubinstein, 'Link Prediction by De-anonymization: How We Won the Kaggle Social Network Challenge', The 2011 International Joint Conference on Neural Networks, October 2011, <https://arxiv.org/pdf/1102.4374.pdf>.
[58] Arvind Narayanan & Vitaly Shmatikov, 'Robust De-anonymization of Large Sparse Datasets', Security and Privacy, May 2008, <https://www.cs.cornell.edu/~shmat/shmat_oak08netflix.pdf>.
[59] Michael Barbaro & Tom Zeller Jr, 'A Face Is Exposed for AOL Searcher No. 4417749' *The New York Times* (9 August 2006) <https://www.nytimes.com/2006/08/09/technology/09aol.html>; Charles Duhigg, 'How Companies Learn Your Secrets', *The New York Times* (16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
[60] Matthew A Lapierre et al, *The Effect of Advertising on Children and Adolescents* (2017) 140(2) *Pediatrics* 140 (Supplement 2) November 2017) S152, S153 <https://doi.org/10.1542/peds.2016-1758V>.
[61] Ibid; Shelly Grabe, L Monique Ward and Janet Shibley Hyde, 'The role of the media in body image concerns among women: a meta-analysis of experimental and correlational studies' (2008) 134(3) *Psychological Bulletin* 460–476.
[62] Unicef, *Children and Digital Marketing: Rights, risks and responsibilities,* Discussion Paper (July 2018) <https://www.unicef.org/csr/files/Children_and_Digital_Marketing-_Rights_Risks_and_Opportunities(1).pdf> 19.
[63] Kennedy, Jones and Williams (n 27), 1493.

Moreover, the use of Big Data analytics to inform marketing activities has the potential to result in manipulation and to impair children's decisional autonomy. This manipulation can arise via combining information gathered about preference and past activities with behavioural research to exploit biases, emotions and vulnerabilities. For example: advertisers may filter the available information; they may target consumers at the time when their willpower is lowest; or they may craft their advertisements to act upon known purchasing triggers of particular individuals, for example, feelings of guilt or obligation, or concerns about missing out, or a desire to emulate friends or celebrities.[64]

This has significant implications for several key rights:

> According to the [United Nations Special Rapporteur in the field of cultural rights], "The dominance of specific narratives and world views promoted through commercial advertising and marketing in public spaces, the family and private spheres, combined with an increased deployment of techniques that may influence people at a subconscious level, raises particular concerns in terms of freedom of thought, opinion and, more widely, cultural freedom."[65]

Increased exposure to e-safety harms

There is a link between the disclosure of children's personal information and their susceptibility to what are commonly described as 'e-safety harms'. Issues relating to e-safety have received in-depth analysis in two reports of Australian Parliamentary Committees[66] and a range of research papers commissioned by the eSafety Commissioner.[67]

An important aspect of e-safety relates to cyberbullying. There is a growing body of literature about the prevalence of cyberbullying.[68] A 2014 synthesis of Australian studies estimated that around 20% of the young Australians aged between 8 and 17 years had experienced cyberbullying over a 12-month period. It is likely that this percentage has increased with increased internet and mobile use. A more recent survey conducted in the US in 2018 found that 59% of teens had been bullied or harassed online.[69] Bullying can result in serious

---

[64] Kayleen Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (2017) 17(2) *Oxford University Commonwealth Law Journal* 265, 278. See further Anthony Nadler and Lee McGuigan, 'An impulse to exploit: the behavioral turn in data-driven marketing' (2018) 35(2) *Critical Studies in Media Communication* 151.
[65] Unicef, *Children and Digital Marketing* (n 62) 18.
[66] Australian Government, Department of Communications and the Arts (Cth), *Reviews of the Enhancing Online Safety Act 2015 and the Online Content Scheme- Discussion Paper* (June 2018); Joint Select Committee on Cyber-Safety, Parliament of Australia*, High-wire act: cyber-safety and the young: Interim report* (June 2011).
[67] For published reports, see <https://www.esafety.gov.au/about-us/research>.
[68] See eg Ilan Katz et al, *Research on youth exposure to, and management of, cyberbullying incidents in Australia*, Synthesis Report 16/2014 (June 2014) (Social Policy Research Centre, Sydney).
[69] Monica Anderson, 'A Majority of Teens Have Experienced Some Form of Cyberbullying', Pew Research Center, Web Page (27 September 2018) <https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/>.

emotional harms, such as anxiety, stress and depression, as well as lead to substance abuse and, in extreme cases, even suicide.[70]

There is also evidence that links a child's susceptibility to bullying to the nature and extent of his or her online activities. This is more likely to be the case with social media disclosures but can also potentially arise due to exposures in other online contexts such as games, especially as disclosures may be encouraged as a means of collecting personal information.

Content-based risk

Children may potentially be exposed to a range of harmful materials online, including sexually explicit material, disturbingly violent material, and material promoting harmful behaviours including drugs, gambling and terrorism. While this exposure is not always privacy-related, children can be more readily targeted if their personal information is available.

This issue has been most closely considered in the context of explicit sexual material. An Australian Senate Committee Report cites a submission by the Royal Australasian College of Physicians stating that:

> the available Australian studies have 'consistently demonstrated that a high proportion of young people are viewing pornography on the internet'. It explained: One study has found that 28 per cent of 9 to 16-year-olds have seen sexual material online, though of particular concern is the indications that the percentage is 73 per cent for 15 to 16-year-olds.[71]

Considering the submissions presented to it about this issue, the report concluded that:

> Depending on their age, stage of development and other factors, there are valid concerns about whether exposure to this material influences the healthy development of children and young people, particularly with respect to the formation of respectful relationships and ability to make decisions about sexual activity. Although some children and young people may not be bothered or affected by this material, it is likely that many others would be.[72]

However, the report also stressed the need to obtain expert advice about the implications for healthy sexual development of children and young people at different ages and different development stages.

Contact risks

Another important category of e-safety is the contact risk to which children may be exposed, including risks of stalking and sexual grooming. The disclosure of their personal information

---

[70] See Sarah Knapton, 'Cyberbullying makes young people twice as likely to self harm or attempt suicide', *The Telegraph (UK)* (22 April 2018) <https://www.telegraph.co.uk/science/2018/04/22/cyberbullying-makes-young-people-twice-likely-self-harm-attempt/>.
[71] Senate Environment and Communications References Committee, *Harm being done to Australian children through access to pornography on the Internet* (November 2016), 10, citing Royal Australasian College of Physicians, Submission 112, 2.
[72] Ibid.

online increases these risks by enabling strangers to identify, locate and contact children. Survey evidence gathered in 2011 indicated that 34% of Australian children had had contact online with someone they had not met face-to-face and that some of these had then gone on to meet in person.[73]

Sexual grooming may be defined as 'engaging in predatory conduct to prepare a child or young person for sexual activity at a later time'.[74] It is facilitated by online environments as 'the anonymous nature of the internet allows offenders to masquerade as children in cyberspace to gain the confidence and trust of their victims over a period of time before introducing a sexual element into the online conversation and eventually arranging a physical meeting. The lack of visual cues in cyberspace that may assist child victims in making judgments about the suitability, trustworthiness and sincerity of others with whom they communicate also facilitates the grooming process for offenders.'[75]

Fraudulent activity

A final category of e-safety relates to fraudulent activity, including scams. While this is generally less of an issue for children given that most do not have access to much money or credit cards, children can potentially be vulnerable to online scams and even to identity theft. The latter may be an issue if it results in reputational harm or poor credit ratings. It may also be the case it that theft of children's identities may pass unnoticed for longer given they are less likely to identify the red flags that would be recognised by adults.

Increased exposure to the risks of reputational harms, negative decisions and reduced opportunities

Reputational damage

An important privacy-related harm that can arise from loss of control over personal information is reputational harm. Reputation has been described as the collective or shared perception about us, which is 'forged when people make judgments based upon the mosaic of information available about us'.[76] These judgments about individuals have social and economic importance because '[w]e look to people's reputations to decide whether to make friends, go on a date, hire a new employee or undertake a prospective business deal'.[77]

---

[73] Lelia Green et al, 'Risks and safety for Australian children on the internet' (2011) 4(1) *Cultural Science* 1, 9.
[74] See Victorian Department of Education and Training, 'Child Sexual Exploitation and Grooming', Web Page <https://www.education.vic.gov.au/school/teachers/health/childprotection/Pages/expolitationgrooming.aspx - link2>.
[75] Kim-Kwang Choo 'Responding to online child sexual grooming: an industry perspective', Trends & Issues in Crime and Criminal Justice No 379 (Australian Institute of Criminology, July 2009) <https://www.aic.gov.au/publications/tandi/tandi379> 2.
[76] Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press (2007) 30.
[77] Daniel J Solove, 'Social Networks May Erode Young People's Privacy', in Roman Espejo (ed), *Social Networking*, Greenhaven Press (2011), 72, 76.

Maintaining their reputation online is a concern for everyone, including children, because damaging information which may continue to exist and be used for decision-making long after it is gathered or has lost its currency. As explained in a Unicef Discussion Paper,

> Even simple activities like playing an online game, attending a public event, or commenting on a news article can indefinitely capture discrete moments in children's lives. Taken together, this information creates public online representations of children's lives about which they may neither know nor feel comfortable. This not only has clear and immediate implications for children's privacy and autonomy, but also extends well into adulthood as it may impact future employment, relationships and financial inclusion.[78]

Negative decisions and reduced opportunities

The persistence of data collected has important implications for children given the expected period of lifetime ahead them, raising 'significant implications for their public/digital identity, their capacity to shape this sphere, and the longer-term impacts and outcomes'[79] that flow from the availability of personal information.

The collection and sharing of children's personal data adds to the overall pool of information which can be drawn on as a basis for making decisions that affect them. This may have potential negative implications, especially for individuals with attributes that have the potential to result in negative profiling (irrespective of whether the information is reputationally damaging).

Big Data Analytics and artificial intelligence increasingly make possible the automation of decision-making based on personal data and algorithms. Automation can affect administrative decision-making by government agencies and the private sector, such as the prices and terms on which key products and services are provided. Potential harms include that children may be exposed to decisions during their childhood and beyond that cause discrimination or otherwise reduce their life opportunities.

It has been suggested that an individual's lack of control over their digital identity:

> could potentially impact their access to educational, employment and financial opportunities, enhance their potential exposure to discrimination, and at the more extreme end of the spectrum, allow political actors to use this data to assert control over their lives and regulate their personal and political expression.[80]

---

[78] Unicef, *Privacy, Protection of Personal Information and Reputation*, Discussion Paper (March 2017) <https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> 18.
[79] Gabrielle Berman and Kerry Albright, 'Children and the Data Cycle: Rights and Ethics in a Big Data World', UNICEF Office of Research – Innocenti Working Paper no. 2017-05 (2017) <https://www.unicef-irc.org/publications/907/> [2.5].
[80] Ibid. See also Mie Oehlenschlager, UK Children's Commissioner: More data is collected about children growing up today than ever before, Blog (15 December 2018) <https://dataethics.eu/uk-childrens-commissioner-report-who-knows-what-about-me/>.

Question 1c — Do digital platforms or other organisations that operate online have any existing restrictions or other measures designed to mitigate risks/harms relating to the collection, use and disclosure of a child's personal information?

Key findings:

All social media platforms evaluated (ie Facebook, Instagram, YouTube, Snapchat, Twitter, Apple and Google) have content moderations controls that specifically address risks to children, although these are not cohesive and are individual to the platform.

All social media platforms and big tech companies evaluated have advertising controls for minors, although these are not cohesive and are individual to the platform or company.

The majority of social media platforms evaluated (Facebook, Instagram, YouTube, Snapchat and Twitter) do not provide parental controls, however, several of them do offer a child-specific platform. Google and Apple have a range of parental controls.

(i) Introduction

This section provides a survey of selected major digital platforms operating in Australia, based on their overall audience (Facebook, YouTube, Instagram, Twitter) and popularity among children (Snapchat, Tiktok). We also included Apple and Google as technology platform providers (iOS and Android) who play a key role in setting rules for app developers, controlling access to device data and sensors, and providing accessibility and parental control features.

The products, services and business models of the platforms reviewed vary widely, and we observed a high degree of variability in policy and approach between platforms. In general, we see a tendency to focus on eSafety and protecting children from inappropriate content and advertising. Publicly available information deals primarily with what platforms do to constrain the behaviour of platform users and other commercial actors (app developers, advertisers, or commercial accounts operating on the platforms). Comparatively little information is available on the ways in which platform providers themselves handle children's data.

None of the platforms presents a single, consolidated approach to addressing children's privacy. Measures relevant to children's privacy appear across online FAQs, news pages, blog posts, community guidelines, terms of service, privacy policies, transparency reports, developer guidelines and other documents. While services which allow users under 13 through managed accounts, namely Google[81] and Apple[82], maintain policies that are specific to the collection, use and disclosure of children's data, children are mostly accounted for within platform's general policies which apply to all users.

[81] Google, 'Family Link Disclosure for Parents of Children under 13', Web Page <https://families.google.com/familylink/privacy/notice/>.
[82] Apple, 'Family Privacy Disclosure for Children', Web Page <https://www.apple.com/legal/privacy/en-ww/parent-disclosure/>.

Most platforms policies are enacted on a voluntary basis and are subject to frequent change. Working through these various sources to come to a holistic view of how a child's personal information is likely to be collected, used and disclosed, what protective measures are in place, and how content is likely to be presented to the child based on what is known about them is an extremely complex task, even for professionals in the field. In particular, we observed that the general trend towards layered presentation of information and policies added complexity and significant friction toward gaining an understanding platform's policies and practices.

(ii) Age verification

The ability to effectively impose restrictions and mechanisms to mitigate the processing of children's data, including the prohibition of access to services by minors, hinges on the ability to identify that users are minors. Among the broad range of technical measures that can be used to establish the age of users, all platforms rely on self-identification by minors on sign-up, presenting a neutral birth date field. In some cases, platforms supplement this approach with technical safeguards such as the implementation of cookies to prevent repeated attempts as well as peer reporting. In relation to platforms which allow managed accounts, Google and Apple, credit card verification is often employed.

Where the age of users is not accurately identified, users may gain access to content that is not age appropriate such as offensive graphic content, and inappropriate advertising such as ads for alcohol, gambling etc. Additionally, differences in functionality will not be properly applied. This applies to users under 13, as well as teen users, where such differences exist.

Age verification is of relevance to platforms that have a minimum age for users. This age is generally set at 13, which may be a result of requirements under the US Children's Online Privacy Protection Act (COPPA), which is discussed in detail in response to question 2a. The effectiveness of age-verification which focuses on self-attestation, seemingly inspired by COPPA, has been subject to criticism, as children commonly lie about their age. A UK Government report on online age verification observed that COPPA's 'implementation has had the unintended consequence of disincentivising platforms from actively recognising which of their users are children and designing age appropriate environments for them'.[83]

Facebook

Facebook requires users to have an account to engage with its services and sets the minimum age to create an account at 13. Facebook primarily relies on self-attestation and implements age verification processes on sign-up by requiring users to enter their birth date.

After users input an age, Facebook employs various technical and design measures to prevent users from circumventing Facebook's policies through repeated attempts.[84] If a user enters a birth date below 13, Facebook displays a general error message rather than

---

[83] UK Government, Department for Digital, Culture, Media and Sport (UK) and Home Office (UK), *VoCO (Verification of Children Online) Phase 2 Report*, Policy paper (November 2020) <https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report> 12.
[84] Facebook, *ICO Age Appropriate Design Code: Consultation* (2019) <https://ico.org.uk/media/about-the-ico/consultations/aadc/2616652/facebook-age-appropriate-design-code-consultation-document-form.pdf>.

informing the user that they were blocked due to Facebook's age requirements. Facebook also places cookies on web browsers that records that the browser was previously blocked due to Facebook's age requirements.

In addition to age-verification measures on sign up, Facebook encourages reporting of underage accounts.[85] Facebook states that if an account is 'reasonably verifiable' as under 13, the account will be deleted. No further information on this standard is provided. Alternatively, Facebook suspends the reported user's account and requires the user to upload evidence of their age. Facebook outlines acceptable forms of identification, including government identifiers. It also allows for the use of non-government identifiers such as school cards and records.[86] This is significant as children under 13 may be less likely to hold government-issued identification.

While the review of accounts of underage users was previously limited to accounts which were specifically reported as underage, Facebook recently updated their guidance to reviewers to suspend any accounts if there is a strong indication that the account is underage, even if the account was reported, or discovered by reviewers, for unrelated reasons.[87]

Facebook states that on detecting an account of a child under the age of 13, the account is promptly deleted. Facebook also provides parents with the opportunity to request information from a child's account before deletion and requires parents to provide a notarised statement declaring their rights as a parent/guardian.[88]

Instagram

As with its parent company Facebook, Instagram requires users to be at least 13 to sign up for an account. However, Instagram only introduced a requirement for users to enter their age on sign up in December 2019. [89] Previously, Instagram merely required users to state that they were 13. The requirement to enter an age on sign up only applies to new users and does not retroactively require users to input their birth date. Therefore, Instagram does not have any self-attestation-based age verification measures in place for pre-existing users.

As with Facebook, Instagram encourages the reporting of underage accounts and adopts do so for age-verification purposes, citing concerns surrounding 'accuracy' and 'transparency'.[90]

---

[85] Facebook, 'Report an Underage Child', Web Page <https://www.facebook.com/help/contact/209046679279097>.
[86] Facebook, 'Please verify your information', Web Page <https://www.facebook.com/help/contact/199052956872279>.
[87] Josh Constine, 'Facebook and Instagram change to crack down on underage children', TechCrunch (20 July 2018) <https://techcrunch.com/2018/07/19/facebok-under-13/>.
[88] Facebook, 'How do I request data from my underage child's Facebook account?', Web Page <https://www.facebook.com/help/173734372685099?helpref=search&sr=28&query=verify%20age&search_session_id=8a0eac07574b325911b198ac8be12231&rdrhc>.
[89] Instagram, 'Making Instagram Safer for the Youngest Members of Our Community', Blog (4 December 2020) <https://about.instagram.com/blog/announcements/making-instagram-safer-for-the-youngest-members-of-our-community>.
[90] Paresh Dave, 'Instagram to collect ages in leap for youth safety, alcohol ads', *Reuters* (5 December 2019) <https://www.reuters.com/article/us-facebook-instagram-children-idUSKBN1Y826Z>.

Snapchat

Snapchat requires users to have an account in order to use the service and requires users to be at least 13 years old. On sign up, Snapchat requires users to provide a date of birth. Similarly, Snapchat does not inform underage users that sign up has failed due to not meeting Snapchat's age requirements, and places cookies on web browsers to discourage repeated attempts.[91]

Snapchat does not have an in-app reporting function for reporting underage users. Rather, Snapchat asks parents to contact Snapchat with the child's username and verification of the parental or guardianship relationship.[92] Notably, this limits the scope of reporting to the parents of underage users and does not seem to allow for peer-reporting or reports from third parties such as teachers.

Additionally, Snapchat has claimed that it looks for 'inference signals' to identify underage accounts.[93] However, it does not define this or provide any information about what this means. Snapchat has expressed concern about the effectiveness of self-attestation, its primary age-verification mechanism.[94]

Snapchat claims that it has robust age-gating measures which prevent the storage of underage user's data on Snapchat's servers.[95]

TikTok

TikTok requires users to be 13 to sign up for a TikTok account. However, notably, most videos on TikTok can be accessed without creating an account. TikTok's terms of service also state that users under the age of 18 may only use TikTok with a parent or guardian's consent.

On sign up, TikTok directs users to a page requiring them to input a date of birth. If this date of birth does not meet TikTok's age requirements, users are informed that they are ineligible for TikTok and are not able to create an account. TikTok's in-app reporting options do not provide an option for users to report underage accounts.

As of February 2019, following settlement of a civil lawsuit alleging violation of COPPA requirements in the US, TikTok has reportedly been prompting users to verify their age.[96] This new policy resulted in the deletion of accounts of videos of users under 13. TikTok

---

[91] Snapchat, *Age Appropriate Design Code: Consultation* (2019) <https://ico.org.uk/media/about-the-ico/consultations/aadc/2616709/snap-inc.pdf>.
[92] Snapchat, 'Snapchat Safety Center', Web Page <https://www.snap.com/en-US/safety/safety-center>.
[93] UK Parliament, Digital, Culture, Media and Sport Committeee, Evidenc (19 March 2019) <https://parliamentlive.tv/event/index/70b4d0f0-7995-4149-91b7-394cc235f1dd>.
[94] Isobel Asher Hamilton, 'Snapchat admits its age verification safeguards are effectively useless' *Business Insider* (20 March 2019) <https://www.businessinsider.com.au/snapchat-says-its-age-verification-safeguards-are-effectively-useless-2019-3?r=US&IR=T>.
[95] ICO, 2020. Age Appropriate Design Code: Consultation. Snapchat
[96] Dami Lee, 'TikTok users over 13 are having their accounts deleted after putting in the wrong birthdays', *The Verge* (28 February 2020)

faced technical difficulties in implementing this change, causing confusion amongst users, and has instructed users to submit government ID for age verification.[97]

Twitter

Twitter requires users to be at least 13 to sign up for an account. However, as with TikTok, Twitter's content is generally accessible to users without an account. Twitter also relies on self-attestation, requiring users to enter a birth date on sign up. If a user enters an age under 13 years old, Twitter displays a general message indicating that sign up is currently unavailable.

Twitter has a form to report underage accounts.[98] After GDPR, Twitter began locking users out of accounts if the user was suspected of being underage. This approach was criticised as being overly aggressive, as it applied to accounts of users who signed up when they were under 13 even if the user met the age requirement at the time of account suspension.[99] In response to this, Twitter has created an option for users to recover such accounts, requiring users to delete all Tweets, likes, direct messages, profile details, moments, lists, and collections created before the user was 13.[100]

Apple

Apple sets its minimum age to create an account and use Apple services at 13. All users are asked to provide a date of birth on sign up. If users do not meet Apple's age requirements, a general error message is displayed, and cookies are placed on the web browser to prevent circumvention through repeated attempts. Notably, some Apple services such as Safari are accessible to users without an account.

However, Apple enables parents and guardians to create accounts for users under 13 through its managed account offering, 'Family Sharing'. Apple has indicated that in order to comply with child online privacy laws, parental consent for the collection of data from users under 13 is obtained through payment method verification. This requires parents or guardians to verify consent with a payment method's CVV, security code or with a verification code sent via SMS.[101] However, Apple does not require proof of relationship between a child and the guardian or parent providing consent.

Apple also states that it will take steps to delete personal information collected of a child under 13 as soon as possible and provides parents the option to contact Apple to access, correct and delete data associated with their Family Sharing account or child's Apple ID.[102]

---

[97] TikTok, *Twitter* (28 February 2019, 8:12am) <https://twitter.com/tiktok_us/status/1100866314204139520?lang=en>.
[98] Twitter, 'Twitter privacy policy inquiries', Web Page <https://help.twitter.com/forms/privacy>.
[99] Sarah Perez, 'After year-long lockout, Twitter is finally giving people their accounts back', Tech Crunch (2018) <https://techcrunch.com/2019/05/14/after-year-long-lockout-twitter-is-finally-giving-people-their-accounts-back/>.
[100] Twitter, 'About account restoration', Web Page <https://help.twitter.com/en/managing-your-account/account-restoration>.
[101] Apple, 'Family Sharing and Apple ID for your child', Web Page <https://support.apple.com/en-au/HT201084>.
[102] Apple, 'Apple Privacy Policy', Web Page (31 December 2019) <https://www.apple.com/legal/privacy/en-ww/>.

Google

Google requires users to be at least 13 in order to manage their own account, but like Apple, allows parents or guardians to set up 'Supervision', Google's managed account option. On sign up, Google requires users to input a date of birth. If the date of birth entered does not meet Google's minimum age requirement, the child is directed to enter the parent or guardian's contact details in order to set up a supervised account. In order to set up parental supervision, parents or guardians are required to live in the same country as their child and are asked to provide parental consent. Unlike Apple, parental consent does not require further verification by payment method or otherwise.[103] Some Google services, such as Chrome and YouTube are accessible to users without the creation of an account although the full suite of features, such as personalisation, may be unavailable.

If an account is flagged for failing to meet Google's minimum age requirements, users are offered a 14-day grace period in order to set up supervision or verify that the user meets Google's age. During this time, Google allows users to download their data. Once this time period ends, users' accounts are disabled and the information associated with the account is deleted. In order to verify age, users must either upload a government-issued ID or charge a temporary authorisation to a credit card to verify date of birth.[104]

YouTube

While YouTube does not generally require users to sign, if a user opts to create an account YouTube requires users to sign in using a Gmail account. YouTube's age requirement and age verification processes are covered by Google's policies. In some cases, YouTube imposes additional age verification requirements. In accordance with the EU Audiovisual Media services Directive, YouTube has stated that it is introducing new age verification measures for users in the EU, when the user is attempting to watch mature content and their systems cannot establish that a user is above the age of 18. This will require users to provide a valid ID or credit card.[105] When content is age-restricted, users coming to YouTube must be signed-in and their account age must be 18 or older in order to view the video.[106]

While YouTube allows for reporting of videos featuring minors, YouTube does not offer a reporting option for suspected underage accounts.

(iii) Content moderation

All of the platforms evaluated rely on their own community standards (sometimes referred to as 'community guidelines') which provide guidance on what is acceptable to post online and explicitly prohibit certain types of content including illegal content; sexually explicit content; and content including harassment and hate speech; self-harm; and dangerous acts. On all

---

[103] Google, 'Provide consent & add supervision to your child's Google Account', Web Page <https://support.google.com/families/answer/9499456?>.
[104] Google, 'Update your account to meet age requirements', Web Page <https://support.google.com/accounts/answer/1333913?hl=en>.
[105] YouTube, 'Using technology to more consistently apply age restrictions', Blog (22 September 2020) <https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/>.
[106] Ibid.

platforms evaluated, child sexual abuse content is prohibited. While this provides a base level of protection for all users, including children, community standards commonly impose additional prohibitions for content featuring children. In addition to prohibiting specific content, platforms such as YouTube and Facebook impose age-restrictions on content that does not violate community standards but may not be appropriate for all users.

Common tools for identifying violative content include the use of AI, content moderation teams and social reporting. Additionally, in relation to age-restricted content, page administrators also contribute to moderation efforts. While enforcement options for violations range from content deletion to account deletion, all digital platforms escalate child sexual abuse violations to the US National Centre for Missing & Exploited Children.

Notably, child-focused products such as YouTube Kids and Messenger Kids do not have separate community standards but instead rely on the standards applicable to their main platforms. However, an increased focus on moderation tools and a stricter approach to enforcement is adopted.

YouTube and YouTube Kids

Among other prohibitions, YouTube's community guidelines include a designated 'Child Safety' section.[107] This section explicitly prohibits content endangering the emotional and physical well-being of minors.[108] These prohibitions focus on content involving or aimed at minors and include prohibitions on content featuring the sexualisation of minors; harmful or dangerous acts involving minors; the infliction of emotional distress on minors; misleading family content; and cvber bullying and harassment involving minors. Child safety reasons account for nearly a third of all video removals on YouTube.[109]

Violative content on YouTube is identified by various means including human-review, community flagging, and 'trusted flagging', which comprises flagging by trusted individuals, government agencies and NGOs with subject matter expertise. Additionally, YouTube's automated flagging systems are a significant means for protecting children from inappropriate content on YouTube, accounting for detection of over 95% of all violative content removed from July -September 2020.[110] Notably, YouTube's machine learning efforts include its proprietary technology for identifying child sexual abuse images and YouTube's Trusted Flagger program includes child safety organisations.[111] YouTube states that it has a zero-tolerance policy towards predatory behaviour. Violative content is removed

[107] YouTube, 'Community Guidelines', Web Page <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/#community-guidelines>.
[108] YouTube, 'Child Safety on YouTube', Web Page <https://support.google.com/youtube/answer/2801999?>.
[109] Google Transparency Report, 'YouTube Community Guidelines enforcement', Web Page <https://transparencyreport.google.com/youtube-policy/removals?>.
[110] Ibid.
[111] Google Transparency Report, 'Featured policies', Web Page <https://transparencyreport.google.com/youtube-policy/featured-policies/child-safety?hl=en>.

in accordance with YouTube's 'three strikes' approach, which results in account deletion for repeat violators or for gross violations.[112]

As well as prohibiting certain types of content, YouTube age-restricts content that does not violate its community standards but may be inappropriate for users under 18.[113] YouTube employs this approach towards content containing themes such as child safety; harmful or dangerous activity; sexually suggestive content; violent and graphic content; and vulgar language. YouTube places the onus on content creators to age-gate content which may not be appropriate for viewers under 18.[114] While primarily reviewed manually by YouTube's Trust & Safety team, YouTube has recently committed to adopting machine learning to better identify and automatically age-restrict this content.[115] Once content is age-restricted, it is not available when 'restricted mode' is enabled, and users must be over 18 and signed in to view this content. Users under 18 are presented with a warning screen and are redirected to more age-appropriate content. To ensure that all videos hosted on YouTube are displayed to appropriate audiences, age-restricted videos cannot be played on third-party sites. Additionally, in response to COPPA, YouTube requires content creators to set an audience and classify whether content is 'made for kids', after which additional safeguards apply.[116]

As noted, YouTube's general community guidelines and moderation tools apply to YouTube Kids. However, YouTube Kids provides a curated ecosystem for children by relying on more restrictive proactive filtering, machine learning and human review.[117]

Facebook, Instagram and Messenger Kids

Like YouTube, Facebook's community guidelines apply across Facebook's products, including Messenger Kids, in which community standards are applied more strictly. While Instagram has its own set of community standards, in general, Facebook and Instagram share content policies on what constitutes violative content.[118] Facebook's policies and enforcement are also informed by the Facebook Safety Advisory Board, which is made up of various online safety organisations, including child safety organisations.[119] Facebook

---

[112] YouTube Help, 'Community Guidelines strikes basics', Web Page <https://support.google.com/youtube/answer/2802032?hl=en#:~:text=Three%20strikes%20in%20the%20same,will%20not%20remove%20your%20strike>.
[113] YouTube Help, 'Age-restricted content', Web Page <https://support.google.com/youtube/answer/2802167?hl=en>.
[114] YouTube Help, 'Age-restrict your own videot', Web Page <https://support.google.com/youtube/answer/2950063?hl=en>
[115] YouTube, 'Using technology to more consistently apply age restrictions'', Blog (22 September 2020) <https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/>.
[116] YouTube Help, 'Determining if your content is "made for kids"', Web Page <https://support.google.com/youtube/answer/9528076?hl=en>.
[117] Jared Newman 'How YouTube is trying to fix its Kids app without ruining it', *Fast Company* (6 October 2019) <https://www.fastcompany.com/90323376/youtube-kids-is-still-ruled-by-the-algorithm-for-better-or-worse>.
[118] Facebook Transparency, 'Community Standards Enforcement Report', Web Page (November 2020) <https://transparency.facebook.com/community-standards-enforcement>.
[119] Facebook Community Standards, 'Child sexual exploitation, abuse and nudity', Web Page <https://www.facebook.com/communitystandards/child_nudity_sexual_exploitation>.

moderates content by prohibiting certain content categories and age-restricting visibility of content to minors.

While Facebook's community standards govern content moderation for all users, with respect to prohibited content such as bullying, Facebook claims that it recognises the increased risk for users between the ages of 13 to 18. As a result, Facebook provides increased protections by widening the definition of what constitutes bullying for individuals who are minors. For example, under Facebook's bullying and harassment policy, comparing a child to an animal such as a 'cow' constitutes bullying and is prohibited, although this may not be considered violative if the comparison is made toward a user over 18.[120] Unlike YouTube, Facebook does not have a designated 'Child Safety' section, however Facebook's standards specify prohibitions on child nudity and sexual exploitation of children. In its latest transparency report, Facebook claims that the prevalence of this content is very infrequent both on Facebook and on Instagram.[121]

Facebook also employs multiple means for identifying violative content and content that may not be age appropriate.[122] Facebook employs proactive match detection which immediately screens all content submitted to Facebook with a focus on identifying child exploitation imagery using AI known as PDQ and TMK+PDFQ.[123] After initial automated screening, Facebook relies on further AI in order to identify potentially violative content, including the use of proactive detection AI to identify suicide and self-injury content,[124] and to detect bullying in photos and comments on Instagram.[125] Algorithms then assess the likelihood that the piece of content violates a community standard, and, if indicated, is either automatically removed or subject to human review. Facebook also relies on social reporting and provides reporting links on every piece of content. In addition, Facebook provides a form for parents for the removal of images of children under 13.[126] After being flagged, an automated system determines whether the content is automatically removed or routed to a human reviewer. Facebook disables accounts for repeat offenders or severe violation.

Facebook also age-restricts the visibility of content which may not be appropriate to minors. Namely, while content of a graphic and violent nature is covered by an interstitial warning for adults, this content is not available for minors. Additionally, the visibility of content promoting regulated goods is restricted to adults over 18. This includes alcohol and tobacco, bladed

---

[120] Facebook Community Standards, 'Bullying and harassment', Web Page <https://www.facebook.com/communitystandards/bullying>.
[121] Facebook Community Standards, 'Child sexual exploitation, abuse and nudity', Web Page <https://www.facebook.com/communitystandards/child_nudity_sexual_exploitation>.
[122] Ben Bradford et al, *Report of the Facebook Data Transparency Advisory Group*, Technical Report (Yale Law School (2019) <https://law.yale.edu/system/fles/area/center/justice/document/dtag_report>.
[123] Antigone Davis and Guy Rosen, 'Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer', *Facebook Newsroom* (1 August 2019) <https://about.fb.com/news/2019/08/open-source-photo-video-matching/>.
[124] Catharine Card, 'How Facebook AI Helps Suicide Prevention', *Facebook Newsroom* (10 September 2018) <https://about.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai>.
[125] Instagram, 'New Anti Bullying Tools on Instagram', Blog (9 October 2018) <https://about.instagram.com/blog/announcements/anti-bullying-tools-on-instagram>; Katy Steinmetz, 'Inside Instagram's War on Bullying', Time (8 July 2020) <https://time.com/5619999/instagram-mosseri-bullying-artificial-intelligence>.
[126] Facebook, 'How do I report a child under the age of 13 on Facebook?', Web Page <https://www.facebook.com/help/157793540954833>.

weapons, weight loss products and potentially dangerous cosmetic procedures. In addition to this, like YouTube, Facebook requires page admins to age-gate their pages if displaying content that may not be appropriate for all users.[127]

On Messenger Kids, Facebook exercises a stricter approach towards removing violations. Content that may be age-restricted on Facebook is deleted on Messenger Kids. For Messenger Kids, Facebook has a specialised kid content moderation team. [128]

TikTok

TikTok's community guidelines have specific guidelines on safety for minors, which are aimed at content depicting minors.[129] Additionally, among TikTok's general guidelines, it explicitly prohibits the posting of: nudity and sexual exploitation involving minors; underage delinquent behaviour (i.e. minors consuming or possessing alcohol, drugs or tobacco); child abuse; grooming behaviour; and content which sexualises minors. In its most recent transparency report, TikTok states that 'minor safety' accounts for 22.3% of video removals.[130] TikTok relies on both technology and human content moderators to identify violative content and offers an in-app reporting feature.

Snapchat

Snapchat's community guidelines specifically address and prohibit the posting, saving or sending of sexually explicit content involving anyone under 18 and provides in-app reporting, where a user can press a 'white flag' button directly on the snap which acts as a report.[131] Snapchat also relies on automated methods for identifying violations.[132]

Twitter

Twitter's Rules state that it has a zero-tolerance approach towards child sexual exploitation, and the platform provides a direct reporting form for such violations.[133] Twitter relies on human moderators and proactive technology to moderate content.[134] Twitter employs

---

[127] Facebook, 'Age gating', Web Page <https://m.facebook.com/policies/pages_groups_events/pages_specific_policies/age_gating>; Instagram 'Why do I have to be over a certain age to view some Instagram accounts?' Web Page <https://help.instagram.com/801322493288277>.
[128] Facebook, 'Facbeook's Messenger Kids" Important new digital-parenting tool', Web Page <https://www.facebook.com/safety/parents/conversations/facebooks-messenger-kids-important-new-digital-parentingtool#:~:text=Messenger%20Kids%20has%20its%20own,informed%20of%20how%20that%27s%20going>.
[129] TikTok, 'Community Guidelines', Web Page <https://www.tiktok.com/community-guidelines?lang=en>.
[130] TikTok, *TikTok Transparency Report* (22 September 2020) <https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en>.
[131] Snap Inc, 'Information for Law Enforcement', Web Page <https://www.snap.com/en-US/safety/safety-enforcement>
[132] Snap Support, 'Brand Safety', Web Page <https://support.snapchat.com/en-US/a/brand-safety>.
[133] Twitter Help Center, 'The Twitter Rules', Web Page <https://help.twitter.com/en/rules-and-policies/twitter-rules>.
[134] Twitter Help Center 'About specific instances when a Tweet's reach may be limited', Web Page <https://help.twitter.com/en/rules-and-policies/twitter-reach-limited>.

multiple means for enforcing its guidelines, including limiting tweet visibility, removing tweets, and suspending accounts. Notably, Twitter is the only digital platform evaluated which explicitly states that child sexual exploitation content will result not only in removal of content, but also in immediate and permanent account suspension. Additionally, Twitter has a sensitive media policy which addresses content that may be inappropriate for minors, such as violent, hateful or adult content.[135] While some of this content is prohibited, in order to limit the visibility and sharing of sensitive content, Twitter requires that users seeking to share sensitive content mark their accounts as sensitive. This results in the content being placed behind a warning message.

(iv) Advertising standards

The digital platforms evaluated lack a cohesive approach towards regulating advertising to minors in their advertising standards. Protective measures include not displaying advertising to children; restricting the personalisation of ads for children; prohibiting content within advertising; and limiting the ability for advertisers to target ads in certain product categories to minors.

Apple

Apple does not allow personalised ads for a child's Apple ID, and only allows non-targeted advertising on devices associated with a child's Apple ID.[136] Additionally, Apple imposes advertising restrictions on apps downloaded with a child's Apple ID by disabling 'Allow Apps to Ask to Track' for a child's account.

Apple provides further advertising protections for users in the App Store Review Guidelines.[137] Apple offers minors protection by requiring ads displayed in apps to be appropriate for the app's age rating and, in addition, provides further protections for users under 13. Apple restricts advertising in apps intended primarily for kids, as well as for apps in the Kids Category. Apple permits contextual advertising in limited cases in which services have publicly documented practices and policies that include human review for age appropriateness. Additionally, apps in the Kids Category are prohibited from disclosing personally identifiable information or device information to third parties such as data brokers. Further safeguards include requiring interstitials (advertisements that appears while a chosen website or page is downloading) to be clearly labelled.

In addition, Apple Search Ads, which serves ads to promote apps within Apple's app store, does not serve ads to any user whose Apple ID is registered to a minor under 13 years of age or set up as a Managed Apple ID. Apple Search Ads also does not allow explicit targeting of people whose Apple ID is registered to a user under the age of 18.[138]

---

[135] 'Twitter Help Center, 'Sensitive media policy', Web Page <https://help.twitter.com/en/rules-and-policies/media-policy>.
[136] Apple, 'Family Privacy Disclosure for Children', Web Page <https://www.apple.com/legal/privacy/en-ww/parent-disclosure/>.
[137] Apple, 'App Store Review Guidelines', Web Page <https://developer.apple.com/app-store/review/guidelines/#1.3>.
[138] Apple, 'Apple Search Ads and privacy', Web Page <https://searchads.apple.com/privacy/>.

Google

Google's advertising policy provides protection against ads that may be inappropriate for minors through multiple means, including prohibitions on certain ad content for all users; restricted advertising categories, in which only users over 18 can be targeted; and additional advertising protections offered for Family Link accounts.

Google prohibits certain types of advertising content for all users, including advertising relating to certain types of adult content, dangerous products and featuring inappropriate content. In addition, Google's 'restricted content and features' category provides enhanced protection for minors. Specifically, advertisers cannot target users under the age of 18 for non-family-safe content; alcohol; gambling; and other restricted businesses such as high fat, sugar and salt food and beverage ads.

For user accounts under the age of 13 managed through Family Link, Google provides additional advertising protections. Notably, Google states that it will not serve personalised ads to users under 13.[139] Google also mandates that advertising intended for children must not be deceptive, unfair or inappropriate for its intended audience.[140] Google offers additional safeguards such as filtering ads which may not be age appropriate and labelling advertising content.[141]

Google does not share personal information about children under 13 with advertisers and prohibits the collection of personal information from children without first obtaining parental consent. However, it but notes that it may share non-personally identifiable information.[142]

YouTube and YouTube Kids

In addition to being required to comply with Google's advertising policies, advertisers on YouTube are required to comply with additional YouTube-specific policies.[143] Particularly, additional advertising restrictions apply when an advertisement is placed on 'Made for Kids' content.[144] Personalised advertising is prohibited on content set as 'Made for Kids'.

On content that is 'Made for Kids', YouTube prohibits advertising on a more extensive list of product categories such as adult content; illegal and regulated products; beauty and fitness; dating and relationships; fight sports; online or virtual communities; food and beverages; gambling and video games with unsuitable industry ratings.[145] YouTube also prohibits

---

[139] Google, 'Family Link Disclosure for Parents of Children under 13 (or applicable age in your country)', Web Page <https://families.google.com/familylink/privacy/notice/>.
[140] Google Support, 'Google Ads policies', Web Page <https://support.google.com/adspolicy/answer/6008942?>.
[141] Google Support 'Ads & Google Accounts managed with Family Link', Web Page <https://support.google.com/families/answer/7087279?hl=en>.
[142] Google Support, 'Family Link Disclosure for Parents of Children under 13 (or applicable age in your country)', Web Page <https://families.google.com/familylink/privacy/notice/>.
[143] YouTube Help 'Ad policy overview', Web Page <https://support.google.com/youtube/answer/188570?>.
[144] YouTube Help 'Determining if your content is "made for kids", Web Page <https://support.google.com/youtube/answer/9528076?hl=en>.
[145] Google Support, 'Ads & made for kids content', Web Page <https://support.google.com/adspolicy/answer/9683742?hl=en>

advertising containing certain content, such as violent and graphic content; profanity; scary imagery and content displaying significant skin exposure.

Advertisements on YouTube Kids are clearly labelled and must not include click-through to websites or product purchase pages.[146] However, safeguards do not apply to more informal advertising that users may include in user-generated content. YouTube describes this distinction as follows: 'a search for trains could result in train cartoons, songs and videos of real trains, as well as a TV commercial for toy trains uploaded by a user or a toy train company, none of which we consider as Paid Ads, as they are not part of the YouTube Kids advertising program'. YouTube states that ads undergo rigorous review and must be preapproved. Ads are not served on YouTube Kids App if using YouTube Premium.

Facebook and Messenger Kids.

In addition to prohibiting specific content, Facebook's advertising policies restrict targeting users under 18 for certain advertising content, including ads for alcohol; contraceptives; over-the-counter medications; online gambling and gaming; ads promoting various financial and insurance products; cosmetic procedures and weight loss; and entertainment intended for mature audiences.

Facebook Messenger Kids does not display ads. Although not included in the Messenger Kids privacy policy, Facebook has explicitly stated that children's data from Messenger Kids will not be sold or used to inform ads on other apps.[147]

TikTok

TikTok's Advertising Guidelines prohibit ads for various products and services in all countries and regions, as well as containing further prohibited advertising categories for specific countries or regions, including Australia.[148] In Australia, TikTok prohibits ads for products or services that are specifically intended for, or appeal to, children, including toys, games, apps, and clothing (even if the product may be for a general audience) as well as ads marketed specifically toward children. They also prohibit ads promoting weight loss and some other products. In addition to prohibiting certain ads, TikTok only allows the targeting of ads to users above 18 in certain product categories including financial services; pharmaceuticals; healthcare; medicine; dating apps and services; and media and entertainment in accordance with classifications.

Additionally, TikTok restricts content within ads in order to protect minors.[149] This stipulates that ads must not display, facilitate, or promote inappropriate or unsuitable behaviours involving minors and must not display excessive skin exposure of minors.

---

[146] Google Support, 'Ads in YouTube Kids', Web Page <https://support.google.com/youtubekids/answer/6130541?hl=en>.
[147] Morgan Brown, 'Giving Parents Even More Control in Messenger Kids', *Facebook Newsroom* (4 February 2020) <https://about.fb.com/news/2020/02/messenger-kids-controls/>.
[148] TikTok Business Help Center 'TikTok Advertising Policies - Industry Entry', Web Page <https://ads.tiktok.com/help/article?aid=6685586866860720134>.
[149] TikTok Business Help Center 'TikTok Advertising Policies - Ad Creatives', Web Page <https://ads.tiktok.com/help/article?aid=6684149081637388293>.

Twitter

Similarly, Twitter's Ad Policies prohibit certain content, and include additional prohibitions on advertising products and services to minors such as regulated and illegal products; aerosol paint; dietary supplements; ultra-violet tanning devices; body branding and permanent cosmetics; and sexual products or content that is adult in nature.[150] Additionally, Twitter explicitly prohibits advertisers from using Twitter products to reach an audience under the age of 13 and prohibits the use of their advertising services for conversion tracking and creating custom audiences on any platform that collects or stores age information from individuals under 13.[151]

Snapchat

As Snapchat's minimum age is 13, it explicitly requires advertisers to ensure that ads are suitable for users aged above 13, or for the advertiser's targeted audience. Similarly, Snapchat prohibits certain content that is harmful for users of all ages, such as deceptive or hateful content, as well as inappropriate content, which includes ads addressed or intended to appeal specifically to users under 13. Snapchat restricts certain advertising product categories by allowing targeting only to users over the age of 18. This includes ads for dating services; alcohol products; financial products; hormonal contraceptives and condoms; and plastic surgery. Additionally, ads for entertainment media must be age-targeted to the intended audience of content promoted.

(v) Developer guidelines

Apple and Google both offer app ecosystems, the Apple App Store and the Google Play Store respectively, which both house a significant number of third-party apps. Both Apple and Google mandate their own policies and guidelines for third-party app developers which impose technical and content constraints and govern the collection, use and disclosure of children's data within apps. Apps must first comply with such policies before being accepted into the relevant app store.

Apple

As a means of ensuring protection of children using apps from the App store, Apple's App Review Guidelines[152] mandate additional requirements for apps in the Kids category. [153] Notably, the Kids category, and its applicable safeguards, only covers apps specifically designed for kids aged 11 and under. Apple's App Review Guidelines rarely require additional protection for users 12 to 18 years old.

---

[150] Twitter Business, 'Prohibited content for minors', Web Page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/prohibited-content-for-minors.html>.
[151] Twitter Business, 'Policies for conversion tracking and custom audiences', Web Page <https://business.twitter.com/en/help/ads-policies/campaign-considerations/policies-for-conversion-tracking-and-custom-audiences.html>.

[152] Apple, 'App Store Review Guidelines – Apple Developer', Web Page <https://developer.apple.com/app-store/review/guidelines/>.
[153] Ibid [1.3].

Apple ensures that apps are appropriately categorised, and do not inappropriately imply that the main audience of the app is children, by reserving the use of terms related to children in app metadata to apps in the Kids Category.[154]

All apps on the App store are subject to Apple's content restrictions. These broadly prohibit broadly prohibits apps that include 'objectionable content', defined as 'content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy.'[155] Apple cites examples such as mean-spirited content; content that encourages violence or features realistic portrayals of people or animals being killed; overtly sexual or pornographic images; false information and features etc. Apple also imposes restrictions on apps with user-generated content or social networking services, requiring apps to include content filtering, user blocking and reporting mechanisms for objectionable content.

Importantly, the above content restrictions apply to all apps and Apple does not require additional content restrictions for apps in the Kids category. It is unclear whether Apple applies its 'objectionable content' standard differently based on context. The only instance in which Apple imposes additional content restrictions for users under 18 relates to prohibiting Apps that encourage minors to consume marijuana, tobacco, or controlled substances.[156]

Apple imposes restrictions on apps in the Kids Category, prohibiting advertisers from including links in the apps, purchasing opportunities or other 'distractions' unless behind a parental gate.[157] The inclusion of parental gates exceeds merely requiring parental consent, and instead requires the completion of an adult-level task.

Apple requires all apps, including apps in the Kids Category, to include a privacy policy. Apple also requires that apps in the Kids Category that collect, transmit or gave the capability to share personal information must comply with all applicable children's privacy legislation.

In addition, Apple generally places its own restrictions on the collection, use and disclosure of information relating to the Kids Category. Notably, Apple prohibits apps in the Kids Category from sending personally identifiable information or device information to third parties.[158]

Apple also prohibits third-party advertising and analytics in apps in the Kids Category, although this is subject to substantial exceptions.[159] While targeted advertising is always prohibited on apps in the Kids Category, contextual advertising may be permitted where apps have 'publicly documented practices and policies' for Kids category apps that include human review of advertising content. Apple permits third-party analytics in circumstances where children's personal information, and Apple's advertising identifier, IDFA, is not collected or transmitted.

---

[154] Ibid [2.3.8].
[155] Apple, 'App Store Review Guidelines – Apple Developer' (n 152).
[156] Ibid.
[157] Ibid, [1.3].
[158] Ibid.
[159] Ibid.

Other important restrictions relate to users under 13, in relation to whom Apple prohibits the use of facial recognition for account authorisation.[160]

Google

Google requires app developers to comply with its Developer Programme Policies.[161] In relation to apps which are designed for all ages including children, this policy is supplemented with Google Play Families Policy requirements.[162] For apps specifically designed for children, developers are required to comply with additional requirements outlined in Google's 'Designed for Families' program. In contrast to Apple, Google protections in Google's Families Policy and 'Designed for Families' program apply to children under 13.[163]

Google ensures that apps are appropriately characterised through its review process. This considers not only the designated audience indicated by the developer, but also the content, imagery and terminology of the app. For apps which, in substance, may be misleading, and could be considered as appealing to both children and adults, Google requires app developers to include a warning label stating that the app is not appropriate for children.

Google requires all apps on the Google Play Store to include a privacy policy which accurately describes the app's data collection, use and disclosure practices. Google also requires that apps comply with all applicable children's privacy legislation.[164] Additionally, Google imposes further restrictions on the collection, use and disclosure of data. In relation to apps which cater to all ages as well as apps which are designed specifically for children, Google requires developers to include an in-app disclosure explicitly informing users of the collection of any personal and sensitive information.

Google maintains general content restrictions outlined in its Developer Programme Policy, which prohibit a broad range inappropriate content such as child endangerment content, apps that appeal to children but contain adult themes, apps which promote negative body image, gambling etc. In addition to this, Google Play Families policy, which applies to apps designed for users of all ages, explicitly requires that app content be accessible and appropriate to children.[165] Google cites examples of violative content such as glamourising the use of controlled substances and violent and shocking content not appropriate for children and apps providing dating services or sexual or marital advice. Content on apps in Google's 'Designed for Families' program, which are designed for users under 13, are not subject to any further content restrictions than those outlined in the Google Play Families policy.

---

[160] Ibid [2.5.3].
[161] Google Play Console Help, *Developer Programme Policy (effective December 16, 2020)* <https://support.google.com/googleplay/android-developer/answer/10286120?>.
[162] Google Play Console Help, 'Designing Apps for Children', Web Page <https://support.google.com/googleplay/android-developer/answer/9893335?hl=en>.
[163] Google Play Console Help, 'Manage target audience and app content settings', Web Page <https://support.google.com/googleplay/android-developer/answer/9867159?>.
[164] Google Play Console Help, 'Developer Programme Policy', Web Page (2 October 2020) <https://support.google.com/googleplay/android-developer/answer/10286120?>.
[165] Google Play Console Help, 'Designing Apps for Children' (n 162).

In contrast to Apple, Google does generally allow for contextual advertising. However, similarly, targeted advertising is prohibited in apps which are designed for users of all ages and may include children. In addition to the restrictions outlined in Google's Developer Programme Policy, Google imposes advertising restrictions to apps designed for all ages in its Google Play Families policy, requiring that advertising content be appropriate for children. Additionally, in apps that target both children and older users, Google restricts the use of application programming interfaces (APIs) and software development kits (SDKs) to Google-Play certified options which are approved for child-directed services, unless the app can ensure that data from children is not collected, by including age screening measures.[166] In relation to apps that solely target children, developers are required to use Google Play certified APIs and SDKs.

Google imposes additional restrictions on apps, including imposing restrictions on the use of augmented reality for apps targeted at both children and older users.[167] Google imposes additional restrictions on apps targeted at children specifically, such as prohibiting the app from requesting location permissions, imposing further technical constraints, and requiring the reauthentication of all users prior to in-app purchases.

(vi) Parental controls

Parental controls are a way of managing children's and parents' consent. They provide a structured division between what the child can choose for themselves and what choices are reserved for the parent. Restriction on purchases, content and time spent are the common baseline for parental controls, but Google also allows parents control over children's privacy settings.

Parental controls are mandatory for digital platforms that allow users under 13, namely, Google and Facebook. While parental controls are available for minors of 13 years and above, the minor's consent is required. The types of parental controls offered differ depending on the nature of the platform, but commonly include usage controls; monitoring controls; content controls; and communication controls. Notably, Facebook, Instagram, YouTube, Snapchat and Twitter do not offer specific parental control tools. Therefore, parental controls do not seem to be a widely used mechanism in relation to users over 13.

Apple

Apple embraces the philosophy that parents are best placed to make decisions for their children, and thus parental controls are core to their 'Family Sharing' service offering.[168] While 'Family Sharing' is mandatory for users under 13, users older than 13 can consent to be added to a family group. Apple allows parents granular settings to limit their children's screen time through various usage control options: Parents can set a daily Screen Time limit and opt to exclude certain apps or features, set individual or combined app limits, after which

[166] Google Play Console Help, 'Developer Programme Policy' (n 164).
[167] Google Play Console Help, 'Designing Apps for Children' (n 162).
[168] Apple, 'You want to do what's best for your family. So do we.', Web Page <https://www.apple.com/au/families/>.

a child's access is either blocked or restricted.[169] Using App Limits, parent accounts have two options for setting the amount of time a child can spend on their device: a parent can either opt to set a time limit on individually selected app categories (such as Games, Entertainment and Social Networking), apps and websites, or can set a time limit on all apps and categories and select exclusions that are always allowed. Additionally, Apple's Down Time feature allows parents to select a time frame, such as bedtime, in which app use and notifications are blocked entirely. Parents can select individual apps and enable communication with specified contacts that are always allowed.

Apple offers various content restrictions for parents across the Apple ecosystem. Apple allows parents to filter website content on Safari and on a device's apps by allowing unrestricted access, limit adult websites or enable children to access allowed websites only. Parents can add specific websites to an approved or blocked list.[170] Parents can also restrict Siri web search and prevent Siri from displaying explicit language. Additionally, in relation to App Store content, parents have the option to select a country or region in the ratings section to automatically apply the appropriate content ratings for that region. Parents can also prevent apps, books, TV shows, films with specific ratings; prevent music, podcast and news containing explicit content and prevent finding and viewing music videos or friend's music profiles.

Apple offers additional parental controls such as 'Ask to Buy', which is enabled by default for users under 13.

Google

Google offers parental controls through Family Link. Family Link enables parental supervision and account management for parents of children under 13 and can be configured for older children at their discretion. The main usage controls offered in Family Link enable parents to set time limits to manage and monitor a child's screen time.[171] This includes the option of setting and monitoring daily screen time limit based on activity for a Google device or for individual apps. Parents can also set a time frame in which device activity is blocked by using the 'bedtime' feature and opt to remotely lock and unlock their child's device at any time.

In addition to limiting the time spent on devices or certain apps, Family Link includes controls that allow parents to limit the content available to their child. These controls span the Google ecosystem, and include managing websites accessible to children on Chrome, filtering explicit content through Google SafeSearch and filtering apps, games and media discoverable by children on Google Play according to content ratings.[172] On Google Play, Google offers additional content controls for parents by configuring approvals and purchasing approvals for downloading all content, paid content or content including in-app

---

[169] Apple Support, 'Use parental controls on your child's iPhone, iPad, and iPod touch', Web Page, <https://support.apple.com/en-us/HT201304>.
[170] Ibid.
[171] Google Support, 'Manage your child's screen time', Web Page <https://support.google.com/families/answer/7103340?hl=en>.
[172] Google Support, 'Set up parental controls on Google Play', Web Page <https://support.google.com/families/answer/1075738?hl=en>.

purchases.[173] Google also grants parents control over general settings, as well as settings relating to the management their children's app and website sharing permissions such as location, microphone and camera access. Using Family Link, parents can restrict access to mature content on YouTube by enabling restricted mode for a teen's account.

YouTube Kids

Except through Google FamilyLink, YouTube does not offer parental control mechanisms in the strict sense and requires users to be over the age of 13. However, parental controls are central to YouTube's service offering for children under 13, YouTube Kids. YouTube Kids enables parents to limit a child's screen time within the platform by setting a timer, once the set time has elapsed, access to YouTube Kids is blocked. Content controls are integrated into the onboarding flow for parents. A parent decides upon an age-based content setting which then informs a child's viewing experience.[174] Parents have additional content control options such as opting to limit the content viewable to their child to 'approved content' subject to manual review, turning off search for their children and blocking certain videos and channels from their child's viewing experience.[175]

Messenger Kids

Similarly, Facebook and Instagram do not offer parental controls. Facebook requires its users to be over the age of 13 and grants its users full control over their account.[176] However, Facebook's offering for users under the age of 13, Messenger Kids, allows parents to exercise control over a child's experience through multiple features.[177] Firstly, in-app usage control is enabled through 'Sleep Mode' which allows parents to set days and times in which their child can use Messenger Kids. Parents can also choose to remotely log out of the app on any device. Various activity monitoring controls are also accessible to parents, including access to contacts, reported and blocked contacts, chat history and a log of images sent in chat. Parents are also given control over children's communications. 'Friending Controls' allow parents to restrict children's ability to add new contacts. Parents are notified when a child receives or declines a friend request and can override a child's friending action by adding and removing contacts.

TikTok

While TikTok is targeted at users over 13, TikTok aims to provide parents with insight and control into how teens use the app through their 'Family Pairing' feature. TikTok's parental controls require teens to first agree to link accounts with their parents.[178] Parents then have access to a variety of controls, including usage controls such as screen time management

---

[173] Google Support, 'Purchase approvals on Google Play', Web Page <https://support.google.com/googleplay/answer/7039872?>
[174] ICT Coalition for Children Online, *ICT Principle Implementation Report (April 2019).*
[175] Google Support, 'Parental controls and settings', Web Page <https://support.google.com/youtubekids/answer/6172308?hl=en>.
[176] ICT Coalition for Children Online*ICT Principle Implementation Report (April 2019).*
[177] Morgan Brown (n 147).
[178] Jacob Kastrenakes, 'TikTok now lets parents set restrictions on their kids' accounts', *The Verge* (16 April 2020) <https://www.theverge.com/2020/4/16/21222817/tiktok-family-pairing-linked-accounts>.

which enables parents to set a time limit between 40 and 120 minutes, content controls such as restricted mode to limit inappropriate content and restricting search and communication controls such as turning off or limiting direct messages to friends.

(vii) **Design and functionality changes**

In order to ensure the highest level of protection, digital platforms which offer services to wide audiences disable certain features, which can render them completely inaccessible to children. Commonly, restrictions are imposed on features that enable the public sharing of children's data with other users or on the internet more broadly or certain types of sensitive data. Additional features are also added to children's accounts, including filtering and reminders.

Apple

On Apple, children can take advantage of most Apple features and services.[179] However, certain sharing features are unavailable such as 'Allow Apps to Ask to Track'. Additionally, features that allow users to disclose personally identifiable information on Apple's online gaming service, game centre, re unavailable. Namely, children cannot send or receive user-inputted text or voice messages and are restricted to sending and receiving present messages and emojis.[180]

Google

Google offers protection for children signed into Family Link through making certain services unavailable to children as well as limiting functionality of features within services. Google limits the ability for children under 13 to access certain apps. Children also do not have access to apps and extensions in the Chrome Web Store.[181] Google Play also imposes limitations on children's ability to download and use apps.[182] Namely, Google's 'Play Games' apps are unavailable to children. While Google Play Music is available to children, features such as free radio and free podcasts are disabled.

Additionally, features that enable the sharing of content is limited. Most importantly, real-time location sharing on Maps is limited to sharing with parents. Children are also unable to post public reviews or ratings on Maps. Google limits sharing on other apps such as Gmail by disabling features such as automatic forwarding and mail delegation.[183] Additionally, children are restricted from sharing content on Google Play by restricting their ability to create public playlists and share their playlists.

---

[179] Apple, 'Family Privacy Disclosure for Children' Web Page <https://www.apple.com/legal/privacy/en-ww/parent-disclosure/>.
[180] Apple, 'Game Center & Privacy', Web Page <https://support.apple.com/en-us/HT210669>.
[181] 'Google Support, 'Chrome & your child's Google Account', Web Page <https://support.google.com/families/answer/7087030?>.
[182] Google Support, 'Google Play & your child's Google Account', Web Page <https://support.google.com/families/answer/7106960?>.
[183] Ibid.

Personalisation options are also limited for children, including personalised recommendations for eBooks and podcasts, and recommendations on maps based on visited places.[184]

While children can access Chrome, Google's Incognito mode filter, which prevents browsing history being stored, is unavailable.[185] This limits a child's ability to browse anonymously or conceal their search history, which are able to be accessed by parents.

YouTube and YouTube Kids

On YouTube, features are restricted both in relation to 'Made for Kids' content and content featuring minors. Namely, to comply with COPPA, 'Made for Kids' content disables features such as comments, notifications, auto play, live chat and channel memberships. YouTube has stated that these restrictions apply in order to limit the collection of data from children.[186] In addition, YouTube disables multiple features on both the channel and video level for content featuring minors, including comments, live chat, live streaming, video recommendations and community posts as content risks attracting predatory behaviour.[187]

Facebook

On Facebook, certain features such as facial recognition is not made available to under 18s. Added protection measures are introduced in relation to children, such as the filtering from a minor's inbox of messages sent from adults who are not friends (or friends of friends). Additional messaging accompanies children's accounts, such as reminders, tutorials and other in-line messaging accompanying setting changes to less privacy-restrictive settings.

TikTok

In addition to their existing controls and measures for messaging all users, TikTok has disabled its direct messaging feature for children under 16 as a preventative measure against inappropriate content.[188]

(viii) **Use of defaults**

In some very limited circumstances, platforms do set stricter, privacy-preserving defaults for children. However, there is also evidence that Facebook, Google and Microsoft deliberately employ privacy intrusive default settings, many of which were obscured or difficult to find and change.[189]

---

[184] Ibid.
[185] Ibid.
[186] 'Set your channel or video's audience', Google Support , Web page <https://support.google.com/youtube/answer/9527654?co=GENIE.Platform%3DAndroid&hl=en>.
[187] Google Support, 'Update on our actions related to the safety of minors on YouTube', Web Page (28 February 2019) <https://support.google.com/youtube/thread/1805616>.
[188] TikTok Newsroom, 'TikTok introduces Family Pairing', Blog (16 April 2020) <https://newsroom.tiktok.com/en-us/tiktok-introduces-family-pairing>.
[189] Forbrukerådet [Norwegian Consumer Council], *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (2018)

Apple

Apple's parental control 'Ask to Buy' is turned on by default.[190]

Google

Google enables its explicit content filter, 'SafeSearch', by default for users under 13. This approach is notably different to YouTube. YouTube does not allow users under 13 and their mature content filter, 'Restricted Mode', must be turned on by parents or teens and is not enabled by default.[191]

Facebook

Facebook provides stricter default settings for teens, particularly in relation to sharing and communication.[192] Namely, information provided by teens such as their email and phone number will not be set to 'public' to limit public search records. To reduce visibility, content sharing settings for minors are set to 'friends' and their default audience options do not include 'public'.[193] When sharing publicly, Facebook requires minors to enable the option from their settings, which is accompanied by an in-line privacy reminder. Additionally, Facebook provides teens with greater control over tagged posts, by turning on the 'Tag Review' tool by default.

To protect minors, Facebook also sets the default audience age which advertisers can target users to18.[194]

Snapchat

Snapchat, and in particular Snap Maps, sets location sharing to 'off' by default for all users, even when users have already granted Snapchat location permissions for another location-based feature.

Twitter

On Twitter, tweet geolocation is turned off by default. [195]

<https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> ('Deceived by Design').

[190] Apple, 'Approve what kids buy with Ask to Buy', Web Page <https://support.apple.com/en-au/HT201089>.

[191] Google Support, 'YouTube Kids, YouTube & your child's Google Account', Web Page <https://support.google.com/youtubekids/answer/7124142?hl=en>.

[192] Facebook, ICO *Age Appropriate Design Code: Consultation (*n 84).

[193] Erin Egan and Ashlie Beringer, 'Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live', *Facebook Newsroom* (17 April 2020) <https://about.fb.com/news/2018/04/new-privacy-protections/>.

[194] Facebook, ICO *Age-Appropriate Design Code: Consultation* (n 84).

[195] UK Council for Child Internet Safety-*Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services* (1 March 2016). <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guidefinal__3_.pdfKCISS>

(ix) **Conclusions**

Platforms are directing significant resources towards user safety, content moderation, and the maintenance of community and advertising standards. This includes investment in human review processes as well as new technologies (including artificial intelligence and machine learning) for automatic flagging of inappropriate content.

Unfortunately, platforms have not been similarly incentivised to develop effective measures to recognise which of their users are children. Most platforms do apply age screening to bar users under the age of 13, but overwhelmingly rely solely on the user self-asserting their age.[196] This has two perverse results. First, children are incentivised to lie in order to bypass restrictions, often with the support of their parents — 34% of parents of 10-13 year-olds report that their child has their own social media account, not including kids' versions of online service such as YouTube Kids or Facebook Messenger Kids. Second, measures aimed at keeping children safe or at limiting the collection, use and disclosure of their personal information are mis-calibrated or not applied at all for children who have lied about their age. As there is no clear industry standard for age verification at present, we do not recommend prescribing a particular approach, however it is important that the Code properly incentivises platforms to pursue an appropriate level of assurance as to their users' age.[197]

Advertising standards provide some limited restrictions on the use of children's personal information for personalised advertising, though these often focus on advertising content and policies and threshold ages vary. Only Apple extends protections to children older than 13. Most platforms also have measures in place to restrict the sharing of children's personal information with advertisers, or to restrict direct collection of children's personal information through their platform by third parties. There is a significant gap between the preferences of parents and industry practice here, with 83% of parents opposing profiling and targeted advertising for children, and 81% believe that businesses should only collect the minimum amount of data needed to provide the service. Possible restrictions on data sharing, profiling and targeted advertising are discussed further in response to question 2f.

With limited exceptions, default settings are not protective of privacy. This too is substantially at odds with the expectations of Australian parents (84% in favour of high privacy defaults) and is discussed further below.

[196] This is an unintended consequence of the US Children's Online Privacy Protection Act (COPPA), which is discussed in response to question 2a below.
[197] The issue of age assurance is further explored in section 2b (vii) below.

Question 2 — What additional protections/requirements could be put in place to mitigate the risks and potential harms faced by children online?

Question 2a — How have international jurisdictions and data protection authorities addressed privacy risks and harms faced by children online?

Key findings:

There is an international trend towards implementing additional privacy protections for children. The USA, the EU and the UK are the most advanced in developing and implementing these protections.

In the US, the Children's Online Privacy Protection Act 1998 imposes requirements to provide notice to parents of children under the age of 13, and to obtain verifiable parental consent, before personal information from these children can be collected, used or disclosed. These measures are now supplemented in California by the Consumer Privacy Act, which also contains special protections for children. The General Data Protection Regulation (GDPR) in the EU has built on, and expanded, these protections, including by imposing stricter requirements on the use of children's personal data for the purposes of marketing or profiling, and by creating a right to erasure. On the basis of the GDPR, the UK Information Commissioner's Office has developed a path-breaking Age Appropriate Design Code that is centred on the principle that the best interests of the child should be the primary consideration when designing and developing apps, games, connected toys/devices and websites that are likely to be accessed by children.

While the Californian Consumer Privacy Act, the GDPR and the UK 'Age Appropriate Design Code' currently provide some of the most substantial and forward-thinking protections, children are also given enhanced protections in the data privacy laws of Canada, China, India and South Korea.

The protection of children in the digital environment is becoming of increasing concern around the world, with a number of multilateral organisations more specifically considering how children's privacy can be safeguarded.[198] To date most countries are still formulating

[198] The Committee on the Rights of the Child is currently drafting a general comment on children's rights in relation to the digital environment: the draft General Comment is available at: <https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx>. The UN Special Rapporteur on the right to privacy is currently preparing a report on Privacy and Children to the Human Rights Council, to be submitted in March 2021: <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx>.

their approaches.[199] This section has the purpose of highlighting the key international developments that have already taken place, or are under active consideration, to provide a better context for the law reform process in Australia. The leading jurisdictions in this field are the US and the European Union; these will be explored first and in most detail. Other developments in Canada, China, India and Brazil are covered briefly.

(i) The protection framework in the USA

The United States lacks a general data protection statute. Instead, regulation at the federal level focuses on specific sectors and aspects of information handling that are regarded as warranting special regulation. One such area is children's online privacy, which is regulated at the federal level by the Children's Online Privacy Protection Act (COPPA).[200] The protection of children's privacy is supplemented in California by the Californian Consumer Privacy Act (CCPA).[201] There is also a dedicated federal statute that applies to children's education records, but that is beyond the scope of this report.[202]

The Children's Online Privacy Protection Act

The COPPA requires the US Federal Trade Commission (FTC) (which currently operates as the key privacy regulator in the US) to promulgate regulations on the collection of children's personal information by operators of commercial websites, online services and mobile apps. The relevant regulations, known as the 'COPPA rule',[203] require compliance with specified practices in the collection, use and/or disclosure of personal information on the internet from and about children.[204]

The COPPA rule applies to (i) commercial websites, online services, and mobile apps 'directed to children' under the age of 13;[205] and (ii) operators of general-audience commercial websites that have 'actual knowledge' that they are collecting personal information from children under thirteen.[206] Entities subject to the COPPA rule must first post

---

[199] See further on the international developments: Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10(1) *European Journal of Law and Technology* 1.
[200] *1998,* 15 US Code §§ 6501–6506.
[201] The California Consumer Privacy Act of 2018, contained in California Civil Code §§1798.100 to 1798.198.
[202] The Family Educational Rights and Privacy Act of 1974 protects such records from unauthorised disclosure and generally requires written consent by parents (and eligible students) before they can be shared. It also gives parents the right to access and seek to amend their children's education records.
[203] On the history of the COPPA rule, see Chris J Hoofnagle, *Federal Trade Commission: Privacy Law and Policy* (Cambridge University Press, 2016), 197–199; Better Business Bureau, National Programs, *Twenty Years of Successful Co-Regulation under COPPA*, Report (October 2019).
[204] 16 C.F.R. §312.3.
[205] The Federal Trade Commission considers a 'variety of factors' to determine whether a site is directed at children, including the subject-matter of the site or service, its visual and audio content and other evidence about the age of its actual or intended design audience: Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, Web page <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>.
[206] 16 C.F.R. §312.2. The rule also applies to parties running a third-party service (like an ad network or plug-in) that collects information directly from users of a site or service directed to children under

a clear and comprehensive online privacy policy and make 'reasonable efforts (taking into consideration available technology)'[207] to ensure that parents receive notice of the website's or online service's collection, use, and disclosure of their child's personal information. Second, the entity must generally obtain 'verifiable parental consent' before any personal information relating to a child is collected, used or disclosed and each time there is 'any material change' in its data handling practices.

Verifiable consent means that the consent mechanism must be 'reasonably calculated, in light of available technology'[208] to ensure that the consent is being given by a child's parent.

The FTC provides further guidance about acceptable methods for obtaining parental consent via a list of FAQs relating the COPPA rule.[209] This states that methods identified in the COPPA rule or otherwise approved by the Commission include:

- providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan (the 'print-and-send' method)
- requiring the parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder.
- having the parent call a toll-free telephone number staffed by trained personnel, or have the parent connect to trained personnel via video-conference
- verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that you promptly delete the parent's identification after completing the verification
- requiring a parent to answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer
- verifying a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.[210]

In the case of the last two methods it is necessary to apply to the FTC for specific approval of the method uses in accordance with the procedure set out in the COPPA rule.[211]

The FTC also permits use of the 'email plus' method of parental consent where children's personal information is used only for internal purposes. This allows businesses to request (in the direct notice sent to the parent's online contact address) that the parent indicate consent in a return message.

13: Federal Trade Commission, *Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, Web page <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites>.

[207] 16 C.F.R. §312.4(b).

[208] 16 C.F.R. §312.5(b)(1).

[209] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, Web page <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>.

[210] Ibid, I.4.

[211] See 16 C.F.R. § 312.12(a). The Federal Trade Commission maintains a website on *Verifiable Parental Consent and the Children's Online Privacy Rule*, Web page <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule>, which contains details of applications that have been approved and also ones that have been denied.

The Guidance clarifies that:

> To properly use the email plus method, you must take an additional confirming step after receiving the parent's message (this is the "plus" factor). The confirming step may be:
>
> - requesting in your initial message to the parent that the parent include a phone or fax number or mailing address in the reply message, so that you can follow up with a confirming phone call, fax or letter to the parent, or
> - after a reasonable time delay, sending another message via the parent's online contact information to confirm consent. Information contained in the direct notice must inform the parent that he or she can revoke the consent, and inform the parent how to do so.[212]

The COPPA rule also contains a right for parents to review personal information provided by a child,[213] to object to the further use or future online collection of their child's personal information and to direct the operator to delete personal information that has been collected so far.[214] Furthermore, the operator must maintain reasonable procedures to protect the confidentiality, security, and integrity of information they collect from children, including when it is disclosed to third parties,[215] and retain personal information collected online from a child for no longer than necessary to fulfil the collection purpose. Finally, operators must not make it a condition for 'a child's participation in a game, the offering of a prize, or another activity' that the child discloses 'more personal information than is reasonably necessary to participate in such activity'.[216] Violations of the COPPA rule are treated as an unfair or deceptive act or practice under the Federal Trade Commission Act, thereby triggering its enforcement mechanisms.[217]

The COPPA rule has had the effect of protecting younger children from some practices of data collection and digitalised advertising that are in play in the case of teens and adults.[218] However, it has been criticised for 'how it balances parental versus website responsibility',[219] in particular that it goes too far in protecting the interests of operators of online services. The most serious weakness of the COPPA regime is that it applies only to children under 13. While the FTC encourages operators also to adopt age-appropriate protocols for personal information collected from teenagers aged 13 and over,[220] the COPPA imposes no statutory requirement for them to do so. There is also no incentive for operators of general audience websites to verify a user's age. On the contrary, the 'actual knowledge' requirement has the consequence that failing to collect information that establishes that a user is under 13 obviates the need to comply with the COPPA rule.

---

[212] Ibid.
[213] 16 C.F.R. §312.6.
[214] Ibid16 C.F.R. §312.6 (a)(2).
[215] 16 C.F.R. §312.8.
[216] 16 C.F.R. §312.7.
[217] 16 C.F.R. §312.9.
[218] Kathryn C Montgomery and Jeff Chester, 'Data Protection for Youth in the Digital Age' (2015) 1 *European Data Protection Law Review* 277.
[219] Cf. Hoofnagle (n 203), 208.
[220] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), 29, 60.

In the past, social media platforms had little incentive to strengthen their age verification procedures. However, as a result of the spotlight shone on Facebook after the Cambridge Analytica revelations,[221] the social media conglomerate appears to have adopted a somewhat more pro-active approach to enforcing its age limits. While still not requiring proof of age upon signup, Facebook and its sister site Instagram have reportedly changed their internal review policies to suspend the accounts of users they identify as being under 13 years of age.[222]

Recent actions by the FTC suggest that it is now treating the protection of children's privacy as an issue of increasing concern. This was illustrated by its action against the operators of the video social networking app, Musical.ly (now known as TikTok), who reached a settlement in 2019 to pay US$5.7 million to settle allegations that it illegally collected personal information from children.[223] The FTC had alleged that the company knew that a significant percentage of TikTok users were younger than 13, and failed to notify parents or obtain parental consent, or to delete children's data on their parents' request.[224] In addition to agreeing to make the payment, the operators agreed to comply with COPPA going forward and to remove all videos made by children under the age of 13.[225] Also in 2019, Google agreed to pay record penalties totalling US$170 million and to review its data collection practices to settle allegations by the FTC and the New York Attorney General that its subsidiary, YouTube, illegally collected personal information from children without their parents' consent. Under the settlement, Google committed to developing a system for third-party content creators to self-designate child-directed content and to take specific measures to ensure its compliance with COPPA, if they collect personal information from viewers of that content. While the FTC heralded this record settlement amount as a 'game changer',[226] two Commissioners and consumer advocates decried it as too low in light of the size of Google and the profits it makes from commercialising children's personal data.[227]

---

[221] See Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', *The Guardian* (18 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

[222] Josh Constine, 'Facebook and Instagram change to crack down on underage children', *TechCrunch* (20 July 2018) <https://techcrunch.com/2018/07/19/facebok-under-13/>.

[223] FTC, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law Press Release*, Press Release (27 Feb 2019) <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc>.

[224] Mitchell Noordyke, 'FTC issues its largest-ever COPPA fine', *APP News* (28 Feb 2019) <https://iapp.org/news/a/ftc-issues-its-largest-ever-coppa-fine/>.

[225] Christine Wilson, The Future of the COPPA Rule: An FTC Workshop Part 1: Oct 7, 2019, Transcript, <https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf> 4.

[226] Angelique Carson, 'FTC touts historic YouTube settlement as 'game changer' for COPPA enforcement', *iAPP News* (4 Sept 2019) <https://iapp.org/news/a/ftc-touts-historic-youtube-settlement-as-game-changer-for-coppa-enforcement/>.

[227] Allen St. John, 'Google Settles Claims YouTube Violated Children's Privacy', *Consumer Reports* (4 Sept 2019) <https://www.consumerreports.org/privacy/google-settles-claims-youtube-violated-childrens-privacy/>.

Against the background of these enforcement proceedings, the FTC announced a review of the COPPA rule.[228] As part the review process it held a public workshop in October 2019 that examined how well the COPPA rule was working and which aspects of it required improvement. The review is timely given the need to respond to a rapidly evolving digital marketplace that is increasingly shaped by new technologies, such as Big Data, the internet of Things and Artificial Intelligence. These developments include new technological applications (such as internet-connected toys; increased tracking across devices) that have spawned new business opportunities and marketing practices in respect of children.

Federal law reform proposals

In addition to the ongoing review process led by the FTC, there is also a raft of law-making proposals before US Congress that seek to strengthen privacy protections for young people. These include:

- A Senate bill for a COPPA 2.0, introduced in March 2019.[229] Measures contained in the Bill include a ban on the use of targeted advertising to users under 13, expanding the scope of COPPA to include users aged 13 to 15 ('minors'), a requirement that internet-connected devices and toys directed toward children meet certain cybersecurity standards and include a privacy policy on their packaging, and a requirement that services offer an 'eraser button' to permit minors at any time to eliminate their personal information submitted online. COPPA 2.0 would also create a 'Digital Marketing Bill of Rights for Minors' and a Youth Privacy and Marketing Division at the FTC.
- A House Bill for a PROTECT Kids Act, introduced in January 2020.[230] The Bill extends existing COPPA consent requirements to all users under age 16, extends the definition of personal information to include 'precise geolocation information' and 'biometric information', strengthens non-discrimination protections in cases where parents demand the deletion of personal information about their child, and directs the FTC to conduct research and make recommendations on the 'actual knowledge' standard found in COPPA.
- A House Bill for Protecting the Information of our Vulnerable Children and Youth Act (PRIVCY), also introduced in January 2020.[231] The Bill imposes new data processing obligations on companies that have actual or constructive knowledge that they are collecting information from children or young consumers (individuals between the ages of 13 and 18 years), including rights to access, correct or delete processed

---

[228] Ibid.
[229] The COPPA 2.0 Bill (S.748 – 116th Congress (2019-2020)), introduced by Senators Edward J Markey (D-Mass.) and Josh Hawley (R-Mo.), is available at <https://www.congress.gov/bill/116th-congress/senate-bill/748/text>.
[230] The PROTECT Kids Bill (S.5573 – 116th Congress (2019-2020)), introduced by Representatives Bobby Rush (D-Ill.) and Timothy Walberg (R-Mich.) is available at <https://www.congress.gov/bill/116th-congress/house-bill/5573/text>.
[231] The PRIVCY Bill (H.R.5703 – 116th Congress (2019-2020)) introduced by Representative Kathy Castor (D-Fl.), is available at <https://www.congress.gov/bill/116th-congress/house-bill/5703/text>.

information, a prohibition on targeted marketing, increased enforcement powers for the FTC and a private right of action for data misuse.

While it is uncertain whether any of these bills, in their current or an amended form, will become law, they demonstrate the increasing unease of US lawmakers with the current state of children's privacy protections, including the exclusion of children aged 13 and over from the scope of COPPA. They also indicate a desire to expand the definition of personal information and to strengthen existing data processing standards, including via bans on targeted marketing, improved rights to access, correction and deletion and greater enforcement of the applicable privacy laws.

Differences between the proposals concern who can make privacy decisions for young people between the ages of 13 and 15. COPPA 2.0 would significantly expand the protection of minors under 13 years of age, but maintain the position that minors above that age can make their own privacy choices. The PROTECT Kids Act would raise the age of digital consent to the age of 16, but otherwise largely maintain the existing privacy standards. Finally, the PRIVCY Act would go furthest in improving children's privacy protecting by both expanding the protections to all young people under the age of 18 years and creating a range of new rights and protections.

The California Consumer Privacy Act

The CCPA is a state-based general data protection law that regulates the handling of the 'personal information' of Californian residents by businesses. It has a broader scope of application than COPPA because it also applies to data collection through in-person interactions and during phone calls. However, it also contains specific provisions relating to children, including restrictions on the collection and handling of children's information that are 'intended to supplement' the COPPA.[232] The CCPA states that a business must not 'sell' a child's personal information without consent if it has actual knowledge that the consumer is less than 16 years of age. In the case of consumers between 13 and 16 years of age, it must be the teenager who has affirmatively authorised the sale of their personal information; in the case of consumers who are less than 13 years of age, that decision rests with the child's parent or guardian.[233] 'Sell' is defined broadly, meaning any disclosure to a third party for valuable consideration.[234] This means that, in the case of children under 16 years of age, a sale is only permissible following an affirmative opt in, whereas young consumers above that age are treated in the same way as adults and provided with a 'right to opt out' of the sale.

A significant feature of the CCPA that is currently absent from the COPPA is that it deems a business that wilfully disregards the consumer's age to have actual knowledge of it.[235] While the requirement of affirmative authorisation is confined to the 'sale' of information, the CCPA requirement for businesses to ascertain a young user's age so that they can determine their obligations in relation to the sale of that information can trigger the collection limitation in the COPPA if the user is established to be under the age of 13.

---

[232] California Civil Code §1798.196.
[233] California Civil Code §1798.120(c).
[234] California Civil Code §1798.140.
[235] California Civil Code §1798.120(c).

Another important feature of the CCPA, which is not specifically focussed on children but is beneficial for them, is a qualified right to request deletion of data. This permits a consumer to request a business or service provider to delete personal information collected by the business from the consumer if it is no longer necessary for the business or service provider to maintain that information for one of more specified purposes.[236] Allowing individuals to demand the destruction of personal information once it is no longer required is especially important in relation to children who may have volunteered their information without fully understanding the full implications of doing so.

(ii) The protection framework in the European Union

Since the enactment of the General Data Protection Regulation (GDPR),[237] data protection laws across the European Union are largely uniform. The , Web page which is directly applicable in each Member State of the EU,[238] is acknowledged to have raised the bar for data protection laws. Its provisions have therefore also become highly influential internationally.

Substantive protections in the GDPR

The GDPR refers specifically to children in a number of its articles and recitals, but it does not define the term 'child'.[239] In the line with the UN Convention on the Rights of the Child (UNCRC), it is understood as referring to a child under the age of 18. The articles set out the binding legal requirements that must be followed, while the recitals are intended to assist with the construction of the instrument and therefore serve a function that is similar to the explanatory memorandum in an Australian statute.

In principle, data protection rights under the GDPR apply to children and adults alike. However, the GDPR contains a specific provision on the exercise of children's data privacy rights, and a number of further provisions giving children special protections. Recital 38 explains that children merit specific protection of their personal data, as they be less aware of the risks, consequences and safeguards concerned, and of their rights in relation to the processing of personal data. It also emphasises that this protection should apply, in particular, in three situations:

- the use of children's personal data for the purposes of marketing
- the use of children's personal data for the purposes of profiling them,[240] and

---

[236] California Civil Code §1798.105(a).
[237] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1 ('GDPR').
[238] While the GDPR operates, as directly applicable law, throughout the EU, member states can adopt domestic legislation to support and supplement the GDPR to the extent where the GDPR requires or allows such member state legislation.
[239] The first draft of the GDPR released by the European Commission in 2012 defined a child as 'any person below the age of 18 years'. But this definition was subsequently removed.
[240] The issue of profiling is also dealt with in recital 71, which states that profiling measures should not apply to a child.

- the collection of children's personal data when they are using services offered directly to a child.[241]

The GDPR contains four key operative provisions that provide enhanced protection for children. These are article 8, which regulates when a child can consent to data processing in the context of the provision of online services by entities such as online marketers, apps and online content providers; article 12, which deals with transparency requirements; article 15, which deals with data access rights; and article 17 concerning the right to erasure.

Article 8, also described as providing for the 'age to digital consent', lays down the age at which children are free to exercise their own data privacy rights. It addresses the issue of capacity in the specific context of 'information society services',[242] which includes social media platforms, search engines, websites, mobile apps, messaging services and electronic games. Only information society services offered 'directly to the child' are caught by article 8. While this term is not defined, it is clear that Art. 8 applies to services that are 'specifically intended to be offered to children',[243] because they are meant for children or include children as part of their target audience. Factors indicating such an intention can be a child-friendly design and a wording clearly directed at children.[244] Conversely, article 8 does not apply to services that are available only to adults, such as services that have effective age restrictions to exclude users of under 18 years of age. This applies even when a service may be of benefit for a child (such as tuition website).

The position is less clear concerning dual use services that are accessible to adults and children alike. Arguably the better view is that general audience websites fall under article 8 if they are also regularly used by children.[245] Some service providers purport to impose age restrictions through their terms and conditions, for example by providing information that their service are only to be used by adults. Others rely on technical measures (so-called age gating) to prevent children from using their service. The European Data Protection Board, an EU advisory body on data protection, provides the following guidance on when information society services are 'offered directly to a child':

> [I]f an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by

---

[241] The other relevant recitals are recital 58 and 75. Recital 75 lists risks to the rights and freedoms of natural persons that may result from personal data processing and lead to physical, material or non-material damage. That list specifically refers to the 'processing of personal data of vulnerable natural persons, in particular of children'.

[242] According to GDPR art 4 No. 25, an 'information society services' is defined as in Directive (EU) No 2015/1535 art 1 para 1 lit. b, i.e. 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.

[243] Centre for Information Policy Leadership, GDPR Implementation In Respect of Children's Data and Consent (6 March 2018) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf> 9.

[244] Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses' (2017) 18(1) *Computer und Recht International* 6, 8.

[245] Eva Lievens and Valerie Verdoodt, 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation' (2018) 34 *Computer Law and Security Review* 272.

other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.[246]

Article 8 specifies a cut off age of 16 for valid consent by a child; this can be varied to a minimum of 13 years by individual member states. This statutory compromise resulted from an inability to find common ground during the legislative process, but the flexibility has now led to a bewildering lack of uniformity across the 27 jurisdictions.[247] Whereas some Member States (such as Germany and Ireland) chose not to derogate from the age of 16 years, the majority adopted 13, 14 or 15 years as the relevant age. Where a child is younger than 16 (or such lower age as is specified by a member country), consent is valid only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child.

It is important to note that consent is only one of the available bases for lawful data processing. Ground (f) of article 6(1) permits processing on the basis that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child. The specific reference to children in this context draws attention to the fact that children have special interests and fundamental rights and freedoms that warrant particular attention. As a general rule, this makes it more difficult for data processing to be justified otherwise than on the basis of consent where the data subject is a child rather than an adult.

Article 12 regulates the transparency of the communications required in other parts of the GDPR, including privacy notices. Under this provision, controllers must provide the information required in privacy notices 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'. The specific reference to children is important because privacy notices play an important role in ensuring the informed exercise of consent and other rights under the Regulation, and this draws attention to the fact that children may require simpler language in notifications. This is reinforced in Recital 58 which emphasises that 'any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.

Article 15, dealing with access rights, gives rise to a number of difficult issues concerning the respective rights of parents and children. These include the question of the age at which a child should be able to make an access request, and, conversely, whether there should be an upper age limit, after which parents should no longer be able to make such requests. These questions are not addressed in the GDPR, and their resolution requires striking a

[246] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679 (GDPR)* (May 2020) [130].

[247] In its first review of the operation of the GDPR, the European Commission has identified the variation in age limits as problematic and considers their possible harmonisation: Communication from the Commission to the European Parliament and the Council, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, 7 and 15.

balance between a parent's right to protect the best interests of their child and the child's right to privacy in relation to access requests for the child's personal data.[248]

The GDPR contains a right to erasure in article 17. This enables individuals to request the erasure of their personal data in specified circumstances, including where that processing has been grounded on consent and they wish to withdraw that consent. Significantly, recital 65 emphasises that this:

> right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

The right to erasure has been touted as providing a person with a legal means to request the removal of embarrassing social media posts. However, this right, like most other data rights, is not absolute. Apart from the practical difficulties of removing data from a social networking site that may have already been shared in the meantime by others, the right depends on the existence of a specified ground and is subject to a number exceptions, including considerations of free speech and public policy.[249]

The emphasis on protecting children's privacy is further reinforced by the requirement in article 57 for the supervisory authorities that provide oversight over data protection in individual member states to give specific attention to public awareness activities addressed specifically to children. The European Data Protection Board (EDPB), which is tasked with ensuring that the GDPR is applied consistently across the EU, has announced the preparation of guidelines on children's data,[250] but this work is still ongoing.

Finally, article 40 requires member states and supervisory authorities to encourage the drawing up of codes of conduct to contribute to the proper application of the provisions in the GDPR. The matters listed in article 40 as examples of what might be regulated under these codes include specific reference to children:

> (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained.

Identified weaknesses of the GDPR protections

While the child-focused protections have appropriately recognised the particular vulnerability of children in data processing and lifted the profile of children's rights in this context, the protection of children's privacy remains a work in progress within the EU. The EU is currently engaged in the first periodic review of the GDPR. As part of this process, the Multistakeholder Expert Group, which is tasked with assisting and advising the Commission

---

[248] Data Protection Commission Ireland, *Public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation*, Consultation Paper (2018), 12.
[249] See Bunn (n 52).
[250] European Data Protection Board, Work Program 2019/2020 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf> 2.

on the application of the GDPR, identified 'difficulties in the application of GDPR as it concerns children and requirements for parental consent'.[251] In particular, the Expert Group mentioned reporting by civil society organisations that:

> a number of controllers do not properly address the fact that children are among the data subjects of which they process the data. They argue that the existing fragmentation of legislation on the age for children['s] consent, inappropriate practices and the lack of enforcement impact the data protection rights of children, with negative effects also for their other fundamental rights and freedoms.[252]

It is therefore to be expected that efforts to harmonise the age of digital consent across the EU will remain on the political agenda. Further work will also need to be undertaken, at EU and member state level, to provide guidance to data processors on how the child-specific protections are to be implemented and how data protection authorities will exercise their powers in this area.

(iii) The Age-Appropriate Design Code in the UK

The ICO Framework

Some data protection authorities, including those of the UK and Ireland, are required under domestic data protection legislation to prepare codes of conduct in relation to the processing of children's personal data.[253] The UK Information Commissioner's Office (ICO) is the first to release a comprehensive code of practice. The path-breaking 'Age Appropriate Design Code', which came into effect on 2 September 2020 with a 12-month transition period, is the result of extensive consultation with stakeholders.[254] The involvement of children and young people (as well as their parents and carers) was a critical component in the consultations leading to the development of the UK code.[255] Consistently with the requirement in Article 12 of the UNCRC, this approach ensured that children's views were properly represented in the design of protections aimed at them, and that the design principles adopted were relevant to them.

The Code applies to 'information society services' that are 'likely' to be accessed by children and defines a child as anyone under the age of 18.[256] This means that it covers services that

---

[251] Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679 Report, *Contribution from the Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation (GDPR)* (17 June 2020) 5.
[252] Ibid, 7.
[253] *Data Protection Act 2018* (UK), s 123.
[254] Information Commissioner's Office UK, *Age appropriate design: a code of practice for online services* (August 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.
[255] For this purpose, the ICO commissioned qualitative and quantitative research into the views of parents, carers and children on a range of issues suggested by the government as areas for inclusion in the code: ICO and Revealing Reality, *Towards a better digital future: Informing the Age Appropriate Design Code* (2019) <https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf> ('Information Commissioner's Office UK, *Towards a better digital future*').
[256] In line with the territorial scope of the *Data Protection Act 2018* (UK), the ICO Age Appropriate Design Code applies to online services based in the UK as well as online services based outside the

'children use in reality',[257] not only those that are designed for children. In determining whether a service needs to comply with the Code, the platform or provider must consider its potential appeal to children, given the nature and content of the service, as well as the way in which the service is accessed or restricted. If a platform or provider identifies children as a substantial user group, the standards of the Code will apply.

The ICO must take the provisions of the Code into account in the exercise of its regulatory functions, in particular in assessing an organisation's compliance with the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.[258] Conformance with the code will be considered particularly in relation to questions of fairness, lawfulness, transparency and accountability of data processing.[259]

The age-appropriate design code represents a new approach to the design of online services likely to be used by children. The standards in the code are centred on the principle that the best interests of the child should be the primary consideration when designing and developing apps, games, connected toys/devices and websites that are likely to be accessed by children. The advantage of this approach over a notice and consent model is that it seeks to address the attendant risks to personal privacy at the design stage, rather than relying on the consent of children or their parents.

In conducting this research, several operational privacy leaders were interviewed about their experiences in managing the privacy risks and obligations unique to children in Australia and abroad. One interviewee had experience in implementing age-based privacy controls for children with chronic illnesses and their families in the United Kingdom. The interviewee noted that whilst the inclusion of a 'best interests' test in the *ICO Age Appropriate Design Code* is positive, because it puts an onus on the organisation to 'do the right thing', entities are currently finding it difficult to navigate and comply with this requirement given that it has not yet been defined by a court.

The ICO Design Standards

The fifteen standards address the following issues:

1. Best interests of the child
2. Data protection impact assessments
3. Age appropriate application
4. Transparency
5. Detrimental use of data
6. Policies and community standards
7. Default settings
8. Data minimisation
9. Data sharing

UK that have a branch, office or other 'establishment' in the UK, and process personal data in the context of the activities of that establishment: ICO *Age Appropriate Design Code* (n 254) 18.

[257] Ibid 17.

[258] See *Data Protection Act 2018* (UK), s 127. See also ICO *Age Appropriate Design Code* (n 254) 89.

[259] ICO *Age Appropriate Design Code* (n 254) 89.

10. Geolocation
11. Parental controls
12. Profiling
13. Nudge techniques
14. Connected toys and devices
15. Online tools

Under each of these headings, the Code formulates a short headline standard, which is then further elaborated on in the main body of the Code. The headline standards set out the ICO's expectations at a relatively high level of generality, and then provide a more detailed explanation of what the standard means, why it is important and how it can be met. The structure adopted in the Code fulfils the objective of ensuring that the standards are neither too general nor overly prescriptive. The intent was to give organisations clear guidance, but also sufficient flexibility to address the standard in a way that is best suited to the organisation's needs and functions, while maintaining the overall aim of fostering children's privacy.

The Code addresses how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the developmental needs of, children. In so doing, the Code takes account of the standards and principles set out in the UNCRC. It sets out practical measures and safeguards to ensure processing of children's personal data can be considered 'fair', as required in a range of provisions under the GDPR and given the specific need for protection required by the GDPR.

For example, the Code requires that settings default to 'high privacy' and that options for profiling and collection of geolocation data are set to 'off'. The Code also requires the collection and retention of only the minimum amount of data needed to provide a service and that children's data should not be shared unless a compelling reason can be demonstrated for doing so, taking into account the best interests of the child.

Other European data protection authorities, including those in France and Ireland, are also focusing their regulatory attention on the specific risks to children's privacy.

(iv) Children's Privacy Protection in Canada

The regulatory context and reform proposals

While has no legislation specifically dealing with children's privacy, Canada is in the process of updating its privacy regime to provide Canadians with greater control over their personal information and privacy, which will also benefit children. The Personal Information Protection and Electronic Documents Act (PIPEDA), the federal privacy law for private-sector organisations in Canada, is supplemented by privacy legislation in a number of provinces, including Alberta, British Columbia and Quebec.

In the Canadian Digital Charter of May 2019, the Government announced the modernisation of PIPEDA.[260] One focal point of the reform agenda, as outlined in a White Paper, is the issue of meaningful consent and improved accountability.[261] The Digital Charter Implementation Bill 2020, which includes a new Consumer Privacy Protection Act, has been introduced to the Canadian Parliament in November 2020.[262] Ontario, the largest Canadian province, is also engaged in consultations as to whether provincial privacy legislation should be introduced.[263] The focus of the Ontario law reform is on enhancing consent and transparency; data erasure, data portability and data sharing; identifying what information should be protected and who should be subject to the new laws; as well as strengthening compliance and enforcement.

While the Ontario law reform process makes no specific mention of children, the particular vulnerability of minors has been recognised in a report by the Canadian Parliament.[264] A House of Commons Committee enquiring into the review of PIPEDA recommended that the 'Government of Canada consider implementing specific rules of consent for minors, as well as regulations governing the collection, use and disclosure of minors' personal information.'[265] These calls were echoed in a recent qualitative study that engaged young Canadians between 13 and 16 years of age and summarised its findings as follows:

> Participants consistently called out a lack of clarity and creativity in current approaches that contribute to a poor understanding of their privacy rights and were equally clear about wanting more information, more protection, more accessibility, more control, and more engagement.[266]

This study, which was financially supported by the Office of the Privacy Commissioner of Canada (OPC), also called for young people themselves to be involved in the design of online consent and privacy settings.[267]

Protection of children under PIPEDA

At present, there is no specified age limit for capacity to consent in Canadian privacy legislation. However, PIPEDA provides that consent is 'only valid if it is reasonable to expect that individuals to whom an organization's activities are directed would understand the

---

[260] Innovation, Science and Economic Development Canada, *Canada's Digital Charter: Trust in a digital world*, <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.
[261] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age From: Proposals to modernize the Personal Information Protection and Electronic Documents Act* (2019), <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html>.
[262] Bill C-11, 2020.
[263] In August 2020, the Government of Ontario released a discussion paper on reforming in Ontario's private sector privacy laws for the digital age: *Ontario Private Sector Privacy Reform: Improving private sector privacy for Ontarians in a digital age*, <https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45716>.
[264] House of Commons, Canada, Report of the Standing Committee on Access to Information, Privacy and Ethics, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act* (February 2018).
[265] Ibid, Rec 9.
[266] Samantha McAleese, Matthew Johnson and Marc Ladouceur, 'Young Canadians Speak Out: A Qualitative Research Project on Privacy and Consent' (MediaSmarts, Ottawa, 2020) 30.
[267] Ibid, 2.

nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.'[268] The wording of the provision applies broadly to all people from whom consent is sought, but it has particular importance where a service, activity or website is directed at young people. Instead of specific age thresholds for providing consent, PIPEDA adopts the concept of 'meaningful consent', which requires a contextual analysis that also has regard to a child's 'cognitive and emotional development'.[269] For example, in the context of online behavioural advertising, the OPC has stated that it is 'hard to argue that young children could meaningfully consent to such practices'.[270] Importantly, PIPEDA does not appear to require an individual assessment of a person's capacity to consent, but depends on an objective assessment of the situational context in which consent is sought from the perspective of the individuals from whom consent is sought and given. It imposes a requirement on data processors to provide affected individuals with the information that allows them to understand the nature, purpose and consequences of the proposed data processing. In that sense, it creates a general condition of valid consent, rather than limit an individual's capacity to consent.

'No-Go' Zones

PIPEDA section 5(3) imposes an overarching limit on all data processing. It provides that an 'organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'.[271] Processing that does not pass this 'critical gateway'[272] is unlawful even if the individual may have provided consent.

The 'appropriateness' of data handling depends on a 'balancing of interests' between the individual and the organization concerned.[273] Canadian jurisprudence, particularly the Federal Court in *Turner v Telus Communications Inc*, has developed the following factors for evaluating whether an organization's purpose was in compliance with subsection 5(3):

- The degree of sensitivity of the personal information at issue;
- whether the collection, use or disclosure of personal information is directed to a *bona fide* business interest;
- the effectiveness of the collection, use and disclosure in meeting those business interests;

---

[268] PIPEDA s. 6.1 (introduced by Digital Privacy Act, 2015, c. 32).
[269] Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, December 2015 <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.
[270] Ibid.
[271] The ACCC *DPI Final Report* (n 3) has recommended a new requirement for the fair use and disclosure of personal information (rec 17.3), which would also provide an additional hurdle intended to protect the individual against illegitimate data processing.
[272] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, May 2018 ('OPC, Guidance on inappropriate data practices').
[273] *Turner v Telus Communications Inc.*, 2005 FC 1601, [39]; aff'd 2007 FCA 21.

- the reasonableness of the collection, use and disclosure against alternative methods of achieving the same objectives at comparable cost and with comparable operational benefits; and
- whether the loss of privacy is proportional to the cost and any operational benefit gained.[274]

Where a data practice does not pass this 'overarching requirement',[275] it will be regarded as 'inappropriate' and constitute an activity that an organisation is generally not allowed to engage in, even if consent was provided. These areas of inappropriate data processing are also described as 'no-go zones'.

In its current Guidance,[276] the OPC has identified the following 'no-go zones':

- collection, use or disclosure that is otherwise unlawful
- profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law[277]
- collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual[278]
- publishing personal information with the intended purpose of charging individuals for its removal
- requiring passwords to social media accounts for the purpose of employee screening
- surveillance by an organization through audio or video functionality of the individual's own device.

The OPC Guidance emphasises that these current 'no-go zones' may change over time. It also clarifies that these are not absolute prohibitions, because 'in exceptional cases, information related to the described contextual factors may lead to the conclusion that a particular use would, in fact, be considered appropriate by a reasonable person, even though it falls within one of the listed no-go zone'.[279]

Such potential exceptions are in line with the general approach under s 5(3) that assessing the appropriateness of data processing requires a balancing of competing interests. This includes that the loss of privacy has to be put into the context of potential benefits accruing to the individual and the data processor, respectively. For example, it could be found that the

---

[274] Ibid, [48]. See also *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, [127]; A*.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310, [73].
[275] *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310, [73].
[276] OPC, *Guidance on inappropriate data practices* (n 272).
[277] The OPC Guidance, ibid, clarifies that profiling that leads to discrimination contrary to human rights law will always be inappropriate, while the decision on whether the treatment is unfair or unethical requires a case-by-case assessment.
[278] In line with PIPEDA subsection 10.1(7), the OPC defined significant harm as 'bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property': see ibid.
[279] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices* (n 272) Fn. 10.

surveillance of a person through that person's own device can have benefits, for example, where it occurs with their knowledge and for their protection, or where it has other significant benefit for the individual so that, in the result, the loss of privacy is proportionate to the benefits obtained.

The current list of 'no-go zones' does not contain any child-specific prohibitions of data practices. However, some of the illegitimate activities identified may be relevant also for individuals under 18 years of age. This may apply to the prohibition of profiling that leads to treatment contrary to human rights and of data practices that are known or likely to cause significant harm to the individual. For each of these no-go zones, the fact that the individual was a child, and therefore in greater need of protection, is likely to weigh heavily in the balancing of the competing interests. In its Discussion Paper on Consent, the OPC has furthermore specifically identified the possibility that a no-go zone may be based on the 'vulnerabilities associated with the group whose data is being processed'.[280] The OPC has also stated a policy position that organisations 'should avoid knowingly tracking children and tracking on websites aimed at children' for the purposes of online behavioural advertising.[281] This 'best practice' position was said to reflect the difficulty of obtaining meaningful consent to such data practices from children, which especially at a younger age may not understand that they are being tracked.[282]

(v) Other jurisdictions with child-specific privacy protections

While the US and the EU have the most developed regulations on children's privacy, it is important to note that children's privacy is emerging as a concern in countries around the globe. There is an increasing number of jurisdictions that have specifically legislated in this area. However, much of this legislation is yet to be implemented or relies significantly on the rules in the US or Europe, so only a brief overview will be given here.

China

With effect from 1 October 2019, the Cyberspace Administration of China adopted *Measures on the Protection of Children's Personal Information Online* ('Measures').[283] This enactment imposes more stringent requirements on network operators which collect, store, use, transfer or disclose the personal information of minors under 14 years old within the PRC. Under the Measures, a network operator must:

- obtain express consent from the child's guardian for the collection, use, transfer, or disclosure, after providing them with a clear, prominent and detailed privacy notice
- not use a child's personal information in excess of the purpose agreed

---

[280] Office of the Privacy Commissioner of Canada, *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*, 17 ('Consent and privacy').
[281] Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising*, <https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp>.
[282] Office of the Privacy Commissioner of Canada, *Consent and privacy* (n 280).
[283] Gil Zhang and Kate Yin, 'China has released its version of COPPA', *iAPP News* (1 October 2019) <https://iapp.org/news/a/china-has-released-its-version-of-coppa/>; see also Sara Xia, 'China's New Child Privacy Protection Rules', *China Law Blog* (22 Sept 2019) <https://www.chinalawblog.com/2019/09/chinas-new-child-privacy-protection-rules.html>.

- not disclose a child's personal information unless required by law or with the child's guardian's explicit consent
- not retain a child's personal information longer than necessary to fulfil the purpose of its collection and use
- designate a person responsible for protecting a child's personal information and restrict access to a child's personal information by its employees
- safeguard a child's personal information by encryption or other means and report data breaches affecting children's personal information
- before a third-party disclosure of children's personal information, conduct a security assessment of the third party and enter into an agreement defining the respective responsibilities and the scope and purpose of the third-party processing, and
- correct and delete a child's personal information on request by the child or the child's guardian.

While it remains to be seen how the Measures will operate and be enforced in practice,[284] their enactment makes clear that China has recognised the need to protect children's data more strongly than the personal data of adults. Of particular note is that the Measures encourage internet industry associations to establish industry standards and codes of conduct for the protection of children's personal information.

Under the draft of a comprehensive new Personal Data Protection Law, which has been published for public consultation in October 2020, data processors require parental consent for the processing of personal data of minors below the age of 14 if they know or should know that they are processing the data of a child.[285]

India

India's Parliament is currently considering the Personal Data Protection Bill 2019, which is intended to create a comprehensive personal data protection framework similar to the EU's GDPR. Clause 16 of the Bill contains specific protections for children, defined as persons under the age of 18. Under this provision, a data fiduciary[286] shall process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child. Data fiduciaries are required to verify the child's age and obtain the consent of the child's parent or guardian, in a manner to be specified by regulations, before processing any personal data of child. The Bill does not appear to provide scope for older children to consent to data processing.

Data fiduciaries that 'operate commercial websites or online services directed at children' or 'process large volumes of personal data of children' can be classified by regulation as 'guardian data fiduciaries'. Such classification means that would be prohibited from

---

[284] Latham & Watkins LLP, 'China Issues New Cybersecurity Law to Protect Children', *Global Privacy and Security Compliance Law Blog* (9 Sept 2019) <https://www.globalprivacyblog.com/security/china-issues-new-cybersecurity-law-to-protect-children/>.
[285] Gil Zhang and Kate Yin, 'A look at China's draft of Personal Data Protection Law', *iAPP News* (26 October 2020) <https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/>.
[286] A 'data fiduciary' is defined as a 'person who determines the purpose and means of processing of personal data', whereas 'data processors' are persons who 'processes personal data on behalf of a data fiduciary': see Personal Data Protection Bill 2019 (India) cl 3.

processing that 'can cause significant harm to children', specifically from 'profiling, tracking, doing behavioural monitoring, or targeting advertisements at children'.[287] This provision gives the Data Protection Authority the power to subject a provider, or group as providers, that fulfils the statutory criteria to stricter data protection requirements. This targeted power has been recommended as 'a good model as to an overall principled approach',[288] however, it can be queried why the protections envisaged by this provision should be limited to classified providers. While it is likely that operators of commercial websites or online services directed at children or processors of large volumes of children's personal data are likely to be a particular concern, a practice that can cause significant harm to children and is therefore incompatible with children's best interests arguably should be prohibited as such – and regardless of whether an operator's activities were directed at children or the volume of children's personal data handled by an operator.

The provision on codes of practice (cl. 50) specifies that codes may address 'processing of personal data of children and age-verification under this Act'. Given that the Bill has yet to become law and that the regulations by the Data Protection Authority have yet to be drafted, the exact scope, content and effect of the law remains to be seen. However, it is now apparent that India plans to adopt international standards in relation to the protection of children's personal information.

Brazil

Brazil's *Lei Geral de Proteção de Dados* (or LGPD) came into effect in September 2020. The LGPD has been inspired by the GDPR, including in relation to the provisions dealing with the processing of children's personal data. Article 14 of the LGPD requires that the processing of personal data belonging to children and adolescents shall be carried out in their best interests, pursuant to that article and pertinent legislation. Controllers must provide information about their processing practices in relation to children's personal data in a simple, clear and accessible manner taking into account their users' characteristics and in a way that is appropriate for the children's understanding. In particular, data controllers must:

- obtain the specific and express consent of a parent or legal guardian before processing children's data
- make all reasonable efforts to verify that the consent was given by the child's representative, considering available technologies
- not make the participation of children in games, internet applications or other activities conditional on the provision of more personal information than is strictly necessary for the activity.

As the LGPD has only very recently come into effect, it is difficult to gage its practical impact and some aspects remain undefined. In particular, it is still unspecified at what age a person ceases to be a child under the LGPD. It is also unclear whether the parent's consent will be a requirement for all data processing or whether, in line with developing understanding, a

[287] Personal Data Protection Bill 2019 (India) cl 16(4).
[288] Peter G Leonard, *Notice, Consent and Accountability: addressing the balance between privacy self-management and organisational accountability - A paper for the Office of the Australian Information Commissioner* (June 2020) 72.

child can make some valid privacy choice without its parents. The data protection authority is still in formation and penalties will not be issued until August 2021. However, similar to the other regulations highlighted in this section, it demonstrates that emerging economies are keen to adopt child-specific protections.

South Korea

Under the Personal Information Protection Act of South Korea, information and communication providers that intend to process the personal data of children aged under 14 need to get explicit consent from the child's parents or legal guardians and verify the consent in accordance with specified regulations. They need to inform children under the age of 14 about matters relating to the processing of personal information, in an understandable format and using clear, age-appropriate language. Recent revisions have provided further clarification on how parental consent can be obtained. Providers collecting children's personal data need to ask children whether their parents provide consent. Parental consent can be given either via text, payment information, or authentication through smartphones, and needs to returned in writing to the providers.[289]

It has also been reported that the Korea Communications Commission (KCC), the national regulator for broadcasting and communication services, fined TikTok in July 2020 for collecting the data of children under the age of 14 without their legal guardians' consent.[290]

[289] Cho Mu-Hyun, 'South Korea strengthens child data protection laws', *ZDNet* (24 June 2019) <https://www.zdnet.com/article/south-korea-strengthens-child-data-protection-laws/>. There is a useful overview of the amended Personal Information Protection Act, which came into force on 5 August 2020, at Linklaters, 'Data Protected - Republic of Korea', <https://www.linklaters.com/en/insights/data-protected/data-protected---republic-of-korea>.
[290] Cho Mu-Hyun, 'South Korean regulator fines TikTok over mishandling child data', *ZDNet* (15 July 2020) <https://www.zdnet.com/article/south-korean-regulator-fines-tiktok-over-mishandling-child-data/>.

Question 2b — How meaningful consent should be obtained from children in relation to the collection, use and disclosure of their personal information in the online environment?

Key findings:

Children's ability to make informed choices is developing throughout the teenage years. It is important to adopt an approach that protects children's privacy rights against undue interference, yet also respects their increasing ability to make their own privacy choices.

Despite a growing body of empirical evidence into the capacities of children and adolescents to make their own privacy decision, there is no consensus as to the most appropriate age of consent. Approaches in overseas jurisdictions are not evidence-based, and range from 13 to 18 years of age.

Future Australian regulation should therefore aim to stipulate an age limit at which it would be safe to assume that a child of ordinary capacities and development will have capacity to make its own privacy decisions. Until further stakeholder engagement on this question is undertaken, this Report favours maintaining and codifying the current Australian threshold of 15 years of age.

(i) Position in Australia

The Privacy Act makes no specific reference to children or young people and offers no additional protection for them. As a result, where data processing requires consent, the ordinary principles relating to consent, and the capacity to give consent, apply.[291] If a child provides consent, this consent is valid only if he or she has the requisite capacity. This requires that the child has sufficient maturity to understand what is being proposed and the consequences of giving or withholding consent.

Capacity must generally be determined on the basis of individualised assessment. This model for individualised assessment of capacity is consistent with the available research on development psychology, which suggests that the age at which children attain maturity may vary significantly between individuals, making the use of bright line approaches based on age for determining capacity problematic. This case-by-case model for assessing capacity is also consistent with the approach taken in Art. 12(1) of the United Nations Convention on the Rights of the Child (UNCRC), which requires all states to:

> assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.[292]

---

[291] Some state privacy and health privacy legislation contains detailed provisions on capacity to consent and the giving of consent by a representative: see, eg, *Health Records and Information Privacy Act 2002* (NSW), s 7; *Privacy and Data Protection Act 2014* (Vic), s 28 and *Health Records Act 2001* (Vic), s 85.

[292] UN Convention on the Rights of the Child, Adopted by the General Assembly of the United Nations on 20 November 1989, (1990) 1577 UNTS 3 ('UNCRC').

However, requiring an assessment of individual capacity for each child whose data an entity wishes to handle adds considerable complexity to business processes. It requires decision-makers to correctly assess whether a child has sufficient capacity to consent. This approach creates risks for children if there is failure to identify correctly any lack of capacity.

The OAIC's Australian Privacy Principles Guidelines (APP Guidelines) seek to address these problems by steering a middle ground between individualised assessment and practicability. The APP Guidelines affirm the general proposition that APP entities need to determine 'on a case-by-case basis'[293] whether an individual under the age of 18 has the capacity to consent and that capacity depends on 'whether they have sufficient understanding and maturity to understand what is being proposed'.[294] However, the APP Guidelines also suggest that, if it is not practicable or reasonable for an APP entity to assess a child's capacity on a case-by-case basis, the entity may rely on two presumptions: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise; second, that a child under 15 does not have capacity to consent.[295]

This approach leaves open a number of questions, including how an entity is to determine the capacity of an individual under the age of 18; when an individual assessment will be considered not to be practicable or reasonable; and how conflicts between a child and a parent in relation to the giving of consent are to be resolved. Additionally, there is currently no specific requirement for providers of services to children to draft privacy notices in a manner that children can understand easily, even though the ability to provide informed consent depends on a full understanding of the consequences involved.

(ii) Age of digital consent in overseas jurisdictions

The COPPA rule

As outlined above, international approaches as to the age of digital consent vary quite significantly between the ages of 13 and 18 years of age. The COPPA rule in the US, which establishes an age limit of 13 years of age, was adopted when the internet was in its infancy and social media platforms were yet to be invented. The major western online platforms (including Facebook, Instagram, Snapchat) stipulate a minimum user age of 13 years and as a result avoid the COPPA rule to seek parental consent from under-age users. Despite the 'de facto standard for parental consent online'[296] that emerged in response to COPPA, more recent enactments, as well as the findings on child development, would suggest a higher age threshold as being more appropriate.

Article 8 of the GDPR

The GDPR also adopts a fixed age of consent, but the age levels are not set uniformly in EU Member States. While the default age limit under the GDPR has been set at 16 years of age,

---

[293] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) [B.56] ('APP Guidelines').
[294] Ibid, [B.57].
[295] Ibid, [B.58].
[296] Milda Macenaite & Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26(2) *Information & Communications Technology Law* 146, 183.

Member States can adopt a lower age, provided it is not lower than 13 years. The GDPR law making process demonstrates that long-standing differences in cultural attitudes concerning child maturity can be difficult to reconcile, especially when there are also significant commercial interests at stake that are forcefully represented by industry lobbies.

The Commission draft of the GDPR stipulated that, in the online environment, processing personal data of children under the age of 13 years requires consent from the child's parent or custodian. The Commission's Impact Assessment acknowledged that the proposed rules on the age of consent had taken 'inspiration for the age limit from the current US Children Online Data Protection Act of 1998 and [were] not expected to impose undue and unrealistic burden upon providers of online services and other controllers'.[297]

When the Council draft of the GDPR subsequently raised the limit to 16 years of age, this revision was met with sharp criticism both by industry representatives but also child rights experts.[298] Industry argued that raising the age would increase the compliance burden and would lead to the withdrawal of some services from children. Child right experts considered that the new age limit was unrealistically high and would require children who are capable of deciding on their own whether to use certain social media services to seek their parents' consent. The concerns caused the EU to develop the present compromise position that maintained the default threshold age of 16, but allowed member states to lower the age limit, provided it was not lower than 13 years of age.

This framework allowed Member States to retain their pre-GDPR approaches, as well as create alignment with the COPPA age limit, if they wished to do so. This resulted in a patchwork of approaches that contradict the objective of the GDPR to create uniform data protection standards throughout the EU. Germany, Hungary, Croatia, Ireland, Luxembourg, the Netherlands, Poland, Romania and Slovakia were content with the age limit of 16 years, whereas Belgium, Denmark, Estonia, Finland, Latvia, Malta, Portugal and Sweden decided on a lower age limit of 13 years; Austria, Bulgaria, Cyprus, Spain, Italy and Lithuania chose 14 years; and the Czech Republic, Greece and France decided on 15 years.[60]

Approaches in other jurisdictions

China has adopted an age level of 14 years of age, whereas the recent privacy enactments in the new data protections laws in Brazil and India do not appear to provide for consent by minors at all.

Canada, similar to Australia, does not lay down an age of digital consent. Instead, PIPEDA provides that consent is only considered valid if the organisation's target audience can

---

[297] European Commission, *Commission Staff Working Paper: Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, SEC (2012) 72 final (25 January 2012) 68.
[298] See discussion by Karen Mc Cullagh, 'The general data protection regulation: a partial success for children on social network sites?' in Tobias Bräutigam and Samuli Miettinen (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia Helsinki 2016), 110, 123-4.

reasonably be expected to understand the nature, purpose and consequences of the collection, use or disclosure proposed.[299]

(iii) The conflicting concerns in setting an age limit

The question of whether a particular age of digital consent should be prescribed raises a number of conflicting concerns. The rationale for requiring the parents to provide their consent for the collection of their children's data is based on the notion that children are not sufficiently developed to make decisions that concern the use of their data. It is also based on the assumption that parents are better positioned to manage their children's privacy. This latter assumption is problematic because parents often also lack understanding of the issues around children's privacy and do not necessarily have the digital literacy to assess the appropriateness of a particular data processing measure for their children.

While the UNCRC enshrines the principle that children are entitled to 'special protection', children's participation rights need to be taken into account as well. Seeking consent from children promotes their online participation. From a children's rights perspective, it is therefore supportive of their right to be heard (Art. 12 UNCRC) and promotes their right to development (Art. 6 UNCRC). Transparency about data processing and providing children with a sense of control and choice is supportive also of their right to receive information (Art. 13 UNCRC).

It is difficult to reconcile these conflicting child rights concerns. In its Digital Platforms Report, the ACCC recommended:

> Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian.[300]

Taken literally, this recommendation would require the obtaining the guardian's consent *whenever* the personal information of children is collected. This would be a retrograde step for teenage children who, because of their more advanced age, experience and understanding, have already developed the capacity to give consent. In line with current Australian law and overseas regulation in the EU and US, it is more appropriate to require the guardian's consent only in the case of younger children who lack capacity or where a practice is not likely to be understood by a child. This approach is more supportive of children's developing ability to make informed privacy choices and is preferable from a children's rights perspective because it enhances their participation in matters affecting them and supports their development of online skills.

If a role for specific children's consent is accepted, the first question to be answered is whether Australia should move to a (more) fixed age level, or whether it should retain its current approach of individualised assessment, aided by presumptions of maturity. The second question, which arises if an age limit is to be introduced, is: what age level would be most appropriate?

---

[299] PIPEDA s. 6.1 (introduced by Digital Privacy Act, 2015, c. 32).
[300] ACCC *DPI Final Report* (n 3) Rec 16(c).

(iv) Fixed age level or individualised assessment?

Under general law, consent is only valid if it is provided by a person with capacity to make decisions. As discussed above, children's cognitive, affective and decision-making skills develop at differing rates and reach the required level of maturity at different ages. The age at which a child reaches this maturity is dependent on a wide variety of individual factors, including the child's intelligence, physical and psychological development, and educational attainment as well as the economic, social, family and cultural circumstances in which the child grows up. While this suggests that a subjective assessment of the capacity to make privacy decisions would be ideal, requiring such assessments is problematic in the context of information society services that are provided at scale and at a distance.

Apart from the burden and practicality of requiring an individualised assessment, such an approach would also be likely to raise further privacy issues. In particular, an organisation might have to collect not only the information needed to provide the service in question, but also further personal information, including sensitive data, to make an assessment on maturity. It would be counterproductive if a requirement to assess a child's capacity to consent created additional privacy risks that outweigh the privacy concerns it sought to address. Innovative age-verification mechanisms, e.g. such as attribute-based age verification,[301] could go some way towards developing protocols that minimise data collection, but presently these require further research and product development.[302] In attribute-based age verification schemes, 'only a particular attribute, such as age, is cross-checked in order to establish an internet user's eligibility to access an online service'.[303] Such schemes, which are often provided through third party services,[304] minimise personal data collection when compared to a full identity verification of an internet user, while still restricting eligibility to use a particular platform or service to those who can establish the requisite attribute.

While a set general age limit may not do justice to each individual, it does provide the benefit of clarity. Companies can more easily establish whether a child has attained a specified age than whether the child is of sufficient maturity to decide on its privacy protections. To address the problem that some children may not have reached sufficient maturity at the set age limit, there could still be scope for individual factors to be taken into account. In particular, when there are reasons to doubt that a user has the requisite capacity, it would be appropriate to expect an organisation to enquire further and to determine on an individual

---

[301] Macenaite and Kosta (n 296) 191–192.
[302] See Australian Parliament, House of Representatives, Standing Committee on Social Policy and Legal Affairs, *Inquiry into and report on age verification for online wagering and online pornography,* <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification>. The European Commission has indicated that it is developing a pilot project for an interoperable technical infrastructure that would support the implementation data protection rules to children, including age-verification and parental consent: European Commission, Communication from the Commission to the European Parliament and the Council, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, 15.
[303] Macenaite and Kosta (n 296), 192.
[304] See, eg, Charles Hymas, *Duty of Care: Children to give parents' mobile numbers when signing on for social media*, The Telegraph (UK) (18 November 2020) <https://www.telegraph.co.uk/news/2020/11/18/duty-care-children-give-parents-mobile-numbers-signing-social/>.

basis whether the child above the age threshold has capacity or whether the parent's consent is required. This would be in line with the current approach adopted by the OAIC that the presumption of maturity at 15 years of age 'unless there is something to suggest otherwise'.

(v) Setting the age limit

There is no international consensus on the appropriate age of consent, with jurisdictions setting this age variously at 13, 14, 15, 16 or 18 years of age. As there is 'little evidence of a magic switch in maturity when children turn 13 (or 16)',[305] all bright-line approaches are somewhat arbitrary. Neither the US nor the EU have published evidence to support the age limit chosen, which appears to have been determined primarily by political and cultural considerations. As a result of the burgeoning interest in children's experiences of the digital world, there is now, however, a much greater body of empirical evidence by child development and child psychology researchers, as further discussed in Part 1.

What is clear from the research is that the majority of children will have acquired the requisite cognitive capacity to make decisions by 13 but that they may still lack the necessary language skills and the necessary contextual knowledge to make fully informed decisions in the context of collections by platforms and other online websites until they are older than that. Until they reach that stage, the requirement of parental/guardian consent is arguably a necessary and proportionate response; the potential for privacy-related harm is substantial and may outweigh any diminution of participative rights.

Evidence also suggests that young people generally lack the maturity to make good decisions in contexts that are emotionally charged or subject to peer pressure until and even into early adulthood. However, as teenagers get older their right to privacy vis a vis their parents becomes more significant, tilting the balance against any requirement for parental consent.

Future Australian regulation should therefore aim to stipulate an age limit at which it would be safe to assume that a child of ordinary capacities and development will have capacity to make its own privacy decisions. When a data processor then relies on the consent of a child of the stipulated age, that consent should be regarded as valid unless the processor is aware (or ought to be aware) that the child did in fact not have sufficient understanding and maturity.

A number of problems have been identified with unrealistically demanding privacy restrictions for persons of young age. While a high age of digital consent may be a well-intended measure to protect children, it is likely to affect a young person's participation in online services and may also delay the development of digital skills. More importantly, this may also hinder adolescents in achieving their development goals of interacting with their peers and increasing their independence from adults such as their parents and teachers.

Children's developmental, emotional and social needs and skills change significantly during their teenage years. As they grow older, children become more aware of the opportunities and risks of online technologies. They also develop their skills in identifying risky behaviour

[305] Sonia Livingstone, 'Children: a special case for privacy?' (2018) 46(2) *Intermedia* 18, 22.

and weighing up the benefits of certain activities with their potential downsides. Restrictions on their digital agency make it harder for children to develop the skills needed to protect themselves in the digital environment, which suggests that, as they grow older, they should be provided with increasing opportunities to make decisions for which they must take responsibility.

The imposition of age-based restrictions has an impact on the availability of services for children. Many general audience platforms provide in their terms of service that account holders must be 13 years of age or older. [306] As indicated, these limits are set to avoid the burden of providing privacy notices to parents and seek their consent, as required under the COPPA rule. It may be seen as a matter of concern from a child's participation rights perspective that business prefers to exclude children from a particular service rather than to develop protocols that allow children to use that service safely.

The fact that a significant proportion of users of these services are in reality below the stipulated threshold reveals a desire on the part of young people to use these services.[307] There is significant evidence that some children lie about their age in order to access these websites or that they manipulate verification procedures.[308] Lax age verification protocols, coupled with inadequate enforcement, have allowed these practices to become widespread – as discussed below, often with parents' tacit or active involvement. However, giving younger children access to content and platforms that are intended for teens and adults can have harmful consequences at a later date. Platforms with content for adults (such as advertising for alcohol, gambling etc) could improperly make such content available before the user actually turns 18 years of age. Another important concern is that rules that the community widely regards as inappropriate, or that are not sufficiently enforced, foster disrespect for the law. It is therefore important not to set the age limit inappropriately high and then turn a blind eye to children circumventing these age restrictions.

Conversely, an age limit must also not be too low because this would enable children to make privacy choices that may turn out to be harmful to them or that they still lack the capacity to comprehend. While children's privacy skills develop with age, parents report that they remain incomplete even in the teenage years.[309]

Parental reluctance to endorse a low age of digital consent is confirmed by the findings of the latest Australian Community Attitudes to Privacy survey. In response to the question of what age parents think is most appropriate for their child to consent to handing over their personal information in exchange for an online service, the largest proportion of parents (38%) preferred the age bracket 16-18 years, and another 24% thought that it should be

---

[306] This includes Facebook, Snapchat, Twitter, Instagram, Skype and YouTube.
[307] The child-friendly off-shoots provided by some platforms, such as YouTube Kids, can lack sufficient appeal to children.
[308] danah boyd, Eszter Hargittai, Jason Schultz & John Palfrey, 'Why parents help their children lie to Facebook about age: Unintended consequences of the "Children's Online Privacy Protection Act"' (2011) *First Monday* 16(11), <https://doi.org/10.5210/fm.v16i11.3850>.
[309] Sonia Livingstone, Alicia Blum-Ross and Dongmiao Zhang, 'What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3' <https://www.lse.ac.uk/media-and-communications/assets/documents/research/preparing-for-a-digital-future/P4DF-Report-3.pdf> 1.

between 13 and 15 years of age.[310] Younger age brackets were identified by considerably smaller cohorts (between 2% and 14%). However, given that participants in this survey were able to vote only for age brackets (rather than a specific age), the data provides no more than a broad indication of parental preferences. In particular, it provides no valid basis for identifying a particular age limit that would have most parental support.[311]

Despite its use in other jurisdictions, including the US and the UK, it would appear that a threshold of 13 years is too low, in particular in relation to data practices that are difficult to understand or that have unclear consequences. It cannot be assumed that children at that age understand the complexity of online data flows and the potential consequences of providing their consent to collection, processing and disclosure of their personal information. Given that children's digital literacy and cognitive capacity are still developing throughout their teenage years, the barriers for children to give informed consent are even greater than for adults. This is supported by research into children in the digital environment, which concluded:

> Yet extensive independent research repeatedly finds not only that children don't fully understand their privacy or rights online, but also that they are actively discouraged from understanding them by the way the information is presented online. … Children don't read terms and conditions or privacy notices and are either unable or discouraged to given their length and complexity.[312]

Recommendation on age limit

Given the complexity of the issues involved, the gaps in the evidence, and the range of interests affected, we would recommend that the age of digital consent should be set after extensive further consultation, including in particular with experts, parents, children and the relevant industries. On the basis of the available evidence, we tentatively favour an age limit of 15 years. This is the age threshold that is stipulated in the current APP Guidelines, under which an APP entity may rely on two presumptions where an individualised assessment is impractical: first, that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise; second, that a child under 15 does not have capacity to consent.[313] We are not aware that this age threshold has caused particular obstacles to the participation of Australian children in online services (although this may, of course, be partly due to lack of enforcement of this age limit). It is important to note, as well, that a higher threshold for children's consent does not necessarily mean that particular data practice

---

[310] Office of the Australian Information Commissioner and Lonergan, *Australian Community Attitudes to Privacy Survey 2020* (September 2020), 100 ('OAIC Community Attitudes Survey').
[311] The survey report suggests that the 'average age parents believe children should be able to consent to handing over their personal information in exchange for an online service is 13 years': ibid. However, it is unclear how this conclusion was drawn from the available data, given that preference for a particular age bracket is not indicative of which age within that bracket parents would consider the most appropriate. It also appears that some parents may have misunderstood the question, given that 2% of parents said the age between 1 and 3 years and another 9% stated that age between 4 and 6 years is the most appropriate for children to be able to consent.
[312] 5Rights Foundation, Submission to Joint Committee on Human Rights – The Right to Privacy and the Digital Revolution, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/the-right-to-privacy-article-8-and-the-digital-revolution/written/97261.html> ('Submission').
[313] Ibid, B58.

involving children's personal information would be, for that reason, impermissible. It merely means the practice needs to be justified on alternative grounds. This could be either parental consent or, if the approach in the GDPR is adopted, on grounds of legitimate interest, which would include consideration of a child's best interest.

A threshold of 15 years is also compatible with findings that emphasise the complexities of modern data flows and the difficulties, even for older children, of comprehending some of the privacy issues involved. It adopts a middle ground in recognition of the fact that developing a sufficient understanding of privacy issues is a continuous process during teenage years:

> From age 12 onwards, children are more aware of privacy risks and often engage in careful consideration of information disclosure. They begin to grasp aspects of institutionalised and commercial privacy – for example, in relation to school monitoring of online activities and exposure to advertising content based on browsing history. Even the oldest children (aged 17) understand little of data flows and digital infrastructure – they mostly see data as static and fractured.[314]

There are further variables that are important for setting an appropriate age threshold, which include, first, digital education; and second, the character and transparency of the data practices in question.

The role of digital education and the data practices in question

Enhanced education can foster children's understanding of the privacy risks and improve their strategies and acts of data self-management. However, measures directed at improved digital agency find their limits in deliberately obscure data practices that make unrealistic demands on individual vigilance. This is addressed in a recent study into the development of adolescents' advertising literacy and privacy protection strategies, which looked at targeted advertisements on social networking sites:

> Even if adolescents were to have sufficient advertising literacy (i.e. understanding that targeted ads aim to sell and persuade), it does not necessarily follow that they also understand the underlying data acquisition and usage due to a general lack of transparency.[315]

Nudging that inhibits free choice by designing the choice architecture so as to alter people's behaviour and 'dark patterns' that make it intentionally hard to understand and implement privacy choices can create the impression of being 'deceived by design'.[316]

Young people have reported feeling 'doubts over the effectiveness of any alternative actions' and 'annoyance [because] the responsibility for action should not fall onto individual users', even when they are made aware of the digital privacy issues and possible counter-strategies to protect their data.[317] Education is therefore unlikely to address the main concern that

---

[314] Stoilova, Nandagiri and Livingstone, *Systematic Evidence Mapping* (n 14).
[315] Brahim Zarouali et al, 'Adolescents' advertising literacy and privacy protection strategies in the context of targeted advertising on social networking sites: implications for regulation' (2020) 21(3) *Young Consumers* 351, 354.
[316] Forbrukerådet, *Deceived by Design* (n 189).
[317] Neil Selwyn and Luci Pangrazio, 'Doing data differently? Developing personal data tactics and strategies amongst young mobile media users' (2018) 5(1) *Big Data & Society* 1, 8.

individual data agency is systematically inhibited and that young people remain inert because they feel disempowered to protect their personal data in the current digital environment. Furthermore, because of systemic disadvantage, educational programs often do not reach those that are most in need of them. They also cannot address the cognitive and emotional barriers that are inherent in the developmental stages of childhood and adolescence. This means that, while they are an important component of digital citizenship, further efforts in digital literacy education are unlikely to provide a complete answer to the issue of privacy protection.

Capacity to consent is dependent on a person's understanding of how their personal information is collected, used and disclosed, as well as the effect of giving or withholding consent. This understanding can be significantly affected by the character and complexity of the data practices in question, and the level of transparency surrounding these data practices. For example, the development literature suggests that institutional or commercial privacy is the area which children are least able to comprehend and manage on their own.[318] This suggests that children will develop a sufficient understanding of more straightforward data practices, in particular interpersonal privacy, earlier than an understanding of more abstract and more opaque forms of data processing. Therefore, they may have capacity to consent to the former practices at an earlier stage in their development than the latter. In recognition of that, the Canadian approach to consent is context-specific and takes into account how intelligible the data practices in question are. Consent is considered 'only valid if it is reasonable to expect that individuals to whom an organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.'[319]

Adopting such a contextual approach should lead to outcomes that are more calibrated to the needs and skills of young people. It also gives an incentive to data processors to simplify their data practices if they seek to rely on a child's consent and to undertake greater efforts to be transparent about their data practices. Providing suitable notice of 'the nature, purpose and consequences of the collection, use or disclosure' in a child-friendly manner would go some way towards enhancing a child's understanding and therefore their capacity to provide consent.

The notion that APP entities have a responsibility to build the capacity of individuals to provide consent is also contained in the existing APP Guidelines, which can therefore be drawn on. The APP Guidelines state that, where age, disability, and limited ability to speak English affect an individual's capacity, an 'APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent'.[320] In the same way in which support tailored to the personal characteristics of the individual can enhance an individual's capacity to consent, it can be argued that simplification of data practices and enhanced transparency through child-friendly notices can support the child's understanding of how their data are collected, used and disclosed and how giving or withholding consent would affect them.

---

[318] Livingstone, Stoilova and Nandagiri, *An Evidence Review* (n 14) 4 and 15.
[319] PIPEDA s. 6.1 (introduced by Digital Privacy Act, 2015, c. 32).
[320] *APP Guidelines* (n 293) [B.54].

Conclusion

There is no international consensus on the appropriate age of digital consent. Despite a growing body of empirical evidence into the capacities of children and adolescents to make their own privacy decision, there is as yet no clear evidence that establishes where the precise cut-off should lie. The speed with which children acquire the language skills and contextual knowledge necessary for informed decision-making is subject to a large number of variables, which include their personal characteristics, their level of digital literacy, as well as the complexity and transparency of the data practices involved. On the basis of the available evidence and subject to the results of further consultation with stakeholders, we see a case for adopting the cut-off age of 15 currently in use by the OAIC.

(vi) Best practice consent mechanisms

There is no 'one size fits all' best practice approach to consent. In practice, consent mechanisms must bring together effective transparency (consent must be informed), appropriate timing (consent must be current), an assessment of the capacity of the individual, and the absence of coercive factors such as bundling, nudging or unequal bargaining positions.

How this is best done depends greatly on context. Research done for the CDR consumer data standards shows the wide range of considerations involved, including trust and safety, transparency and accountability, agency and self-directed choice, accessibility and clarity, and vulnerability and disadvantage.[321] That research also shows the level of consideration, engagement and testing required to develop effective consent flows in any given context.

Where children are involved, there is an added layer of complexity relating to each of these requirements. Appropriate information must be provided to both the parent and the child, 'just in time' consent may be inappropriate if a young child may be left alone with the service, the question of capacity is complex, and children may be more susceptible to coercive factors. There is also the additional challenge of appropriately dividing decision rights between parents and children and allowing that division to evolve as a child develops.[322] These challenges are less apparent for older children who can make their own privacy choices, and for very young children who rely entirely on their parents.

We consider that the general level of maturity in the design of consent flows for children, particularly in the middle years (around 9–14), is low. We have been unable to identify any clear examples of best practice in this area. However, in terms of defining best practice, we consider that the ICO Age Appropriate Design Code presents the best synthesis of the literature covering developmental stages and needs as it relates to the design of privacy notifications and consent for different age groups. We cover that guidance in detail in response to questions 2d and 2e below.

---

[321] Data61, *Consumer Data Standards: Consent Flow* (2019) <https://consumerdatastandards.gov.au/wp-content/uploads/2019/07/Phase-2-CX-_-Stream-1-_-Consent-Flow.pdf>.

[322] We surveyed the range of parental controls offered by the dominant digital platforms in section 1c (iv), and will further discuss the role for and challenges associated with reliance on parental consent in section 2c.

(vii) **Recommendations and implementation**

Recommendation 1

Subject to the results of further consultation with stakeholders, the existing standard under the Privacy Act and OAIC guidance should be maintained. That would apply:

- the cut-off age of 15 for a rebuttable presumption with respect to capacity; and
- the ordinary standard for the quality of consent, which requires that the individual must have capacity, and consent must be informed, voluntary, current and specific.

Recommendation 2

The Code should further clarify that consent is considered 'only valid if it is reasonable to expect that individuals to whom an organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting.'

This also recommended as an economy-wide measure.

Recommendation 3

The Code should require that digital platforms take a risk-based approach to age assurance; for example, by requiring reasonable steps proportionate to the nature and risks of the processing activities.

We consider that these requirements could be implemented through a Code as additional requirements linked to APPs 3, 6, 7 and 8. We would support these requirements also as an economy-wide measures.

In practice, an age of consent below 15 could be adopted by a digital platform if it could justify that the nature of the processing is such that it is reasonable to expect a younger child to understand. This could be done through a PIA. Digital platforms could limit the complexity and invasiveness of data practices and adopt more effective transparency measures in order to support younger users. Adoption of a younger age could be supported by effective transparency measures (discussed below).

In practice, we anticipate that digital platforms and other online organisations would need to establish mechanisms for age assurance and by which parental consent may be sought for children under 15 (discussed below). We suggest use of the term 'age assurance' as a broad term to refer to the spectrum of methods that can be used to assure a user's age online with differing levels of confidence.[323] By contrast, age verification typically refers to the establishment of an individual's age to a very high level of confidence, usually requiring identity verification as well. Requiring an appropriate level of age assurance allows

[323] Government Communications Headquarters (UK), Department for Digital, Culture, Media and Sport (UK) and Home Office (UK), *VoCO (Verification of Children Online) Phase 2 Report* (November 2020) 12 <https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report>.

companies and users to jointly choose from a range of measures that are suited to specific risks and service needs.

Mechanisms for age verification may be constructed based on a wide range of information sources, each with their own set of trade-offs with respect to confidence and privacy. For example, age verification mechanisms might rely on:[324]

- official data sources such as central databases, government issued identity documents, or other trusted data sources
- user reported information, which could be sourced from parents, children or peers
- automatically generated indicators, which could be derived from body metrics (such as a user's physical movements or interactions with a device), environmental data (such as the type of device used), behavioural data from app use, or static biometrics from the user.

Research has shown that combining several age assurance methods relying on different data sources can enhance a platform's level of confidence about a user's age over time, and technical trials conducted in the UK have demonstrated that reliable, safe and unobtrusive age assurance is achievable. However, technology in this field is far from mature. At present, platforms overwhelmingly adopt simplistic age-screening mechanisms which rely exclusively on the user self-asserting their age, placing responsibility for attesting age onto the child.[325] This is ineffective, and incentivises children to lie in order to bypass restrictions or parental consent requirements.

The recent Australian Parliamentary inquiry into age verification for online wagering and online pornography provides a comprehensive summary of the attributes of an effective online age-verification model, and the current state-of-the-art methods for age verification.[326] While the technology now exists to support more effective age assurance, more work is required to establish technical standards and develop more mature age assurance solutions.

Because of this, Regulation should avoid codifying specific methods or processes for age verification at this stage, but should seek to incentivise industry to continue to develop more effective ways to identify children and tailor their products and services. We anticipate that rising regulatory standards with a continuing emphasis on risk-based age assurance will drive the market towards better technical approaches for effective, non-invasive age assurance.

We recommend requiring organisations to adopt a risk-based approach to age assurance. For lower risk services such as media streaming, it may be appropriate to accept a high degree of uncertainty as to users' age, whereas higher risk services, such as a dating app,

---

[324] See data source type taxonomy outlined in: Government Communications Headquarters (UK), Department for Digital, Culture, Media and Sport (UK) and Home Office (UK), *VoCO (Verification of Children Online) Phase 2 Report* (November 2020) 17 <https://www.gov.uk/government/publications/voco-verification-of-children-online-phase-2-report> 17.
[325] Ibid, 2.
[326] Australian Parliament, House of Representatives, Standing Committee on Social Policy and Legal Affairs, *Inquiry into and report on age verification for online wagering and online pornography,* <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification>.

should require a higher degree of age assurance. This would be similar to the approach adopted under GDPR — guidance from the European Data Protection Board requires that information society services make reasonable efforts to verify that the user is over the age of digital consent, and that these measures be proportionate to the nature and risks of the processing activities.[327]

Digital platforms could assess and select the most appropriate age assurance mechanisms for a service as part of their PIA process.

[327] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* (4 May 2020) 27 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

Question 2c — Are there risks associated with the parental/guardian consent model? How can meaningful consent be obtained from parents/guardians?

Key findings:

Using parental consent to enable children to access the online environment raises the same problems as the consent model more generally. Due to the complexities of the data environment, parents are often not able to understand the conditions they are agreeing to, and this same problem applies equally to parents providing consent on behalf of their children.

(i) Overseas approaches

COPPA adopts a risk-based approach to the consent requirement. It imposes more stringent obligations on service providers who make invasive use of personal data (eg. disclose it to third parties, employ behavioural advertising, or allow children to publicly post information). More limited measures suffice in the case of services that use children's data for internal purposes. There are also limited exceptions to the requirement to provide notice or to obtain verifiable parental consent prior to data collection.[328]

Where a provider's data handling falls into the high-risk category, parents must provide verified consent using one of five FTC-specified methods, including:

- sign a provided consent form and send it back to the operator via postal mail, fax or electronic scan
- use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder
- call a toll-free number staffed by trained personnel
- connect to trained personnel via a video conference, or
- provide a copy of a form of government issued ID, which is checked against a database and where the parent's ID is promptly deleted after verification.[329]

An operator that does not 'disclose' children's personal information to third parties or the public can avail itself of the less burdensome 'E-mail Plus Method'. Under this method, a consent by email is sufficient, provided it is coupled with some additional assurance that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or fax or phone number from the parent and confirming the parent's consent by letter, fax or phone call.[330]

---

[328] 16 C.F.R. §312.5 (c). The exceptions are limited with regard to the reasons for data collection, the kind of information collected and the purposes for which the collection information may be used.
[329] 16 C.F.R. §312.5 (b) (2) (i)–(v). See for detail above text accompanying note X.
[330] 16 C.F.R. §312.5 (b) (2)(vi).

There are also a handful of safe harbour programs which provide other approved methods for obtaining parental consent.[331] These safe harbour programs are self-regulatory regimes approved and overseen by the FTC, which contain notice and consent mechanisms that are at least as stringent as the COPPA requirements.[332]

In California, the CCPA provides verified consent methods that are largely equivalent to the five methods contained in the COPPA rule, although, in line with the CCPA's broader scope, in-person communication is added as a possible consent mechanism.[333]

Article 8(2) of the GDPR particularly adds that the 'controller shall make reasonable efforts to verify […] that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology'. Unfortunately, this wording provides little guidance on the meaning of 'verify', leaving it largely up to the controller to assess what constitutes reasonable efforts to obtain verification. It would appear that the controller needs to make efforts in relation to ascertaining both that the consent has been given or authorised by an adult, rather than the child, and that the adult was the holder of parental responsibility. The European Data Protection Board provides limited further elaboration by saying that such a proportionate approach should have regard to the risk involved in data processing and that the verification process itself, in line with Article 5(1)(c) of the GDPR (data minimisation), should itself not lead to excessive data collection and processing.[334]

(ii) Risks associated with parental/guardian consent model

There are a number of difficulties and risks associated with the parental/guardian consent model.

The general weakness of the notice and consent model

First, it is based on an assumption that parents and guardians are better able to assess the consequences of providing consent than children. This might be correct insofar as adults tend not to suffer from the age-based vulnerabilities that affect children. However, it is by now well-established that the complexity of the modern data flows and uses makes reliance on a notice-and-consent model difficult for all consumers, whether they are children or adults.[335] These difficulties are aggravated under the prevailing notice and consent mechanisms, where the information provided is often unduly long, convoluted and difficult to understand. Children and parents may labour under the same lack of clarity regarding the benefits and risks of digital applications. If a parent, as much as a child, does not read a privacy policy because they find it too long or too complicated, or because they have no real choice but to accept it to use a service, it may make little difference to the protection whether it is the parent or the child who presses the consent button – unless a parent decides to

[331] 16 C.F.R. §312.5 (b) (3). See the list of approved safe harbor organisations at Federal Trade Commission, *COPPA Safe Harbor Program*, <https://www.ftc.gov/safe-harbor-program>.
[332] Hoofnagle (n 211) 207-8.
[333] California Consumer Privacy Act Regulations, California Civil Code § 999.330.
[334] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679 (GDPR)*, May 2020, [135] and [145].
[335] ACCC *DPI Final Report* (n 3).

withhold consent. The parent/guardian consent model therefore shares many of the shortcomings that are identified generally for notice and consent models.

Unrealistic expectations regarding the digital literacy of parents or guardians

Second, there is the added risk that parents may lack digital literacy in relation to applications and services used by their children. Ofcom, the UK communications' regulator, reports relatively low levels of awareness amongst parents regarding the minimum age rules for leading social media platforms.[336] Even more concerningly, parent surveys also revealed that a quarter of parents with a child between 5–15 years of age say they would allow their child to have a social media profile before reaching the required minimum age.[337] A separate study, conducted at Oxford University into parents' awareness of data protection policies of mobile apps, made three key findings:

1. Parents commonly associated privacy risks with access to the Internet, exposure to inappropriate content, in-app adverts, or strangers. However, their knowledge of personal data collected by mobile apps is low.

2. Parents often think their children are too young to understand privacy risks online and delay these conversations with their children. As a result, children often rely on their parents' guidance to cope with unknown risks, and they [are] not always capable of recognising personal privacy-related risks.

3. When children do seek help from their parents, parents do not necessarily fully understand the risks themselves. Existing privacy safeguarding technologies mainly focus on enabling content control and offer little choices for raising parents' awareness of personal data collection risks or supporting their children's learning.[338]

These findings suggest that many parents have difficulty in making appropriate privacy choices for their children and in supporting children to become privacy-aware and digitally literate. The authors of the study consider the usefulness of 'better support for parents to scaffold their children's ability of recognising and coping with online privacy risks, particularly those associated with implicit personal data tracking'.[339] However, the opacity of modern data collection practices, as well as structural information and power imbalance between app providers and consumers, cannot be fully counteracted through providing better support to parents. They may need to be addressed through changes in data collection and usage practices themselves.

---

[336] Ofcom, *Children and Parents: Media Use and Attitudes Report 2019* (4 February 2020) <https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf> 260–1 ('*Media Use and Attitudes Report')*. Only 27% of parents participating in the survey knew the minimum age requirement for Facebook, followed by 20% for Instagram, 15% for Snapchat and 5% for WhatsApp.
[337] Ibid, 18.
[338] Jun Zhao, 'Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?' — KOALA Project Report 2 <https://arxiv.org/pdf/1809.10944.pdf> (emphasis in original).
[339] Ibid, 1.

Circumvention of parental consent requirements

A third problem with relying on parental consent mechanisms, at least in their current form, relates to their effectiveness. It is well known that children circumvent age restrictions to gain access to particular sites that they wish to join, and that parents are often complicit in either helping their children to join or not stopping them from using the sites to which they have got access, even if this is in violation of the site's restrictions.[340] Ofcom reports that more than half of UK children have a social media profile by the age of 12,[341] although most platforms set a minimum age of 13 years. There are a number of unintended consequences of imposing age restrictions that are then insufficiently enforced. These include that parents, and possibly children, misunderstand their purpose and their status as terms of service. A further consequence is that under-age users appear to providers as older than they are, with the result that they are exposed to content that may not be age-appropriate or otherwise missing out on child- (or teen-) specific protections.

The digital divide between parents

A fourth problem is that 'adults' are themselves not a coherent group, where all members share a similar level of ability, experience and interest in issues of children's privacy. Some cohorts of parents face considerably more challenges than others when confronted with the responsibility to make informed decisions in the digital environment. For example, evidence from the US suggests that the children of parents without college degrees are at higher risk of privacy violations from digital apps than those of parents with higher degrees.[342] This raises the concern that the level of a child's protection may significantly depend on the educational and socio-economic status of their parents. The authors of the US study explain that there appears to be a positive correlation between the level of educational attainment and the degree of digital savviness or privacy awareness, and that more educated parents may undertake more research into the privacy risks before installing an app for their children.[343] These explanations are supported by broader research into the 'digital divide', according to which people with higher levels of education are more likely to use the internet for information and research[344] and are more likely to engage in active (safety) mediation of their children's internet use.[345]

(iii) **Conclusions**

Taken together, these findings suggest that reliance on parental consent mechanisms may be a problematic way of protecting the privacy of children online.

---

[340] Ibid.
[341] Ofcom, *Media Use and Attitudes Report* (n 336) 19.
[342] Beata Mostafavi, 'Some Children at Higher Risk of Privacy Violations from Digital Apps', *MHealth Lab* (8 September 2020 <https://labblog.uofmhealth.org/health-tech/some-children-at-higher-risk-of-privacy-violations-from-digital-apps>.
[343] Fangwei Zha, Serge Egelman and Heidi M Weeks, 'Data Collection Practices of Mobile Applications Played by Preschool-Aged Children' (2020) 174(12) *JAMA Pediatrics online* (8 Sept 2020) <https://jamanetwork.com/journals/jamapediatrics/article-abstract/2769689>.
[344] Alexander JAM van Deursen and Jan AGM Van Dijk, 'The digital divide shifts to differences in usage' (2014) 16(3) *New Media and Society* 507 <http://dx.doi.org/10.1177/1461444813487959>.
[345] Sonia Livingstone et al. (2011), *EU Kids Online: final report 2011* (EU Kids Online, London, UK) <http://eprints.lse.ac.uk/45490/1/EU Kids Online final report 2011%28lsero%29.pdf> 35.

Parents are faced with similar dilemmas whether they decide on their own or their children's privacy. They need to balance the promise of convenience, information and entertainment of digital apps against the trades off that may affect privacy, safety and security. While some parents may prefer to err on the side of better privacy, safety and security, an overly risk-averse approach may have the consequence that their children may miss out on some of the opportunities that arise from the digital environment.

In conducting this research, several operational privacy leaders were interviewed about their experiences in managing the privacy risks and obligations unique to children in Australia and abroad. Interviewees commonly expressed the view that parents play an important role in setting privacy controls until a child reaches capacity, but cautioned against taking the role of the parent too far. One noted that helicopter parenting can interfere with a child's development and their ability to recognise and manage risks, autonomy, and trust. Another interviewee noted that there is a natural transition stage at which parents and children may be mutual decision makers. Their view was that any future code must cater for this transitional stage, where there may be overlap between the parent and child as decision makers.

Just as in the offline environment, not all risk is bad, because responsible risk-taking is part of making experiences and growing up. Research shows that digitally literate children take more risks and come to less harm. A survey into parent attitudes on Facebook use by pre-teen children found that: 'when it comes to online privacy and safety issues, parents are not interested in approaches that lead to curbing children's access but rather in approaches that provide more support for their involvement in children's decision-making process while treating access as a given'.[346]

This calls for a multi-faceted approach that seeks to improve the digital agency of parents and children alike. Parents need to be enabled to make the privacy choices that they consider best for their families, drawing on a robust framework of knowledge and competencies. When data processing is supposed to be based on parental consent, then the information provided to them needs to put them in a position to make an informed decision. More broadly, parents are expected to facilitate digital literacy in their children and support them in becoming competent users themselves – and also need support in doing so.

Even with greater support to develop digital literacy, a regulatory framework that relies heavily on parental consent cannot fully address some fundamental problems, which include the digital divide between parents and the general weakness of the notice-and-consent model. Regarding digital consent, it is as true for privacy protection, as it is for many other aspects of life, that children depend on their parents' concern, skill and motivation for their safety and well-being. This dependency is more accentuated in a parental/guardian consent model, which routinely leaves many decisions on children's privacy in the hand of parents. These problems can be reduced in models that rely more heavily on corporate accountability and make particularly problematic privacy-invasive practices a 'no-go' zone or require justification on grounds other than parental consent. As discussed in response to question 2f below, measures could include an overall requirement for fair, lawful and reasonable

---

[346] danah boyd, Eszter Hargittai, Jason Schultz & John Palfrey, 'Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act"' (2011) *First Monday* 16(11) <https://doi.org/10.5210/fm.v16i11.3850>.

handling of personal information, high privacy default settings, stronger data minimisation standards with respect to children, and limitations on nudging, and profiling.

Questions 2d and 2e — What constitutes effective notification for children? Are there particular measures should be adopted for children of different ages? How could privacy policies be effectively tailored to apply to children?

Key findings:

The length and complexity of privacy policies and notices are a barrier to children just as they are to adults. In addition to this, children need specific modes of communication to ensure they understand and engage with the information that is being given to them. Research has shown that although they struggle with 'standard' social media platform privacy policies, older children and teens are easily able to understand simplified privacy policies that have specifically been drafted for children.

Privacy transparency for children should aim for more than mere disclosure of material facts. It should aim to educate, empower and enable privacy self-management, accounting for a child's developing needs and capabilities.

Children are not equipped to bear responsibility for reading and understanding disclosures (however simply drafted), nor is it reasonable to expect them to have the cognitive ability and background knowledge to understand how a disclosed act or practice is likely to impact them.

The onus should be on platforms to help children to understand and contextualise privacy disclosures by:

- using the most effective tools and strategies for clear communication
- taking into account children's specific needs, vulnerabilities and contexts, and
- adopting design practices for privacy disclosures that involve children and ensure their effectiveness.

(i) What constitutes effective notification for children?

Information Design – Tools and strategies for clear communication

As a starting point, effective notice must be drafted in a way that facilitates understanding and is presented in a way that effectively engages its audience. This is a baseline requirement for all forms of communications about privacy (including consents, notices of collection and privacy policies) for adults as well as for children. There are many resources, and a broad consensus from regulators, academics, industry and others around the world, covering the basics for effective communication about privacy – see, for example, guidance

from the OAIC,[347] OPC of Canada,[348] UK ICO,[349] Article 29 Working Party,[350] IAPP,[351] FTC,[352] and others.[353]

The same challenges of designing disclosures about complex products are faced in other industries, including insurance,[354] utilities[355] and telecommunications,[356] and there is a substantial body of behavioural insights research aimed at understanding the ways in which consumers in those industries engage with disclosures, and how their presentation might be improved.[357] Learnings from that research are incorporated in the discussion below, but more work is needed to understand and explore the ways in which consumers process privacy notices in their daily lives.

Still more generally, the fields of legal design and information design address the challenge of organising and displaying information in a way that maximises its clarity and understandability for the reader.[358] Research groups such as the Legal Design Lab at Stanford Law School work on redesigning the ways parties interact and legal concepts are

---

[347] *APP Guidelines* (n 293) ch 1 and 5; Office of the Australian Information Commissioner, 'Guide to Developing an APP Privacy Policy' (5 May 2014) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/>; Office of the Australian Information Commissioner, 'Mobile Privacy: A Better Practice Guide for Mobile App Developers' (5 September 2014) <https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/>.

[348] Office of the Privacy Commissioner of Canada, 'Guidelines for Obtaining Meaningful Consent' (May 2018) <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

[349] Information Commissioner's Office (UK), 'Right to Be Informed', *Guide to the General Data Protection Regulation (GDPR)* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/>.

[350] Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679* (wp260rev.01) (11 April 2018) ('Guidelines on Transparency').

[351] International Association of Privacy Professionals, 'Organizational Privacy Policies', *IAPP Resource Centre* <https://iapp.org/resources/topics/organizational-privacy-policies/>.

[352] Federal Trade Commission, '.Com Disclosures - How to Make Effective Disclosures in Digital Advertising', Report (March 2013) <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf>.

[353] Ari Ezra Waldman, 'Privacy, Notice, and Design' (2018) 21 *Stanford Technology Law Review* 129; Ingrida Milkaite and Eva Lievens, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies' (2020) 14(1) *Journal of Children and Media* 5; Anca Micheti, Jacquelyn Burkell and Valerie Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand' (2010) 30(2) *Bulletin of Science, Technology & Society* 130.

[354] See generally Senate Economics References Committee, *Australia's General Insurance Industry: Sapping Consumers of the Will to Compare* (Parliament of Australia, 10 August 2017) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Generalinsurance/Report> ch 3.

[355] Australian Energy Regulator, 'Retail Pricing Information Guidelines 2018' (23 April 2018) <https://www.aer.gov.au/retail-markets/guidelines-reviews/retail-pricing-information-guidelines-2018>.

[356] Australian Communications and Media Authority, 'Critical Information Summaries', Web page (16 September 2019) <https://www.acma.gov.au/critical-information-summaries>.

[357] Oxera Consulting, *Review of Literature on Product Disclosure* (Financial Conduct Authority, 29 October 2014) <https://www.fca.org.uk/publication/research/review-of-literature-on-product-disclosure.pdf>.

[358] Helena Haapio and Stefania Passera, 'Visual Law: What Lawyers Need to Learn from Information Designers', *Legal Information Institute Blog* (15 May 2013) <https://blog.law.cornell.edu/voxpop/2013/05/15/visual-law-what-lawyers-need-to-learn-from-information-designers>.

communicated around the needs of the user, and these approaches are gaining traction in Australia.[359]

In very broad terms, best practice in all these fields converges on the same toolbox of strategies and techniques. These general strategies are also identified by children themselves when questioned about how privacy policies or online terms and conditions could be improved.[360] Many are covered in OAIC guidance.[361] They include the following matters.

Clear and plain language

Clear and plain language should be used, such as short sentences, active tense, avoiding jargon and defined terms,[362] using concrete and definitive language, avoiding abstract or ambivalent terms which leave room for different interpretations (such as 'may' or 'might').[363] The vocabulary, tone and style of the language should be appropriate to and resonate with children of the target age, so that the child addressee recognises that the message is being directed at them.[364]

As well as avoiding jargon, notifications should be sensitive to terminology that may confuse or mislead children who are less familiar with the internet or app ecosystems, clarifying or avoiding terms where a child's lay understanding may differ. An example of this is when 'private' data is accessible to a parent or the platform operator, or when 'deleted' information remains recoverable for a period of time, or when app data will not be deleted along with the app itself.[365]

A study conducted by the UK Children's Commissioner in 2017 showed how Instagram's Terms and Conditions could be redrafted as a one-page, child friendly document that could be easily understood by a test group of children aged 13–17.[366] The Children's Commissioner has also published simplified Terms and Conditions for Facebook, Snapchat, WhatsApp and YouTube as an educational tool for use in UK schools, designed to be an accessible, child-friendly way to help children understand their digital rights and make

---

[359] Catriona May, 'How Better Design Can Improve the Law', *Melbourne Law School News* (22 November 2019) <https://law.unimelb.edu.au/alumni/mls-news/issue-22-november-2019/how-better-design-can-improve-the-law>.
[360] Information Commissioner's Office UK, *Towards a better digital future* (n 255) 52.
[361] Such as Office of the Australian Information Commissioner, *Guide to Developing an APP Privacy Policy* (May 2014); Office of the Australian Information Commissioner, *Mobile Privacy: A Better Practice Guide for Mobile App Developers* (n 347).
[362] Office of the Australian Information Commissioner, *Guide to Developing an APP Privacy Policy* (ibid).
[363] ACCC *DPI Final Report* (n 3) 405; Article 29 Working Party (n 373) 8.
[364] Article 29 Working Party, *Guidelines on Transparency* (n 350). For an example of child friendly language and presentation, see UNICEF, 'UN Convention on the Rights of the Child in Child Friendly Language' (UNICEF) <https://sites.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf>.
[365] Livingstone, Stoilova and Nandagiri, *An Evidence Review* (n 14) 23.
[366] Children's Commissioner, *Growing up Digital – A Report of the Growing Up Digital Taskforce* (January 2017) <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf> 8–12 ('Growing Up Digital').

informed choices.[367] This work shows that it is possible to design simplified privacy notices for younger audiences.

Structural and other design features

Structural features that improve understanding include the use of headings, breaking up text into paragraphs, ordering topics in a logical way, and keeping related information together rather than scattered throughout the document.[368]

Other design elements that aid comprehension include visual features such as use of font, colour and indentation to aid readability, as well as display of icons, visualisations, infographics and charts.[369] In addition to making content more engaging and readable, these elements can help to convey to children that the message is being directed at them.[370]

Layering is recommended by most privacy regulators as well as in other industries, and was noted as a beneficial approach by the ACCC.[371] An effective multi-layered notice should set out a concise summary of the most important information for consumers in an easily digestible first layer, with links to more detailed information.[372] A multi-layered notice will not be effective if it fails to draw attention to important or unexpected information immediately for the user.[373]

Alternative timings and modes of delivery

Alternative modes of delivery should also be considered, both in terms of the notification itself (audio, video, or even structured learning or tutorials) as well as its timing. Privacy information may be provided at the point where a decision is made, or when personal information is collected, used or disclosed. Other information may be provided at the user's convenience, for example where a privacy dashboard draws together all relevant choices and information into a single location for easy ongoing management. Importantly, privacy information can also be provided through means other than text, such as a light or icon to indicate a camera or microphone is active, or even through the look and feel of the interface itself – a button or section of a site coloured red warrants more caution than one coloured green.

---

[367] UK Children's Commissioner, 'Simplified Social Media Terms and Conditions for Facebook, Instagram, Snapchat, YouTube and WhatsApp' (29 September 2017) <https://www.childrenscommissioner.gov.uk/report/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/>.
[368] Micheti, Burkell and Steeves (n 353) 131.
[369] Ibid 132.
[370] See, for example, various examples of the UN Convention on the Rights of the Child in child-friendly language: <https://www.unicef.org/sop/convention-rights-child-child-friendly-version>; <https://www.unicef.ca/sites/default/files/imce_uploads/UTILITY%20NAV/TEACHERS/DOCS/GC/CRCPosterEN_FA.pdf>; <https://sites.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf>; <https://plan-international.org/sites/default/files/field/field_document/child-friendly_crc_poster_a4_-_final_-_english.pdf>. Compare these with the look and feel of YouTube Kids' notice for children: <https://kids.youtube.com/t/noticeforchildren>.
[371] ACCC *DPI Final Report* (n 3) 485.
[372] Article 29 Working Party (n 373) [8], [11], [17].
[373] ACCC *DPI Final Report* (n 3) 406.

Where notification is directed at children, consideration should be given to modes of delivery that may be particularly accessible to children, such as video, comics or animations. Examples of privacy communications through alternative modalities include the ICO's video privacy policy,[374] The Guardian's video privacy policy,[375] an educational comic developed by OPC Canada,[376] and various animations and other resources in the *My data and privacy online* toolkit produced by the London School of Economics and Political Science with funding from the ICO.[377]

The most effective timing and modality will differ depending on the user ages and the service in question. For very young children, who may be signed up by parents and left alone, the best approach may be to provide upfront privacy information aimed at parents, combined with much simpler just-in-time contextual information targeted at the child user.[378]

Consistency and comparability

Consistency and comparability of notifications across a range of products is a feature that is less commonly emphasised in relation to privacy, but which is central to other disclosure regimes. Research in relation to financial services disclosures shows that it is important that any specific disclosure be considered within the general information 'landscape' of all the disclosures with which a consumer is likely to be presented.[379] In that context, it is common for disclosures to be required to adhere to a common format, with common terminology and key metrics placed at the same location within a summary statement, all as defined by the regulator. An example of standardised language for privacy can be seen in the Consumer Experience Standards for the Consumer Data Right, which mandate terms for describing data 'clusters' or categories and specific data types to ensure consistent use across different CDR implementations.[380]

Consistency of terminology and structure across privacy policies and notifications would assist readers to understand the comparative and cumulative privacy effects of using different services, decrease the burden associated with assessing the privacy effects of each new service, and enable users to navigate quickly to the matters that they care about the most. For children in particular, consistency would significantly aid accessibility and understanding.

The use of standardised definitions in privacy notifications is endorsed by the ACCC in its Digital Platform Inquiry final report:

---

[374] Information Commissioner's Office, *ICO Layered Privacy Notice*, Video (25 May 2018) <https://www.youtube.com/watch?v=ZqzGM8nUsDo>.
[375] Scriberia, *Why Your Data Matters to Us – Guardian Animation* (8 November 2016), Video <https://www.youtube.com/watch?v=P9-5vzbjxtQ>.
[376] Office of the Privacy Commissioner of Canada, 'Social Smarts - Privacy, the Internet and You' (2017) <https://www.priv.gc.ca/media/3609/gn_e.pdf>.
[377] London School of Economics and Political Science, 'My Data and Privacy Online - A Toolkit for Young People', Web page <https://www.lse.ac.uk/my-privacy-uk>.
[378] 5Rights Foundation, '5Rights Foundation's Response to the Information Commissioner's Call for Evidence – Age Appropriate Design Code' <https://5rightsfoundation.com/uploads/5rights-final-call-for-evidence.pdf> 14 ('Response').
[379] Oxera Consulting (n 357) 17–19.
[380] Data61, *Consumer Experience Guidelines* (2020) <https://consumerdatastandards.gov.au/wp-content/uploads/2020/08/CX-Guidelines_v1.4.0.pdf> 19.

Standardised definitions could be particularly useful for consumers to describe types of third parties to whom information may be provided. For example: media companies, data analytics firms, or market research companies.

Examples of standardised categories that could be useful to develop for consumers in order to more clearly identify the types of purposes for which a digital platform could use a consumer's data could include: 'market research and product development'; 'diagnostics and troubleshooting'; 'personalised advertising', or 'personalised services'.

Providing clear differentiation between categories would be particularly beneficial for consumers to assist in understanding the purpose in which their data may be used by a platform. For example, the ACCC considers that there is an important distinction between 'personalised services' and 'personalised advertising'; especially for businesses which consider providing an individualised experience an important part of the service they provide.[381]

Addressing the factors that make children vulnerable

As outlined in response to question 1a, there are a range of factors that make children vulnerable. Effective notice should be designed to address these vulnerabilities.

Background knowledge and literacy

Effective notification should address children's limited background knowledge and literacy. Depending on the age of the child, organisations should assume that they do not understand:

- the commercial basis on which services are provided to them or the business models which support those services
- that data will be passively collected in addition to the data that is provided
- that their data will be combined with information from other sources and used to infer further details about them
- that their data will be used and shared for other purposes and by other organisations.

As we have discussed above, children will understand privacy primarily in terms of interpersonal relations and the active sharing of data.[382] This should be the starting point for the design of communications, and organisations should actively seek to correct for misconceptions and misplaced anticipations that may flow from this mental model. Examples of this include:

---

[381] ACCC *DPI Final Report* (n 3) 487.

[382] See, eg, Maria Stoilova, Sonia Livingstone and Rishita Nandagiri, *Children's data and privacy online: Growing up in a digital age – Research Findings* (London School of Economics and Political Sciences, 2019), 43–44 ('Research Findings').

- Many younger children have been taught that explicit permission must always be obtained before sharing a person's photo or other details online. As a result, they may assume that the same norm will apply in relation to data held by an online service provider.[383]
- Children expect the tactics, workarounds and deceptions (such as false names, secret accounts, 'private browsing', deleting history/messages) that protect their privacy from friends, parents and teachers also apply with companies.[384] As a result, they tend to over-estimate their ability to hide their own identity or activities.

Cognitive capacity and maturity of judgement

As previously established, children are often unable or unwilling to think through the short- and long-term consequences of their privacy decisions. Therefore, where it is known that the target audience will be unable to reason effectively about the content of the notification and its impact on them, additional care should be taken to spell out any potential impacts. That is, in addition to the fact of the collection, use or disclosure privacy notifications to children should spell out the most important *consequences* of that collection, use or disclosure. This would be consistent with the position adopted by the Article 29 Working Party in relation to the principle of transparency under the GDPR that:

> for complex, technical or unexpected data processing … controllers should also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject? [385]

Human-centric design and testing

Human- (or user-) centric design refers to an iterative design process that focuses on understanding the needs, capabilities and behaviours of the target audience, and seeks to design explicitly to accommodate those needs, capabilities and ways of behaving.[386] The need for more human-centric design in privacy transparency is widely acknowledged.[387] Effective notification for children should be iteratively designed and tested with its target

---

[383] Information Commissioner's Office UK, *Towards a better digital future* (n 255) 50.
[384] Stoilova, Livingstone and Nandagiri, *Research Findings* (n 382) 18; Information Commissioner's Office UK, *Towards a better digital future* (ibid) 50.
[385] Article 29 Working Party, *Guidelines on Transparency* (n 350) [10].
[386] Victorian Government, Department of Premier and Cabinet, 'Human-Centred Design Playbook' <https://www.vic.gov.au/human-centred-design-playbook>; Don Norman, *The Design of Everyday Things* (Basic Books, 2013) 7; see also International Organization for Standardization, 'ISO 9241-210:2019: Human-Centred Design for Interactive Systems' (International Organization for Standardization, July 2019) s 3.7 <https://www.iso.org/standard/77520.html>; NSW Government, 'Human-Centred Design Toolkit' (November 2017) <https://www.finance.nsw.gov.au/sites/default/files/policy-documents/hcd_toolkit.pdf>.
[387] Centre for Information Policy Leadership and Telefonica, *Reframing Data Transparency* (Centre for Information Policy Leadership, 30 June 2016) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/reframing_data_transparency.pdf> 9; Waldman (n 353).

audience to ensure that it most effectively applies the tools and strategies available to accommodate the needs, capabilities and behaviours of children in the specific context in which the notice will appear.

OAIC guidance on APP 1.3 and APP 5 indicates that the standard required depends on the circumstances of the collection and the needs of the individual. That is, the content of the obligation to 'take reasonable steps to ensure awareness' or to provide a 'clearly expressed' privacy policy is determined by the context and characteristics of the notice recipient. Other jurisdictions apply similarly human- or user- centred standards around transparency and consent.[388]

Privacy regulation in Australia and elsewhere does not mandate design, testing or any particular approach to the creation of notifications. However, guidance from regulators often includes recommendations to engage relevant experts in the design of communications as well as consultation and testing with the target audience. For example, the OAIC recommends engaging public relations expertise in the development of an organisation's privacy policy and testing it on target audiences.[389] Similarly, guidance from the Article 29 Working Party suggests controllers might test user interfaces, notices or privacy policies 'through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies'.[390] Relevantly, the principle of accountability under the GDPR requires that a controller be able to demonstrate that personal data are processed in a transparent manner. Documented testing, trialling of different modalities and feedback from target audiences would assist data controllers to meet this obligation.[391]

Direct engagement with children in relation to matters that affect them is also consistent with the *Convention on the Rights of the Child*, which provides for the child's rights to be heard,[392] and to receive information.[393]

The ACCC, in the final report of its Digital Platform Inquiry, also recommends consumer testing to measure the effectiveness of various forms of notification and express opt-in consent, noting that there is a wealth of behavioural economics literature on the ways in which the presentation of information (in relation to financial services) can influence consumers' understanding of an issue and their behaviour.[394] The ACCC also notes successful work commissioned by the Association of Super Funds of Australia and the European Commission to understand and explore ways of improving consumers comprehension of product disclosure statements and terms and conditions.[395]

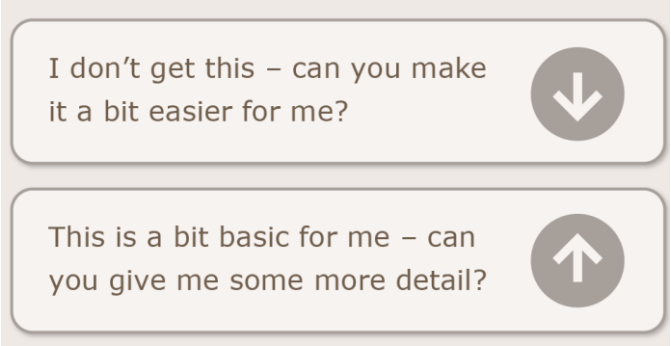
---

[388] See, eg, Article 29 Working Party, *Guidelines on Transparency* (n 350) [1].
[389] Office of the Australian Information Commissioner, *Guide to Developing an APP Privacy Policy* (n 370).
[390] Article 29 Working Party, *Guidelines on Transparency* (n 350) [9].
[391] Ibid 14.
[392] UNCRC (n 292) art 12.
[393] Ibid art 13.
[394] ACCC *DPI Final Report* (n 3) 487–8; Oxera Consulting (n 357).
[395] Ibid 488.

(ii) Are there particular measures that should be adopted for children of different ages?

Aside from age, there are several other factors that influence privacy literacy, and children's development can vary based on their individual characteristics and personal circumstances.[396] In many cases, a child's understanding, ability to engage and think critically about privacy issues appears to be more dependent on the child's parents and school experience rather than their age.[397] The design goal should be an approach to notification and transparency that meets each child's individual needs, understandings and circumstances.

As a starting point, the development of children's understanding of privacy can be roughly mapped against age groups, and notifications can be tailored to the specific needs of each group. However, flexibility should be offered to the user to adjust the complexity of the material being presented to them, to account for both the significant variation between children within and across age groups, as well as the difficulty of precisely determining the age of any particular user. For example, a service provider could incorporate mechanisms to allow a child or parents to choose which version of a notification that they see, and shift up or down the scale of complexity depending on their individual level of understanding:[398]



There is significant literature covering developmental stages and needs, much of which is covered in previous sections. The following summarises aspects of those stages as they relate to the design of privacy notification for different age groups. The following specific recommendations for each age group draw mainly on the ICO Age Appropriate Design Code, which presents a good synthesis of the body of research on how to provide privacy information and seek consent at various ages.[399]

[396] Livingstone, Stoilova and Nandagiri, *An Evidence Review* (n 14) 17.
[397] Information Commissioner's Office UK, *Towards a better digital future* (n 255) 14.
[398] Information Commissioner's Office UK, *Age appropriate design code of practice* (n 254) '4. Transparency'.
[399] Ibid.

Pre-literate & early literacy (0-5)

Children in this age group are entirely reliant on parents, and their digital use is limited to adult-guided activities or limited autonomous activities within walled gardens or video platforms.[400]

Privacy notifications and policies should be targeted at parents and provided at sign-up and on demand. Privacy settings should be established by parents on sign-up or via 'parents-only' dashboards. As children may be left alone with a device, reliance on consent or contextual notifications should be limited. Any communication directed at the child should be by audio or video. If important information needs to be conveyed, or a decision needs to be made about privacy settings, children should be prompted to get help from a parent or trusted adult.

Core primary school years (6-9)

Children in this age group are becoming more able to understand and comply with rules and requirements around online privacy and may have encountered information about risks from parents or at school. However, their general awareness remains limited, and they have few strategies for managing risk.[401] Understanding, capacity for critical thinking and ability to engage with privacy messages remains limited.[402] Digital use is expanding and may involve independent communication with family and commercial third parties, but remains primarily within limited 'walled gardens'.[403] Almost half (46%) of Australian children aged 6–9 own their own device.[404]

A key objective for this age group should be to assist children to begin the transition to independent use of technology. As before, privacy options, notifications and policies should be targeted at parents and provided at sign-up and on demand. However, services could also provide educational materials for children, explaining basic online privacy concepts, how the service works and how to be in control of their own information. Services could also provide resources for parents to use with their children to explain privacy concepts and risks as they relate to the service.

As before, reliance on contextual notifications and decisions should be limited and any communication directed at the child should be primarily audio or video. Privacy settings should be established by parents on sign-up or via 'parents-only' dashboards. If important information needs to be conveyed, or a decision needs to be made about privacy settings, children should be provided a simplified explanation but still prompted to get help from a parent or trusted adult.

---

[400] Beeban Kidron and Angharad Rudkin, *Digital Childhood – Addressing Childhood Development Milestones in the Digital Environment* (December 2017) <https://5rightsfoundation.com/static/Digital_Childhood_report_-_EMBARGOED.pdf> 14.
[401] Stoilova, Nandagiri and Livingstone, Systematic evidence mapping (n 14).
[402] Kidron and Rudkin (n 400) 16.
[403] Ibid 14.
[404] OAIC Community Attitudes Survey (n 310) 92.

Transition years (10-12)

Children of this age are more likely to have a personal device and increased digital autonomy, though parents and families still tend to be the main source of influence. Digital use expands to a broader range of activities including open communication and sharing across a range of sites including games and social media. Social relationships are becoming more important, and children increasingly use the online environment to explore and develop their self-identity.[405]

For this age group, privacy notifications and policies should be provided for both parents and children, in formats suitable to each. Children should be provided with both written and audio/video options and should be given the choice to access materials developed for older or younger audiences. As before, privacy settings should be established by parents on sign-up or via 'parents-only' dashboards. Children should be prompted to discuss notifications with a parent or other trusted adult if they have any concerns or do not understand.

Teens (13-15) and approaching adulthood (16-17)

Teens and young adults are increasingly independent, experimental, and reliant on online environments in all aspects of their lives, including the exploration and development of their self-identity.[406]

Younger teens should begin to be empowered to make their own privacy decisions relating to matters they are more likely to understand, such as interpersonal sharing. More complex consents, such as for profiling or targeted advertising should still be referred to parents until at least age 15.

(iii) How could the existing APP 5 standard apply to children?

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards.

OAIC guidance in relation to APP 5 makes it clear that the standard required depends on a range of factors relating to the circumstances of the collection as well as the knowledge and needs of the individual.[407] Judicial consideration of APP 5 is limited, but OAIC guidance has been affirmed in the Australian Administrative Appeals Tribunal:

> The assessment of what constitutes 'reasonable steps' must be influenced by the nature of the information itself, the likelihood of the user's awareness of the collection, the nature and extent of the collector's collection explanations, the nature and potential utility of any invitation to request further information, and the disclosed purposes of information use.[408]

---

[405] Kidron and Rudkin (n 400) 18.
[406] Ibid 20–23.
[407] *APP Guidelines* (n 293) [5.3]–[5.6].
[408] *Freelancer International Pty Ltd and Australian Information Commissioner* [2017] AATA 2426, [72].

In 2014, the Australian Information Commissioner determined that the onus lies with the organisation to show that steps taken are reasonable given the knowledge and awareness of an individual:

> In order to meet the requirements of NPP 1.3, it is not sufficient for Telstra to assume that the complainant knew that his personal information would be published in the White Pages unless he requested a silent line feature. Telstra bears the onus of showing that the complainant was aware that it was Telstra's usual business practice to disclose phone line information in the White Pages.[409]

Neither OAIC guidance nor APP 5 itself deal specifically with children, and we were unable to identify any judicial consideration of the matter. The APP Guidelines do note that 'any special needs of the individual' should be taken into account in determining what steps are reasonable, and that 'more rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters'.[410]

'Reasonable steps to notify' is arguably a lower standard than 'reasonable steps to ensure awareness'. An obligation to notify is discharged when that notice is given, provided it is in a form that is accessible and intelligible by the individual. An obligation to ensure awareness may go further, requiring an organisation to consider whether the individual is likely to, or has in fact, read the notice, and possibly to adopt additional measures as required to effectively convey the relevant information.

In view of the vulnerability and need for special protection of children, the standard of 'reasonable steps to ensure awareness', as expected under APP 5, would generally be high. For a well-resourced, global digital platform whose services are targeted to or used by children, the standard that might reasonably be expected is higher still. As such, it may be argued that such platforms' existing obligations under APP 5 require them to take considerable care in designing effective privacy notifications for children, including taking steps to ensure that they:

- adopt appropriate design practices for privacy transparency measures, which take into account the needs, capabilities and behaviours of children of varying ages who may use their service, and which include consultation and testing to ensure effectiveness
- tailor notification content, style, mode of delivery and timing to be effective for all users, and offer a version or versions of the notification that are appropriate for the variety of ages and abilities of individuals whose information will be collected
- consider significance of the collection in terms of the possible adverse consequences for children at various stages of development, and present privacy notifications in a manner that reflects that significance (i.e. by emphasising higher risk or unexpected practices), and

---

[409] *DK and Telstra Corporation Limited* [2014] AICmr 118, [32]. See also *APP Guidelines* (n 293) [B.104]–[B.109].
[410] *APP Guidelines* (ibid) [5.4].

- are able to demonstrate why the organisation considers the steps taken were reasonable in the circumstances (including by measuring and reporting on how many users review privacy information or access privacy settings).

These requirements could be included in a code as an explicit, granular set of additional requirements under APP 5 along the lines of those outlined above. This would have the benefit of providing a clear set of mandatory requirements around design, testing, consultation and reporting. However, it may be overly prescriptive to dictate these matters, and may result in significant compliance costs if, for example, organisations were required to undertake a full design, consultation and testing process for even minor updates to a notification.

Our preferred approach would be for the code to set an enhanced general obligation under APP 5, which could be given content through guidance materials. This recommendation is discussed in more detail below.

(iv) Are additional or different requirements necessary?

Globally, regulatory action on transparency issues is increasing, though so far we observe little change in behaviour. For example:

- The Data Protection Commission of Ireland is investigating whether Facebook meets GDPR Transparency requirements in its provision of Instagram to children.[411]
- The French data protection authority recently fined Google for violating transparency obligations in relation to ad personalisation.[412]
- In 2019, the Privacy Commissioner of Canada criticised Facebook for 'overbroad and conflicting language in its privacy communications'.[413]
- The US FTC's record $5bn settlement with Facebook last year was principally in relation to inadequate and misleading disclosures.[414]

In Australia, the OAIC's proceedings against Facebook about the 'This is Your Digital Life' App turn in part on Facebook's failure to adequately inform affected Australian individuals of

---

[411] Data Protection Commission, 'Data Protection Commission's Two Statutory Inquiries into Facebook's Processing of Children's Data on Instagram (Opened in Sept 2020)', Press release (19 October 2020) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commissions-two-statutory-inquiries-facebooks-processing>.
[412] Commission Nationale de l'Informatique et des Libertés, 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC', Web page (21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.
[413] Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia, *Joint Investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia – Report of Findings* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>; ACCC *DPI Final Report* (n 3) 405–6.
[414] Federal Trade Commission, 'FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making' Blog (24 July 2019) <https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history>.

the manner in which their personal information would be disclosed.[415] Regulatory action by the ACCC under the Australian Consumer Law resulted in HealthEngine being ordered to pay $2.9m in penalties for misleading conduct in relation to the sharing of patient personal information,[416] and the ACCC has commenced proceedings against Google in two separate transparency-related matters.[417]

Notwithstanding increased regulatory attention, the current framework has not been effective in driving transparency sufficient for Australian children to understand and self-manage their privacy online. In the absence of detailed guidance or enforceable standards, APP entities have ample discretion regarding their approach to APP 5 compliance. This can lead to a significant gap between best practice and what can be justified as reasonable. There is substantial evidence that in practice, privacy notifications from digital platforms are far from effective, even for adults.

One of the key barriers for children and adults is the sheer volume of information that is presented to them. The OAIC's *Australian Community Attitudes to Privacy 2020* Survey found that just 1 in 5 Australians (20%) both read privacy policies and are confident that they understand them.[418] The main reason cited for not reading privacy policies were their length (77%) and their complexity (52%), with younger Australians being most likely not to read policies because they were too long.[419] This finding is supported by research conducted for the UK Information Commissioner's Office, which found that the more information children were given, the harder they found it to engage with the process and make decisions about what was and was not an acceptable trade-off:

> The way the information is presented, the assumption that it has to be accepted, and the lack of understanding about what it really means, all combine to create a situation

---

[415] OAIC, 'Concise Statement – Australian Information Commissioner v Facebook Inc' (Federal Court of Australia, 9 March 2020) <https://www.oaic.gov.au/assets/updates/news-and-media/facebook-federal-court-concise-statement.pdf>.

[416] Australian Competition and Consumer Commission, 'HealthEngine to Pay $2.9 Million for Misleading Reviews and Patient Referrals', Media release, (20 August 2020) <https://www.accc.gov.au/media-release/healthengine-to-pay-29-million-for-misleading-reviews-and-patient-referrals>.

[417] Australian Competition and Consumer Commission, 'ACCC Alleges Google Misled Consumers about Expanded Use of Personal Data', Media release (27 July 2020) <https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data>; Australian Competition and Consumer Commission, 'Google Allegedly Misled Consumers on Collection and Use of Location Data', Media release (29 October 2019) <https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data>.

[418] OAIC Community Attitudes Survey (n 310) 69–70.

[419] Ibid. Further, it is likely that self-reported numbers are exaggerated, as empirical studies show significantly lower proportions (in one study, less than 1 in 1000) reading privacy policies and license agreements in detail: Yannis Bakos, Florencia Marotta-Wurgler and David R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (2014) 43(1) *Journal of Legal Studies* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443256>; Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' [2018] *Information, Communication & Society* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465>.

where the sheer volume of information disempowers children, providing them with a seemingly binary choice between using and not using a service.[420]

An examination of the length and readability of privacy policies for Instagram, TikTok and Snapchat found that only Snapchat provided any privacy information in a format accessible to their youngest users – see Table 1.[421]

Table 1 – Length, format and readability of privacy policies[422]

	Length in words	Hyperlinks to follow	Visuals	Format	Readability
Instagram	4471	90	White spaces Bullet points Bold headings	Plain text	Difficult 18–19 years
Snapchat	3889	32	White spaces Bullet points Bold headings	Plain text	Fairly difficult 15–17 years
Snapchat Summary	763	14	7 illustrations Bigger headings Shorter paragraphs	Plain text	Fairly easy 11–13 years
TikTok	3329	4	White spaces Bullet points Bold headings	Plain text	Difficult 18–19 years
TikTok Summary	413	0	Part of the main privacy policy, not easy to distinguish	Plain text	Difficult 17–18 years

Studies conducted with children show that they are just as confused and disheartened by privacy disclosures as adults. Research conducted for the UK Information Commissioner's Office found that most children reported that they never read terms and conditions, despite most feeling that they *should*, and many wanting to learn more about how their personal information is used.[423] Another study, conducted by the UK Children's Commissioner, tested children's comprehension of the Terms and Conditions of Instagram and found that 'after 20 minutes of reading the 13 year olds had only got halfway through the current Terms and Conditions and were begging to be allowed to stop'.[424] However, the same kids were readily able to understand a one-page summary of the same terms and conditions, which had been deliberately drafted to clearly set out their rights in a way that was accessible to them.[425]

The same set of deficiencies in digital platforms' disclosure practices are documented in the ACCC DPI Final Report, including that policies and notices:

- are often long, complex, vague and difficult to navigate
- use different definitions for key terms such as personal information, which do not accord with user expectations or the Privacy Act

[420] Information Commissioner's Office UK, *Towards a Better Digital Future* (n 255) 14.
[421] Milkaite and Lievens (n 362) 13–14.
[422] This table is taken from ibid 14.
[423] Information Commissioner's Office, *Towards a better digital future* (n 255) 52.
[424] Children's Commissioner, *Growing Up Digital* (n 366) 8–12.
[425] Ibid.

- permit a range of data practices of particular concern to consumers, such as location tracking online tracking for targeted advertising, and third party data sharing, though often in understated or ambiguous language.[426]

Recommendation 16(b) of the ACCC DPI Final Report is that notification requirements be strengthened by removing entities' discretion as to whether and how to notify customers (i.e. what steps are reasonable) in favour of a requirement that all collection of personal information be accompanied by a notice, unless the customer already has the information or there is an overriding legal or public interest reason. The ACCC also recommend additional requirements that notifications must:

- be concise, transparent, intelligible and easily accessible, written in clear and plain language, and provided free of charge
- clearly set out how the APP entity will collect, use and disclose the consumer's personal information, and
- be written at a level that can be readily understood by the minimum age of the permitted digital platform user.[427]

For digital platforms, the ACCC additionally recommends that:

- notifications be layered, and that the Code set out a baseline requirement for the content of each layer
- standard language is defined and mandated for describing key matters, such as the types of third parties to whom information might be provided, and types of purposes for which information might be used or disclosed.[428]

(v) Recommendations and implementation

Recommendation 4

The Code should adopt the ACCC recommendation 16(b) for strengthened notification requirements. This would include an expansion of the APP 5 matters to include clear statements of how the organisation will use and disclose the consumer's personal information. We also support the ACCC recommendation for further work to be done on standardised language, templates, icons or other tools for privacy transparency.

ACCC recommendation 16(b) should also be adopted as an economy-wide measure.

Recommendation 5

The Code should further expand the APP 5 matters to include how users can report concerns, exercise their rights, or use any other privacy self-management tools available to them (such as how to use account privacy settings or turn off profiling, targeted advertising or location tracking).

---

[426] ACCC *DPI Final Report* (n 3) 421–422.
[427] Ibid 461.
[428] Ibid 485.

Recommendation 6

The Code should strengthen APP 5 so that digital platforms must take reasonable steps to ensure awareness of the APP 5 matters in their users, **in addition to** providing notice per ACCC recommendation 16(b).

Recommendation 7

The Code should require organisations to collect evidence of the extent to which users engage with privacy notifications and use privacy features. Organisations should be able to demonstrate the reasonableness of steps taken.

Recommendation 8

Guidance should make clear that certain steps are presumed to be reasonable with respect to ensuring awareness of the APP 5 matters, including:

- considering and designing for the needs, capabilities and behaviours of various user groups (such as children and other vulnerable groups)
- offering versions of notices appropriate for different groups
- embedding information and indicators within a service.

The strengthened notification measures proposed by the ACCC would be beneficial, but still place primary responsibility for understanding and engaging with privacy information on the user. As long as the information has been provided in the appropriate format, nothing else is required from the entity. For children (and other vulnerable groups), we do not consider that this strikes the right balance between organisational accountability and enabling self-management.

A greater onus should be on the platforms — not just to provide information about their practices in an accessible way, but to provide resources as well as ongoing support and guidance, and to design their services in such a way that people of all ages and abilities can use them safely.

Additionally, one-off, text-based notifications on sign-up for a service are unlikely to be effective in bringing key matters to a user's attention, however clearly worded or structured. As outlined above, alternative timings and modes of delivery for privacy information are important to enable understanding and engagement, particularly in younger children. Rather than exhaustively covering everything up front, children will benefit from platform providers providing privacy information in bite-sized chunks, embedded into the experience of the service itself. The growing prevalence of Internet of Things devices, including smart toys and home assistants, further underscores the need for ongoing, transparency about data handling that is built into the product experience itself.

As such, in addition to the general measures to strengthen notification requirements proposed by the ACCC, online platforms should be subject to an ongoing obligation to take reasonable steps to ensure children's awareness of:

- the matters outlined in the notice and privacy policy (including how their personal information is being collected, used and disclosed); and
- how they can report concerns, exercise their rights, or use any other privacy self-management tools available to them.

Guidance should give content to this new obligation without being prescriptive as to specific measures that an organisation must implement. Emphasis should be on encouraging inclusive and evidence-based design processes that produce notices and design features for privacy transparency that are effective for all users, regardless of their specific needs, vulnerabilities and behaviours. The ICO Age Appropriate Design Code provides detailed guidance, drawing on a wide evidence base, on the key considerations with respect to the evolving interests, needs and capacity of children.[429] The Consumer Experience work stream for the CDR Consumer Data Standards provides a good example of how a program of consumer experience research can be deployed from exploratory research through to prototype testing to understand consumer expectations, needs and behaviours in a given field.[430]

A new obligation to collect evidence of user engagement with privacy policies, notifications and features would support enhanced organisational accountability, and drive ongoing research and development.

These recommendations would significantly raise the bar for APP 5 compliance. Digital platforms would be required to review existing privacy notices and policies to ensure they comply with enhanced requirements as to content and clarity. Digital Platforms would likely also need to establish ongoing programs linked to design and user-experience functions to ensure that platform features make it clear to users (explicitly or intuitively) how their personal information is being collected, used and disclosed. A good example of how this may look in practice can be seen in IKEA's app design implementing their new 'Data Promise'.[431]

However, we consider that these obligations are broadly consistent with transparency obligations under the GDPR, and so would not constitute a substantial new regulatory burden for organisations. Transparency requirements in the GDPR apply throughout the life cycle of processing and require organisations to adopt the most appropriate measures and modalities for providing information, taking into account user experience and testing.[432] The approach is also consistent with the ICO Age Appropriate Design Code, which requires organisations to 'provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated'.[433]

---

[429] Information Commissioner's Office UK, *Age appropriate design code* (n 254) 'Annex B: Age and developmental stages'.
[430] Data61, 'Consumer Experience Reports', *Consumer Data Standards* <https://consumerdatastandards.gov.au/engagement/reports/reports-cx/>.
[431] IKEA, *The New IKEA Data Promise Gives Privacy and Transparency to Customers* (30 January 2020) <https://www.youtube.com/watch?v=j1MsEl9cTRc>.
[432] Article 29 Working Party, *Guidelines on Transparency* (n 350) 7–13, 14.
[433] Information Commissioner's Office UK, *Age appropriate design code* (n 254) '*4. Transparency'*.

Question 2f — What additional restrictions could be imposed to mitigate the risks and harms associated with the handling of children's personal information?

(i) Considerations

Children have a right to privacy, and to be free from economic exploitation. To the extent that these rights are balanced with other legitimate competing interests, the established tests of reasonableness, necessity and proportionality should apply.

Respect for the best interests of the child should be a primary consideration in the formulation of any additional restrictions.[434] Children's best interests when using digital platforms and spaces encompass more than simply protecting them from harm. Participation, autonomy and agency are key objectives alongside safety. Without the agency needed to participate and exercise rights, children can neither take advantage of the opportunities digital media afford, nor develop resiliency when facing risks.[435] There is strong public support for this policy goal, with 82% of parents agreeing that 'children must be empowered to use the internet and online services, but their privacy must also be protected'.[436]

The OAIC's regulatory approach is built on four key pillars – enabling privacy self-management, organisational accountability, global interoperability and a contemporary approach to regulation. Regulation should balance self-management and organisational accountability in the best interests of the child. That balance should reflect children's varying capabilities and development needs (including the need for agency) and allocate responsibility for the protection of children's rights and interests appropriately between organisations, parents and children themselves. Responsibility for protecting a child's rights and interests should never lie with the child alone.

As we explore in response to questions 3 and 4, similar considerations apply to the protection of vulnerable adults online. Our view is that the best way to protect both groups is to adopt strong but flexible baseline protections for all adults and children, combined with specific enhanced protections or requirements for specific groups that may not be adequately protected by the baseline requirements. This approach also lowers the likelihood that children or certain groups may be excluded by platforms seeking to avoid heightened compliance obligations (as we have seen with COPPA).

(ii) General protections

Fair, lawful and reasonable information handling

Recommendation 9

[434] 'Convention on the Rights of the Child' art 3 <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>.
[435] Amanda Third et al, *Children's Rights in the Digital Age* (Unicef, September 2014).
[436] OAIC Community Attitudes Survey (n 310) 94.

The Code should establish an overriding obligation to handle personal information in a manner that is lawful, fair and reasonable.

This obligation could be enacted in the Code as an additional requirement linked to APPs 3, 4, 6 and 7.

We recommend this also as an economy-wide measure.

Recommendation 10

The Code should also set out a non-exhaustive list of factors to be considered in determining whether a collection, use or disclosure is fair and reasonable in the circumstances, including:

- where the personal information of a child is being processed, whether the processing is in the best interests of that child, and
- any foreseeable privacy harms that could result from processing and any measures that could be taken to prevent them.

The Privacy Act allows organisations a broad discretion to collect, use and disclose personal information, provided that the information is 'reasonably necessary for, or directly related to, one or more of the entity's functions or activities' (APP 3.1), the means of collection is lawful and fair (APP 3.5), and that the individual is notified of the purpose of the collection (APP 5). Beyond this, there is no obligation on organisations to balance their commercial interests with individuals' privacy interests.

There is a critical need for some mechanism by which individual interests are better balanced against the commercial interests associated with information handling. This need is particularly acute in relation to children and vulnerable groups, who are more exposed to privacy risk and less able to manage harms as they materialise.

There are a number possible approaches to achieving greater balance, which may be applied individually or in combination. The ACCC DPI report presents a market-based mechanism, recommending enhanced transparency and consent requirements to address the existing imbalance of information and bargaining power between consumers and organisations.[437] This, in turn, is anticipated to enable individuals to better manage their own privacy and drive more equitable exchanges. While these recommendations may go some way towards empowering consumers across the economy, we anticipate that this approach will have the least impact among the most vulnerable – particularly children, or those consumers who lack the technical, critical and social skills to engage with the internet in a safe and beneficial manner, or those with reduced levels of resilience or self-control.

Peter Leonard presents an alternative approach more focused on organisational accountability, which would establish a new legislated standard of care by reference to defined privacy harms.[438] This would require APP entities to define and implement a

[437] ACCC *DPI Final Report* (n 3) 461–470.
[438] Peter G Leonard, *Privacy Harms – A Paper for the Office of the Australian Information Commissioner* (June 2020).

comprehensive privacy program to identify, mitigate and manage privacy risks to individuals. This is a promising approach but would require substantial amendment to the Privacy Act.

A third approach would be to establish an overriding obligation to handle personal information in a manner that is lawful, fair and reasonable. This would be similar to article 5(1) of the GDPR, which requires that personal data be 'processed lawfully, fairly and in a transparent manner', and to the 'reasonable purposes' requirement in section 5(3) of the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA).[439]

An obligation of this type would require organisations to examine whether information processing is appropriate in all the circumstances, and to balance their own commercial interests with the privacy interests of individuals. The Code could set out a range of factors to be taken into account, which should include any foreseeable privacy harms that could result from processing, any measures that could be taken to prevent them, and where personal information about children is involved, whether the handling is in the best interests of the child.[440]

Guidance should provide further detail about the capabilities and vulnerabilities of children and the types of practices that present the greatest risk, and should require that the best interests of children be a 'primary consideration' in accordance with article 3 of the UNCRC. Guidance should also provide a framework for assessing and weighing the best interests of the child, such as that:

- Privacy risks or impacts to children should only be accepted as reasonable if they can be justified as necessary and proportionate against a legitimate competing interest (such as the rights of others).
- It would be unlikely that the commercial interests of an organisation would outweigh a child's right to privacy.
- Children's interests should be construed broadly and understood to vary with age, but include safety from exploitation risks; health and wellbeing; physical, psychological and emotional development; rights to freedom of association and play; support for disabilities; recognition of the role of parents and giving appropriate weight to a child's own views.

We consider that such a duty presents the most efficient and effective means of establishing a balance between organisational and individual interests. It also allows for a variable standard of protection to be applied for children and other vulnerable groups. (Factors to be taken into account for vulnerable groups are outlined in response to question 4e below.)

Though new to Australian law, similar obligations already exist in Canada and the EU. Organisations in those jurisdictions incorporate this assessment into routine PIA processes, and the same could readily be done here.

---

[439] Section 5(3) of the PIPEDA is discussed in detail in section 4a(v).
[440] Other factors that could be included for the protection of other vulnerable groups are discussed in section 4e below.

Privacy Impact Assessments

Recommendation 11

The Code should require digital platforms to conduct a Privacy Impact Assessment (PIA) for all online products and services, and for all new products and services prior to launch.

The OAIC strongly encourages APP entities to undertake Privacy Impact Assessments (PIAs) as a matter of course.[441] Though not strictly mandatory, in some circumstances a PIA may be a reasonable step to implement practices, procedures and systems that will ensure compliance with the APPs, and so may be required under APP 1.2. Australian government agencies are required under the *Privacy (Australian Government Agencies — Governance) APP Code 2017* to conduct a PIA for all 'high privacy risk projects'.[442]

Digital platforms by their nature involve a range of high-risk practices, including large scale information collection and profiling, online tracking, geo-location, collection of biometric data and other sensitive information, and integration of diverse data sets. Considering the scale and penetration of digital platforms it may be assumed that most if not all products and services will involve the processing of personal information of children or other vulnerable groups. Given the heightened risk of harms faced by children and vulnerable groups online, set against the scale and resources of digital platform operators themselves, one would expect that PIAs should be undertaken as a matter of course.

A PIA should assess compliance with the APPs and the Code, including the obligation to handle personal information in a manner that is lawful, fair and reasonable. It should be a holistic assessment and response to privacy impacts and risks, holding the best interests of the child as a primary consideration, and taking into account differing ages, capacities and development needs.[443]

The ICO Age Appropriate Design Code includes an overriding requirement that the best interests of the child should be a primary consideration in the design and development of online services to be accessed by a child.[444] We would support such a requirement in Australia, but consider that it is beyond what is achievable in a privacy code. As such, we recommend incorporating consideration of children's best interests in the context of a PIA.

The approach of requiring a PIA for online services offered to children is consistent with GDPR, which requires a Data Protection Impact Assessment to be conducted where processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.[445]

---

[441] Office of the Australian Information Commissioner, 'Guide to Undertaking Privacy Impact Assessments' <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>.
[442] Meaning any project likely to have a significant impact on the privacy of individuals: *Privacy (Australian Government Agencies – Governance) APP Code 2017* section 9.
[443] This is based on the ICO Age Appropriate Design Code (n 254), Standards 1 and 2.
[444] ICO Age Appropriate Design Code (ibid), Standard 1.
[445] GDPR art 35(1).

High-privacy default settings

Recommendation 12

The Code should require that platforms and services are set to the highest privacy settings by default. High-privacy default settings should cover both user-to-user privacy settings (such as who can see activity or posts) and user-to-platform privacy settings (such as profiling, location tracking, or targeted advertising).

This is based on ICO Age Appropriate Design Code, Standard 7, and eSafety Commissioner, *Safety by Design* Principle 2: User empowerment and autonomy.

Research in behavioural economics shows that when people are presented with a pre-selected option, they are significantly more likely to select that option – particularly in consumer contexts where the default choice is conveyed as either a recommendation or the status quo.[446] This is often referred to as the 'default effect'. The default effect is particularly powerful for settings and defaults that remain 'under the hood' and are not presented to users as choices to be made.[447] An investigation by the Norwegian Consumer Council in 2018 found that Facebook, Google and Microsoft all employed privacy intrusive default settings, many of which were obscured or difficult to find and change.[448]

It is important to distinguish between user-facing and platform-facing controls. Requirements as to privacy protection by default should be clearly defined to apply to both. Digital platforms often emphasise privacy settings that give a user control over what is shown to other users, without necessarily changing the amount of user data that is collected by the digital platform or available to third parties such as advertisers.[449] Parents surveyed in the development of the ICO Age Appropriate Design Code were considerably more likely to support high-privacy defaults for user-to-user functions (such as 'letting other site users contact your child' (78% support) or 'letting other site users see when your child is online' (76% support)) than user-to-platform functions (such as 'suggesting personalised or targeted content' (48% support)).[450] A majority of UK parents nevertheless thought 'using location to make recommendations' and 'suggesting personalised or targeted adverts' should be off by default.[451]

Requiring high-privacy default settings would contribute to user awareness and control. As a practical matter, this requirement would likely result in services presenting users with a range of choices as to basic privacy settings and defaults as part of their account creation process — who should see posts, should posts include the user's location, can data be shared or used for advertising, and so on. Where possible, choices should be able to be

---

[446] Jon M Jachimowicz et al, 'When and Why Defaults Influence Decisions: A Meta-Analysis of Default Effects' (2019) 3(2) *Behavioural Public Policy* 159.
[447] For example, an analysis of Microsoft Word users showed less than 5% of users changed any settings at all: Jared Spool, 'Do Users Change Their Settings?' <https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/>.
[448] Forbrukerrådet, *Deceived by Design* (n 189).
[449] ACCC *DPI Final Report* (n 3) 422–434.
[450] Information Commissioner's Office UK, *Towards a better digital future* (n 255) 31.
[451] Ibid.

deferred or made on a temporary basis.[452] In combination with a prohibition on nudging, strengthened transparency and consent requirements and protections under the Australian Consumer Law, this would contribute significantly to children's awareness and agency in how their data are used and shared. Australian parents overwhelmingly support default privacy settings for children being set to high-privacy (84% support, 3% oppose).

Nudging

Recommendation 13

The Code should prohibit the use of 'nudge' techniques in online platforms which lead or encourage children to provide unnecessary personal data or turn off privacy protections.

This recommendation is based on standard 13 on the ICO Age Appropriate Design Code.

A nudge is 'any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives'.[453] An investigation by the Norwegian Consumer Council in 2018 found that Facebook, Google and Microsoft all employ numerous tactics to nudge or push consumers toward sharing as much data as possible, including: privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, presenting take-it-or-leave-it choices, not permitting choices to be deferred or made on a temporary basis, and generally adopting choice architectures where choosing the privacy friendly option requires more effort for the users.[454]

The ACCC DPI report also recognises the ways in which digital platforms exploit behavioural biases and nudge consumers towards more privacy intrusive settings. These include using defaults and preselection of certain options (discussed above), using framing and presentation to emphasise positives and draw attention away from practices that consumers may not approve of, and hiding privacy options.[455]

Children are particularly susceptible to behavioural manipulation. They lack the background knowledge and cognitive capacity to identify and adjust to manipulative features and are even more vulnerable than adults to the cognitive biases that nudge techniques exploit, such as immediate gratification bias.

Nudge techniques are indirectly regulated through consent requirements and consumer protection laws. Overly aggressive attempts to direct user behaviours might compromise the quality of consent, such that it is not 'voluntary'. In some circumstances, nudge techniques may also contravene consumer protection laws such as the prohibitions on misleading or deceptive conduct and unconscionable conduct. If the ACCC's recommendation for a

[452] Requiring users to complete a settings review at a time determined by the service provider, without a clear option to postpone the process is a common nudge technique to push users into acceptance or to make certain choices: Forbrukerrådet, *Deceived by Design* (n 189) 27–31.
[453] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (Yale University Press, 2008) 6.
[454] Forbrukerrådet, *Deceived by Design* (n 189) 3.
[455] ACCC *DPI Final Report* (n 3) 422–434.

prohibition on certain unfair trading practices were to be implemented, it would also likely restrict some nudge techniques.

Profiling

Recommendation 14

The Code should require that whenever a person is profiled, they must be provided with age-appropriate information explaining the process and its implications for them and be able to express their point of view about their profile.

We recommend this also as an economy-wide measure.

Recommendation 15

The Code should establish a presumption that profiling of children for advertising or other commercial purposes is not fair or reasonable.

Profiling is defined under article 4(4) of the GDPR to refer to any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. A similar definition should be adopted under the code.

Profiling is ubiquitous in today's online environment. It is the key technology that drives personalisation of content, including the advertising that funds free online services. It shapes what we see, how we consume content and how we engage with each other. But it poses significant privacy risks, particularly for children:[456]

- **Profiling is often highly privacy invasive**. Deeply personal information (such as emotional states, sexual preferences and personality traits) can be inferred from seemingly unimportant data traces, by processes that are highly opaque and beyond the control of the individual. This is particularly harmful for children, who often lack awareness of both profiling and the data traces that support it.[457]
- **Profiling can lead to discrimination**. Profiling makes assumptions about the prospects and preferences of children based on factors beyond their control, and is often applied without adequate oversight, transparency or accountability. For example, profile-driven advertising on Facebook has been shown to display job ads for truck drivers to men, despite the company working actively restricting its algorithm from considering gender when finding audiences for the ads.[458]
- **Profiling is particularly risky for children**. Personalisation of the information and experiences of children based on their assumed interests and preferences limits autonomy and may be harmful to development. At best, over-personalisation can

[456] See generally, Privacy International, *Data is power: Profiling and automated decision-making in GDPR* (2017).
[457] See, eg, Stoilova, Nandagiri and Livingstone, Systemic Evidence Mapping (n 14); Information Commissioner's Office UK, *Towards a better digital future* (n 255) 50.
[458] Ava Kofman and Ariana Tobin, 'Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement', *Pro Public*a (Web Page, 13 December 2019). See also, Piotr Sapiezynski et al, 'Algorithms That "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences' [2019] arXiv preprint arXiv:1912.07579.

lead to filter bubbles which may prevent children from discovering or exploring new things. At worst, it can perpetuate discriminatory stereotypes.

- **Children are particularly susceptible to behavioural advertising.** Children are particularly susceptible and more easily influenced by behavioural advertising.[459] Advertising can have significant impacts on children's behaviour, in ways that children are not aware of.[460]

Australian parents also show strong support for restrictions on profiling and targeted advertising for children (83%), and for children's right to grow up without being profiled or targeted (84%). Only one in five (21%) Australian parents say they are comfortable with businesses targeting ads to children based on information they have obtained by tracking a child online. A similar proportion (23%) say they are comfortable with businesses inferring sensitive information about a child.

Limitations on profiling and targeted advertising are likely to be strongly opposed by industry. Advertising is the core business of digital platforms, and children are a key market. Behaviourally targeted ads have been shown to be significantly more effective and are heavily relied on by marketers.[461] Criticism may include that limiting profiling and targeted advertising will compromise the funding model for platform services used by children, thereby decrease their quality, limiting user choice and/or increasing the cost of services. Limiting profiling for non-advertising purposes may be said to decrease the quality and relevance of content presented to children.

This restriction is broadly consistent with the ICO Age Appropriate Design Code, other than the restriction on targeted advertising. It goes further than the GDPR, which restricts solely automated decision-making which produces legal or similarly significant effects and requires 'specific protection' for marketing to and profiling of children.

The right to erasure

Recommendation 16

The Code should provide for a right to withdraw consent for processing and set specific requirements for digital platforms to action such requests. For example, to cease any processing and to delete any information collected or retained on the basis of consent or reasonable expectation of the individual, unless another permissible purpose applies.

We also recommend this or a full right to erasure as an economy-wide measure.

---

[459] Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (wp251rev.01) as last Revised and Adopted on 6 February 2018 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> 19 ('Guidelines on Automated individual decision-making').

[460] Francisco Lupiáñez-Villanueva et al, *Study on the Impact of Marketing through Social Media, Online Games and Mobile Applications on Children's Behaviour* (London School of Economics and Political Science, March 2016) <https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en>.

[461] IHS Markit, *The Economic Value of Behavioural Targeting in Digital Advertising* (2017) <https://datadrivenadvertising.eu/wp-content/uploads/2017/09/BehaviouralTargeting_FINAL.pdf>.

We do not consider that a GDPR-style right to erasure could be effectively implemented as part of a Code. However, we anticipate that such a right would be of value to children if implemented as part of economy-wide reforms. However, a more limited right to withdraw consent for processing could be included.

This would differ from a full right to erasure as it would only have effect where consent or reasonable expectation is relied on as the basis for collection, use or disclosure. The ability to withdraw consent already exists implicitly under the APPs because once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information.[462] However, establishing a right to withdraw consent through the Code would allow for the setting of specific requirements for the actioning of such a request. For example, the Code could require that requests be processed within a reasonable timeframe, and that organisations take specific steps to review information holdings and delete any information collected or retained on the basis of consent or reasonable expectation, where no alternative basis applies.

The right to erasure is discussed in section 2a above. It is a qualified right to obtain deletion of an individual's personal data in specified circumstances, and subject to certain exceptions. It is broader than a right to withdraw consent, as it may apply to data not processed on the basis of consent. In practice, decisions on requests for erasure can involve a complex balancing of interests between the data subject, the data controller and third parties — particularly where the privacy interests of a child conflict with others' rights to freedom of expression and information, or other public interests. Implementing a suitable framework for balancing competing rights with respect to a request for erasure would be a significant task, and is likely to be beyond the scope of a Code.

A right to erasure or to the withdrawal of consent for processing is a key component of privacy self-management.[463] The ACCC DPI report recommends the adoption of a right to erasure across all APP entities, as a key component of strengthened consent requirements for consumers. The ACCC emphasises the various challenges to a meaningful consent framework for consumers, including platform practices such as bundled consents and take-it-or-leave it terms, as well as the sheer complexity of the information economy itself.

As we have discussed above, relying on consent as a basis for processing poses particularly difficult challenges for children, but at the same time, it is essential that children are permitted (age-appropriate) agency over their online lives, so that they can both take advantage of the opportunities digital media afford, and develop resiliency when facing risks. A strong right to erasure is key to striking the balance between autonomy and protection, particularly for adolescents.

There is broad support for a GDPR-like right of erasure among Australians generally (84% support),[464] as well as among experts and industry, including from some digital platform providers, provided it incorporates or is compatible with existing frameworks.[465]

---

[462] *APP Guidelines* (n 293) [B.51].
[463] Ibid 470–473.
[464] OAIC Community Attitudes Survey (n 310) 67.
[465] ACCC *DPI Final Report* (n 3) 471.

A right to erasure would also be consistent with the CCPA, which includes a similar qualified right to request deletion of data.

(iii) **Specific protections**

Data minimisation

The OAIC has stated that it supports additional privacy safeguards for the handling of personal information of children (and other vulnerable groups) so that collection, use and disclosure is minimised, particularly for targeted advertising and online profiling.[466]

The APPs permit online platforms to collect, use and disclose a wide range of personal information from their users (including children), beyond what is reasonably necessary to provide the functionality of the platform itself.

APP 3 permits the collection of personal information from an individual where 'reasonably necessary for one or more of the entity's functions or activities'. Provided that the collection is not unfair or unlawful and other APP requirements are complied with,[467] APP 3 does not restrict the number or variety of functions or activities for which information may be collected, nor does it require that functions or activities be related to each other or to the interaction in which the information is collected. Once information has been collected for a nominated primary purpose, APP 6 permits its use and disclosure for that purpose.

This leaves APP entities with a very broad discretion to determine for themselves what information they will collect about their users and for what purposes they will use and disclose it. Digital platforms rely on this discretion to collect an ever-widening variety of data about children who use their platforms,[468] and to leverage these collections for marketing and other commercial purposes as 'primary purposes'. Because the purpose for which the data are collected goes beyond the provision of the digital platform, information may also be retained and used even after the associated account is deactivated.

The ACCC DPI report found that this broad discretion significantly undermines consumer control, and permits information to be collected, used or disclosed for purposes not in accordance with the consumer's own interests.[469] The ACCC recommend strengthened consent requirements to address this: that consent be required for any use or disclosure of data other than to supply the consumer with a service or product that they have contracted for.[470] It is likely that the ACCC proposal would be effective in constraining the discretion available to platforms and increase consumer control. It would also move Australia closer

---

[466] Office of the Australian Information Commissioner, 'Digital Platforms Inquiry Final Report — Submission to the Australian Government' (23 September 2019) <https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-final-report-submission-to-the-australian-government/> [59].
[467] And consistent with the other APPs – i.e. the required information is set out in the entity's privacy policy (APP 1), adequate notice of the collection is provided (APP 5) and consent is obtained or an exception applies for collection of sensitive information (APP 3).
[468] Including data about their activities on and off the platform, contact lists, what apps they have installed, and their physical location. See, eg, 5Rights Foundation, *Response* (n 387) Appendix C-Data routinely gathered by popular services.
[469] ACCC *DPI Final Report* (n 271) 465.
[470] Or as required by law, or as necessary for an overriding public interest reason: Ibid.

into alignment with GDPR, though the ACCC proposal is more restrictive in that it would not permit 'legitimate interests' as a basis for processing.

To address the short- and long-term negative consequences of unrestrained collection and sharing of children's data,[471] the following recommendations are directed at establishing a higher standard of data minimisation for children.

Collection

Recommendation 17

The Code should prohibit collection of personal information about children beyond the minimum amount of personal data necessary to provide the elements of a service in which a child is actively and knowingly engaged, or as required by law or for a defined public interest. For younger children, consent should not be available as a basis for collection of personal information beyond the minimum necessary to provide the service. Collection of personal information for profiling and targeted advertising should be presumed to be unnecessary.

Children generally have limited awareness of the ways in which they are tracked or how data can be combined, and instead focus on data that they provide to the apps and services that they use.[472] A data minimisation requirement would more closely align data practices with children's understanding and expectations.

There is very strong support among parents for a general data minimisation requirement (81% support) and even stronger support for data minimisation for technology in schools and educational settings (87%).[473]

This recommendation is based on standard 8 of the ICO Age Appropriate Design Code, and would be more restrictive than the GDPR.

Geo-location data

Recommendation 18

The Code should require that location data is subject to additional protection. Unless necessary to provide elements of a service in which a child is actively and knowingly engaged and except as required by law or for a defined public interest:

- location tracking must be off by default; and
- options which make a child's location visible to others should default back to 'off' at the end of each session.

Recommendation 19

[471] These are discussed in detail in response to question 1b above.
[472] Livingstone, Stoilova and Nandagiri, *Research Findings* (n 382) 22; Information Commissioner's Office UK, *Towards a Better Digital Future* (n 255) 50.
[473] OAIC Community Attitudes Survey (n 310) 94, 96.

Services should also be required to provide an obvious indication when location tracking is active and every time the child's location is used or disclosed to others.

Recommendation 20

Consideration should be given to additional requirements for services that allow for persistent monitoring of or access to a child's location, such as requiring that:

- younger children are only tracked with parental consent, and older children only with their own consent;
- children are aware and regularly reminded that they are being tracked; and
- a list of all persons authorised to monitor the child's location is readily available to both parent and child.

Location tracking is widespread and highly invasive[474] and presents unique and heightened risks for children, but location data is not afforded special protection under Privacy Act. There are obvious risks to physical safety, in that the availability of location data can make children more vulnerable to bullying, physical and mental abuse, abduction, sexual abuse and trafficking. Less obvious risks relate to the impact of persistent monitoring on children's developing sense of self and independence. Location tracking of children by parents is a growing market.[475]

More than two thirds of parents (69%) are uncomfortable with businesses tracking the location of a child without permission, and three quarters (76%) support requiring geo-location tracking to be switched off by default.[476]

This recommendation is draws from standard 10 of the ICO Age Appropriate Design Code, as well as recommendations made by 5Rights Foundation in consultation on the Code.[477] Additional protections such as those outlined above would bring Australia closer into line with jurisdictions such as the EU and US, which treat location data as a special category of data subject to greater protections.[478]

Data sharing

Recommendation 21

The Code should provide that children's data must not be disclosed except as necessary to provide the elements of a service in which a child is actively and knowingly engaged, or as required by law or for a defined public interest. This restriction should apply the same

---

[474] Jennifer Valentino-DeVries et al, 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret', *The New York Times* (10 December 2018) <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>.
[475] See, for example, Melanie Vujkovic, 'More Parents Using GPS to Track Children but Experts Warn There Could Be Consequences', *ABC News* (4 April 2019) <https://www.abc.net.au/news/2019-04-04/digitally-tracking-kids-more-parents-use-devices/10957906>.
[476] OAIC Community Attitudes Survey (n 310) 91, 96.
[477] Based on recommendations made by 5Rights Foundation: 5Rights Foundation, *Response* (n 378) 16.
[478] Stacey Gray, 'A Closer Look at Location Data: Privacy and Pandemics', *Future of Privacy Forum* (25 March 2020) <https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/>.

standard to restrict information collection directly by third parties via cookies or other tracking technologies.

The data sharing and third party tracking ecosystem is opaque and complex.[479] Digital platforms sell, license or exchange data with a variety of third parties, including advertisers and app developers. Platforms may also permit data to be gathered directly by third parties through the use of cookies and other tracking technologies. Third parties may then transform the data, combine it with information from other sources and on-sell data, profiles or analyses to others.

Privacy disclosures do not provide sufficient information to enable user self-management.[480] Privacy policies refer in general terms to information shared with 'partners' and 'advertisers', without detailing who these partners are, what information is shared with them and for what purposes. Further, users have no visibility or control of how their data might be combined, transformed, or on-disclosed by third parties. The ACCC DPI report recommends enhanced information requirements under the Code to address this, including a requirement for multi-layered notification where:

> The final layer should contain all relevant information that details how a consumer's data may be collected, used, disclosed and shared by the digital platform, as well as the name and contact details for each third party to whom personal information may be disclosed.[481]

Improvements in transparency and usability of self-management controls may lower the bar to some degree. However, most children do not have the inclination, background knowledge or capacity required to actively manage such a complex ecosystem. Even with enhanced transparency, self-management is unrealistic for children.

This recommendation is aligned with standard 9 of the ICO Age Appropriate Design Code.

[479] ACCC *DPI Final Report* (n 3) 391–393.
[480] Ibid 418–421.
[481] Ibid 485.

Question 2g — What mechanisms will digital platforms and other online organisations require to comply with proposed additional requirements and protections, and would these mechanisms involve further privacy risks, for example, age verification mechanisms or parental controls?

We have touched on what would be required to comply with our recommendations throughout the discussion above. We do not consider that any of our recommendations would require substantial new mechanisms or processes beyond what is already required under Australian law or in other jurisdictions.

(i) Age verification

As outlined above, we consider that the best way to protect both children and vulnerable groups is to adopt strong but flexible baseline protections for all adults and children, combined with more limited and specific enhanced protections or requirements for specific groups as required. Fewer specific enhanced protections reduces the need to provide separate services or environments for children, meaning that there is less of a requirement on digital platforms to proactively verify the age of specific users, and less likelihood that children or other vulnerable groups will be excluded to avoid enhanced requirements.

The age of users generally (as opposed to the age of a specific user) is relevant in determining whether a particular act or practice is fair, lawful and reasonable. Specific users' age is relevant in determining whether their consent can be accepted as valid, and whether additional restrictions around profiling or data minimisation apply to that user. We consider that profiling of children for the purpose of age assurance and to determine whether these additional protections should apply would be reasonable for the purposes of Recommendations 9 and 15. Recommendation 3 aims to incentivise the development of more robust age verification approaches while at the same time minimising any privacy risk arising from age verification mechanisms themselves by permitting organisations to accept a higher degree of uncertainty as to users' age with respect to lower risk information handling.

(ii) Parental controls

In the context of privacy, parental controls provide a mechanism for separating matters for which a child may make their own decisions from matters where parental authority is required. Beyond privacy, parental controls also play an important role in enabling parents to supervise and protect their children from other harms.

We make no recommendations with respect to parental controls. Recommendation 1 with respect to consent would simply codify the existing position under the Privacy Act and OAIC guidance that digital platforms should seek parental consent for users under age 15. Our recommendations 2-3 would provide flexibility to organisations to accept a higher degree of uncertainty with respect to a user's age, and to accept consent from younger users with respect to simple, low risk information handling.

Question 3 — What other groups may be vulnerable in relation to the collection, use and disclosure of their personal information online?

Question 3a — What other groups may be physically or legally incapable of making their own privacy decisions?

Key findings:

There are no groups of people other than children that are considered physically or legally incapable of making decisions about privacy. The ability to make decisions about privacy needs to be assessed on an individual basis. It is decision-specific and may fluctuate depending on the individual's circumstances.

While some state legislation expressly sets out when a person is considered incapacitated and how incapacity to make privacy decisions should be dealt with, the Privacy Act does not contain equivalent provisions. There is a case for giving the OAIC guidance on these matters statutory effect or otherwise to reform the law to ensure its conformity with the National Decision-Making Principles recommended by the Australian Law Reform Commission.

(i) General considerations

The issue of lack of capacity to make decisions, including privacy decisions, is a complex one. Under the principle of autonomy, everyone should in principle be free to decide their own affairs, without interference by others. Autonomy requires capacity, which is the ability to make decisions for oneself. Every individual of adult age is presumed to have such decision-making capacity, unless there is evidence to the contrary.[482]

Physical incapacity refers to a situation where an individual is unconscious or otherwise incapable of giving consent. Legal incapacity arises where an individual lacks the legal competence to make that decision – in particular where a guardian has been appointed to represent the person. Legal incapacity – in the sense of lack of competence to make a legally binding decision – is the result of some factual incapacity to make decisions with understanding of their effect or to communicate such decisions.

The ALRC discussed the complex relationship between mental and legal capacity in its Equality, Capacity and Disability in Commonwealth Laws report.[483] Mental capacity refers to the cognitive understanding and decision-making ability of a person. The ALRC criticised the use of the concept of 'mental incapacity' in Commonwealth legislation and pointed out that '[l]egal capacity is a different concept from "mental capacity" and should not be confused

[482] *Goddard Elliot (a firm) v Fritsch* [2012] VSC 87.
[483] Australian Law Reform Commission, *Equality, Capacity and Disability in Commonwealth Laws*, Final Report No 124 (August 2014) ('ALRC Equality Report').

with it'.[484] The Commission referred to submissions by People with Disability Australia, the Australian Centre for Disability Law and the Australian Human Rights Centre that any proposal for a uniform approach to legal capacity should remove any notion that the assessment of mental capacity is also an assessment of legal capacity. In its view, these reflected two concerns: 'first, that legal capacity should not simply be *equated* with mental capacity; and, secondly, that people with cognitive impairment should not be assumed to have limited legal capacity, in the sense of being able to exercise legal agency'.[485]

The ALRC's final report contains a set of National Decision-Making Principles that are intended to ensure that all adults have an equal right to make decisions; that persons who require support in decision-making must be provided with access to the support necessary and representative decision-makers are appointed only as a last resort; and that decisions that affect their lives must be directed by their will, preferences and rights of persons direct.[486]

These principles reflect Australia's obligations under the UN Convention on the Rights of Persons with Disabilities,[487] to which Australia is a signatory. Article 12 of this Convention provides that 'persons with disabilities enjoy legal capacity on an equal basis with others in all aspects of life'.

In consequence, other than where an individual is a child, there are **no other groups** that are considered to be physically or legally incapable of making their own privacy decisions.

The assessment of capacity needs to take into account any fluctuations in individuals' circumstances. As explained in a guide on *Privacy and people with decision making disabilities,* issued by the NSW Information and Privacy Commission (IPC):[488]

> A person's capacity may change over time. The ability to make decisions may be affected by factors that are pre-existing or acquired, temporary, episodic or chronic. For example, a person with a mental illness may not be able to make particular decisions during periods of their illness where they are acutely unwell, but may have capacity at other times. A person with dementia may have capacity in the early stages of dementia but lose capacity to make decisions about parts or all areas of their life later on.[489]

The assessment of capacity is also 'decision-specific'. The IPC Guide comments that 'if a person does not have capacity to make decisions about particular types of personal information such as their financial information, they may still have capacity in relation to other kinds of personal information and how their information is collected, used, disclosed or otherwise handled.[117]

---

[484] Ibid, [2.45].
[485] Ibid, [2.47].
[486] Ibid, Recs [3-2]–[3-4].
[487] UN Convention on the Rights of Persons with Disabilities and its Optional Protocol (A/RES/61/106), adopted on 13 December 2006 and opened for signature on 30 March 2007, UNTS 2518, 283.
[488] Information and Privacy Commission NSW, *Guide: Privacy and people with decision making disabilities* (February 2004) ('IPC NSW Guide').
[489] Ibid, 6.

It follows that even persons with severe cognitive disabilities will generally have the ability to make some decisions. If a person has difficulty making or communicating a particular decision, it should first be considered whether the person could make or communicate the decision with adequate and appropriate support. Only if a person is unable to make or to communicate a decision even with such support, that person will be considered to lack capacity.

If a person lacks capacity, someone else will need to make the relevant decisions for them. This substitute decision-maker can be an appointed guardian, some other responsible person or the court. However, it will not be apparent in all cases that a person lacks capacity. Moreover, not every person who lacks capacity will have an appointed representative who can act for them.

(ii) Capacity in privacy legislation

Unlike some state privacy acts, the Privacy Act does not contain a specific provision on capacity. The term 'physically or legally incapable of giving consent' is used in s 16B(5) of the Privacy Act in the context of disclosure of an individual's health information to a person responsible for that individual.[490] The juxtaposition of 'physical' and 'legal' appears at first slightly curious.[491] The APP Guidelines explain physical or legal incapacity in the context of a 'permitted health situation' as follows:

> **Incapacity to give consent**
>
> D.33 An individual may be 'physically or legally incapable of giving consent' if they cannot understand the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. Issues that may affect an individual's capacity to give consent include:
>
> - age
> - physical or mental disability
> - temporary or incremental incapacity, for example, during a psychotic episode, a temporary psychiatric illness, or because the person is unconscious, in severe distress, or suffering dementia
> - limited understanding of English.

It is important to note the factors of 'age', 'physical or mental disability' or 'limited understanding of English' do not, as such, suffice to assume that a person lacks the capacity to make their own privacy choices. These identified personal characteristics are merely circumstances which *may* affect a person's capacity. An individual's personal circumstances

---

[490] It also appears in GDPR art 9(2)(c) (allowing the processing of special category data without consent where necessary to protect the vital interests of the data subject or another person); and see further GDPR art 49(1)(f) and Recital 112 (derogations from restrictions on data transfers due to important reasons for public interest).

[491] It is more common to see the pairing of 'physical' and 'mental' – as is, for example, demonstrated by the reference in the APP Guidelines (n 293) to 'physical or mental disability'.

and their effect on capacity always need to be examined on a case-by-case basis. Where capacity fluctuates, a capacity assessment made at a particular point in time may need to be undertaken again if circumstances change. This is recognised in the APP Guidelines' references to 'temporary incapacity' and 'incremental' incapacity. In contrast to the federal Privacy Act, some state privacy legislation contains express provisions on capacity. These are generally consistent with the National Decision-Making Principles, which as discussed above, aim to protect as far as possible autonomy and independence. The emphasis on the will and preferences of a person who may require support in making decisions is at the heart of the paradigm shift away from the 'best interests' standards.

For example, in Victoria, section 50 of the *Privacy and Data Protection Act 2014* provides for substitute decision-making where an:

> individual is incapable (despite the provision of reasonable assistance by another individual) by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder of—
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or
>
> (b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires).[492]

Similarly, in New South Wales, section 7 of the *Health Records and Information Privacy Act 2002* gives an authorised representative the power to perform an act authorised, permitted or required under the Act where:

> the individual is incapable (despite the provision of reasonable assistance by another person) by reason of age, injury, illness, physical or mental impairment of—
>
> (a) understanding the general nature and effect of the act, or
>
> (b) communicating the individual's intentions with respect to the act.

The Information and Privacy Commission (NSW)'s 'Guide: Privacy and people with decision making disabilities'[493] contains much valuable guidance on the relationship between privacy rights and capacity.

(iii) Conclusion

Apart from children, there are no groups that are considered to be physically or legally incapable of making their own privacy decisions. However, where age, injury, illness, physical or mental impairment render a person, even with reasonable assistance, incapable of understanding or communicating their privacy choices, they are considered to be legally incapable. Their privacy decisions will then need to be made by a substitute decision-maker. Appropriately, the threshold of physical and legal incapacity is set quite high so as not to unduly curtail the autonomy of persons whose decision-making capacity is affected.

---

[492] *Privacy and Data Protection Act 2014* (Vic) s 50(3); see also *Health Records Act 2001* (Vic), s 85.
[493] IPC NSW *Guide* (n 488).

The Privacy Act does not contain provisions on capacity to consent or to make other privacy choices. Instead, these issues are addressed in OAIC guidance. The more detailed provisions in some state legislation are likely attributable to the fact that they originated in health privacy legislation, where issues of incapacity are likely to arise more regularly than in other contexts. In line with such state legislation, it may be appropriate for the Privacy Act to spell out more explicitly when a person is to be considered incapacitated and how difficulties to make privacy decisions should be dealt with.

There appears to be no compelling evidence that the current approach causes uncertainty among entities regulated by the Privacy Act. Nonetheless, there would be some benefits if the Privacy Act expressly set out the relevant principles. In particular, this would provide an opportunity to ensure that the Privacy Act operates consistently with the National Decision-Making Principles recommended by the ALRC. Dealing with these matters in the statute, rather than in regulatory guidance, would also give the principles more authoritative force and, possibly, make them more accessible to regulated entities than the current guidance.

Taken together, there is a case for giving the OAIC guidance statutory force, or for making other legislative changes to the current approach to dealing with incapacity.

Question 3b — In addition to the above, are there any other groups that are particularly vulnerable in relation to privacy (consider insights identified in the ACCC's Digital Platforms Inquiry final report and any relevant submissions made to that inquiry on this topic)?

Key findings:

Vulnerability is can be defined as heightened susceptibility to harm. It is preferable that any definition of 'vulnerable groups' engages with vulnerability as a state rather than a status.

Vulnerability is dynamic and relative, rather than a fixed trait that is associated with belonging to a specific group. The causes of vulnerability are complex and can intersect with one another. Both individual characteristics and situational factors shape our susceptibility to harm.

The preferred approach in other areas of consumer protection is to consider 'vulnerability factors' that put people at higher risk of suffering harm or detriment.

The particular needs of vulnerable people for privacy protection have been recognised at the highest international level. The United Nations (UN) General Assembly[494] and Human Rights Council[495] have called on States 'to further develop or maintain […] preventive measures and remedies for violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular adverse effects on women, as well as children and persons in vulnerable situations or marginalized groups'.

With the exception of children, the GDPR makes only oblique reference to the needs of vulnerable groups.[496] However, EU data protection law has long recognised that some segments of the population require special protection, such as the mentally ill, asylum seekers, or the elderly'.[497]

The Privacy Act currently does not make explicit reference to vulnerable groups and their particular needs for protection. Likewise, the APP Guidelines do not make any special provision for vulnerable groups.[498]

---

[494] UN General Assembly (2014), Right to privacy in the digital age, A/RES/71/199.
[495] UN Human Rights Council, Resolution 34/7 (23 March 2017) <https://www.right-docs.org/doc/a-hrc-res-34-7/>.
[496] See, for example, GDPR, recital 75 and the other provisions discussed at 4(a) below.
[497] For example, Art 29 Working Party, *Opinion 03/2013 on purpose limitation*, WP 03/2013, 25 (discussing that for assessing the impact of secondary uses it may be relevant to consider 'whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly').
[498] There is only one mention of vulnerable groups in the APP Guidelines (n 293) at 10 in relation to an example of other information that could be included in a privacy policy. It states that 'if the entity interacts with and collects personal information about a vulnerable segment of the community (such

However, the principles-based regulation of the Privacy Act allows for vulnerability to be considered as an aspect of fairness. For example, APP 3.5 imposes a requirement on APP entities to solicit and collect personal information only by 'fair and lawful means'.[499] It could be considered unfair if an entity collect data from vulnerable individuals through exploitation of their vulnerability. This is implicitly recognised in the APP Guidelines, which give as examples of unfair collection practices that persona information is collected 'from an individual who is traumatised, in a state of shock or intoxicated' or 'in a way that disrespects cultural differences'. [500]

(i) Concept of vulnerability

Vulnerability is a flexible and wide-reaching concept that can adopt different meanings. It can shortly be defined as *susceptibility to harm*. Vulnerability can be described as a position or situation of disadvantage that creates a heightened exposure to harm, or weakens the ability to protect oneself against harm.

Vulnerability has traditionally been associated with a belonging to a particular group that is in need of greater protection, such as the those with disabilities.[501] In the context of privacy, this conceptualisation is evident in giving greater protection to children[502] solely by virtue of their age and withdrawing that protection when children reach an upper age threshold. Consumer protection laws and the law of fiduciaries also have similar rationales because they seek to provide additional protections to individuals who are in relationships that typically give rise to a particular vulnerability, in particular where it arises from a power or information imbalance (such as consumer/business, doctor/patient, solicitor/client etc).

Vulnerability is also an important theoretical framework. The binary concept of vulnerability has been critiqued by scholars, who prefer to see vulnerability as a state, rather than a status.[503] This alternative approach emphasises that vulnerability is a *universal* constant and an *inevitable* aspect of the human condition. This understanding owes much to the writing of Martha Albertson Fineman. Fineman criticises the frequent use of the term 'vulnerable' to define particular social groups, such as children, the aged, people with disability etc. In her view, this use of the term is 'typically associated with victimhood, deprivation, dependency, or pathology'.[504] Fineman rejects the idea that an 'individual or group should be considered more or less vulnerable, […] or specifically or especially vulnerable'.[505] Instead, Fineman calls for a recognition that vulnerability is a 'universal, inevitable, enduring aspect of the human condition'.[506] Her vulnerability theory stresses the importance of relationships, and

---

as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information'.

[499] *Privacy Act* 1988 (Cth) sch 1 pt2 s3.

[500] *APP Guidelines* (n 293) [3.63].

[501] See discussion in Florencia Luna, 'Identifying and evaluating layers of vulnerability – a way forward' (2019) 19(2) *Developing World Bioethics* 86, 87.

[502] See above, Part 1 and 2.

[503] Ryan Calo, 'Privacy, Vulnerability, and Affordance' (2017) 66(2) *DePaul Law Review* 591, 591 and passim.

[504] Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20(1*) Yale Journal of Law and Feminism* 1, 8.

[505] Martha Albertson Fineman, 'Fineman on Vulnerability and Law', New Legal Realism (30 November 2015) <http://newlegalrealism.org/2015/11/30/fineman-on-vulnerability-and-law>.

[506] Ibid.

the values of compassion, trust and care. Fineman argues that 'inequality of resilience' is at the heart of vulnerability, and that it is this inequality that needs to be addressed, rather than vulnerability itself.

Both approaches, the traditional understanding of vulnerability and Fineman's vulnerability theory, lead to important insights. They are best seen as complementary because each approach avoids some weaknesses of the other. It is indeed problematic to focus on the ideal of an autonomous, self-sufficient individual, when all humans are vulnerable both at the beginning and end of their lives, and many also experience significant challenges throughout their middle lives. Fineman's vulnerability theory allows a richer, and more complete, understanding of vulnerability and how it is most appropriately addressed. It also provides a basis for arguing more forcefully that the state owes a positive duty to provide support and protection so that all members of society can enjoy equal social and economic participation. If policy making recognises more openly that vulnerability is the norm, rather than an exception, society is bound to give the values of care, empathy, inclusivity and support greater recognition than at present. Understood in that way, providing support is not only the state's responsibility, but also needs to be identified as a common obligation on all members of society, including industry and business.

However, it is also problematic to say – as Fineman does – that '[n]o one is born resilient. Rather, resilience is produced within and through institutions and relationships that confer privilege and power'.[507] This position does not appear to acknowledge sufficiently that humans do have natural resilience and that not everyone in a vulnerable position would like to be considered as 'vulnerable'. There are also significant differences in the levels of natural resilience between individuals, and it is important to support autonomous decision-making, and to encourage self-protection, wherever possible.

Some privacy laws, mainly overseas, contain special protections for data subjects who belong to a particular group, most prominently through provisions that give special protections to children or consumers. The UN resolutions referred to above, as well as the Australian federal government's announcement of its intention to enact specific privacy rules to 'protect the personal information of children and vulnerable groups',[508] recognise that some groups have a more limited ability to withstand privacy invasive practices or are at greater risk of suffering privacy harms. This suggests that the traditional, group-based understanding of privacy is likely to remain highly influential as a model for future privacy regulation.

However, it is important to recognise that belonging to a particular group is not in all cases a reliable proxy for vulnerability. Vulnerability arises in a large variety of contexts, and depends on individual, situational and structural factors. Some people have the ability to cope successfully with highly adverse circumstances, whereas others in like or better circumstances may require considerable support to avoid harm. This suggests that vulnerability should not be seen exclusively as the product of a particular status or personal

[507] Ibid.
[508] Australian Government, Treasury, *Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (2019), 5.

characteristics. The regulatory framework should be inclusive of those who fall outside these established categories but nonetheless are at a similar risk of suffering privacy harms.

(ii) Identifying vulnerability

The focus on a heightened exposure to detriment and harm in defining vulnerability explains why vulnerability is a 'relative' as well as a 'dynamic' concept.[509]

Vulnerability is *relative* because – at least for the understanding of vulnerability adopted here – some people are more vulnerable than others, and a person's susceptibility to harm can be greater or smaller. Furthermore, the degree of vulnerability, and the (self-) perception of vulnerability, can differ from person to person. Vulnerability is therefore 'best viewed as a spectrum rather than a binary state'.[510]

It is a *dynamic* because it can increase or diminish, depending on a person's circumstances, life stage and life events. As discussed above, we are all dependent on receiving support and protection at some stage of our lives. A person's vulnerability can change over a time, and those changes can arise suddenly, eg. through illness or bereavement. Vulnerability can pass, or it can be of a permanent or sporadic nature. In other cases, vulnerability is the result of longstanding physical or mental conditions.

The causes of vulnerability are complex and can intersect with one another. Both individual characteristics and circumstantial factors shape our susceptibility to harm. Individual characteristics are important indicators of vulnerability, but vulnerability can also be affected, for better or worse, by the individual's external circumstances and their environment. Supportive interaction can, in many cases or at least partially, reduce the effects of a person's vulnerability.

(iii) Consumer vulnerability

Consumer law is one of the areas in which the concept of vulnerability has been considered extensively. Consumers are considered to be in a structurally weaker position when they are dealing with business, because they often lack the sophistication, information or power to withstand practices that may cause them disadvantage. However, more recently there has also been increasing recognition that some consumer groups are in circumstances of particular disadvantage.

There is much current and emerging work in consumer studies on which the present discussion of vulnerability in the privacy context can draw. For example, the UK Regulators Network (UKRN) has identified the issue of supporting consumers in vulnerable circumstances as one of its current priority areas.[511] The UKRN brings together the regulator

---

[509] Consumer Affairs Victoria, *What do we mean by 'vulnerable' and 'disadvantaged' consumers?*, Discussion Paper (2004), p 4; see also Florencia Luna, 'Identifying and evaluating layers of vulnerability – a way forward' (2019) 19(2) *Developing World Bioethics* 86, 90.
[510] London Economics, VVA Consulting and Ipsos Mori consortium, *Consumer vulnerability across key markets in the European Union*, Final report (European Commission: Justice and Consumers, 2016).
[511] UK Regulators Network*, Annual Report and 2020/21 Workplan* <https://www.ukrn.org.uk/publications/ukrn-annual-report-and-2020-21-work-plan/>.

of major industries, including the ICO, the media regulator Ofcom and the regulator for the utility and financial services industries. In Australia, the Essential Services Commission Victoria, which regulates providers of essential services, has embarked on developing a strategy to address consumer vulnerability.[512] Vulnerable consumers are also an 'enduring priority' of the enforcement and compliance activities of the ACCC.[513]

(iv) Developing a definition of vulnerability

Consumer vulnerability is an important regulatory challenge globally. A recent large-scale, multi-national evidence-based study in Europe has defined a vulnerable consumer as:

> A consumer, who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment:
>
> - Is at higher risk of experiencing negative outcomes in the market;
> - Has limited ability to maximise his/her well-being;
> - Has difficulty in obtaining or assimilating information;
> - Is less able to buy, choose or access suitable products; or
> - Is more susceptible to certain marketing practices.[514]

This definition makes reference to the main drivers as well as the main effects of vulnerability. It acknowledges that consumer vulnerability can be the result of personal characteristics, a person's particular situation, external factors, or often a combination of these.

There are many other well-considered definitions of consumer vulnerability[515] of which it is appropriate to take note. The examples in the following discussion have been chosen because of their particular relevance for a definition that could be adopted in a social media online code.

(v) The approach of the eSafety Commissioner

The approach adopted by the eSafety Commissioner is interesting for a number of reasons. Importantly, the eSafety Commissioner's Office has a mandate to respond to online harm, which can include interference with privacy. Furthermore, the eSafety Commissioner has gained considerable regulatory experience in engaging with online service providers and in using an evidence-based approach to create strong protective frameworks.

---

[512] Essential Services Commission, *Building a strategy to address consumer vulnerability*, (Approach paper, 17 September 2020).
[513] Australian Competition and Consumer Commission, 'Compliance & enforcement policy & priorities', Web page <https://www.accc.gov.au/about-us/australian-competition-consumer-commission/compliance-enforcement-policy-priorities>.
[514] London Economics, VVA Consulting and Ipsos Mori consortium, *Consumer vulnerability across key markets in the European Union*, Final report (European Commission: Justice and Consumers, 2016).
[515] Lists of definitions are contained in: Essential Services Commission, *Building a strategy to address consumer vulnerability*, Approach Paper, 17 September 2020, Appendix 4.

The first issue to note is a terminological one. The eSafety Commissioner uses the approach of 'at risk' groups in preference to 'vulnerable' groups.[516] This language is less disempowering[517] and responds to some of the criticisms identified above relating to the traditional understanding of vulnerability. It signals that belonging to a disadvantaged group does not immutably equate to exposure to harm, and that susceptibility to harm is contextual and dynamic.

The 'at-risk groups' identified by the eSafety Commissioner include:

- children and young people
- older Australians
- women
- people with disability
- Aboriginal and Torres Strait Islander peoples
- people from culturally and linguistically diverse communities
- people who identify as LGBTQI+.[518]

(vi) Vulnerability in Australian financial services industry codes

Recent Australian industry codes also give greater recognition to issues of consumer vulnerability.[519] While not directed specifically at online harms, they provide an insight into recent debates in other Australian industry sectors that have been subject to criticism for not responding adequately to customers that may be particularly at risk.

The Banking Code of Practice (1 March 2020) contains specific provisions in relation to customers who may be vulnerable:

> **We will take extra care with vulnerable customers.**
>
> 38. We are committed to taking extra care with vulnerable customers including those who are experiencing:
>
> a) age-related impairment;
>
> b) cognitive impairment;
>
> c) elder abuse;
>
> d) family or domestic violence;
>
> e) financial abuse;
>
> f) mental illness;

---

[516] This is also the preferred language of some non-governmental organisations working in the support sector, such as Access Now; available athttps://www.accessnow.org/.
[517] London Economics, VVA Consulting and Ipsos Mori consortium, *Consumer vulnerability across key markets in the European Union*, Final report (European Commission: Justice and Consumers, 2016).
[518] Julie Inman Grant, 'Protecting voices at risk online',(eSafety Commissioner 2020).
[519] See Review of General Insurance Code of Practice, <http://codeofpracticereview.com.au/about-the-code> (website also contains submissions).

g) serious illness; or

h) any other personal, or financial, circumstance causing significant detriment.[520]

39. We will train our staff to act with sensitivity, respect and compassion if you appear to be in a vulnerable situation.

40. If you tell us about your personal or financial circumstance, we will work with you to identify a suitable way for you to access and undertake your banking.

Another Australian industry code which has recently been revised to make specific provision for vulnerable consumers is the General Insurance Code of Practice 2020.[521] In relation to retail insurance products, the newly introduced Part 9 of the Code states that:

91. We are committed to taking extra care with customers who experience vulnerability. We recognise that a person's vulnerabilities can give rise to unique needs, and that their needs can change over time and in response to particular situations.

92. A person's vulnerability may be due to a range of factors such as:

a. age;

b. disability;

c. mental health conditions;

d. physical health conditions;

e. family violence;

f. language barriers;

g. literacy barriers;

h. cultural background;

i. Aboriginal or Torres Strait Islander status;

j. remote location; or

k. financial distress.

93. We encourage you to tell us about your vulnerability so that we can work with you to arrange support — otherwise, there is a risk that we may not find out about it. […]

A number of features in these Codes are noteworthy. First, neither of the Codes attempts a definition of vulnerability or of vulnerable groups. Second, the listed vulnerability factors are used by way of example and intended to be inclusive. Third, the Codes express a commitment to taking extra care with customers experiencing vulnerability,[522] but put some

---

[520] Australian Banking Association, *Banking Code of Practice* (1 March 2020 release), Ch 14.
[521] General Insurance Code Governance Committee, *2020 General Insurance Code of Practice*, <https://insurancecode.org.au/resources/2020-general-insurance-code-of-practice/> The Code will be binding from 1 July 2021.
[522] This coincides with the definition of vulnerability used by the Financial Conduct Authority, which defines a vulnerable consumer as is 'someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care': Martin

burden on customers by encouraging them to disclose their vulnerability. Fourthly, the Insurance Code of Practice adopts a factor-based approach, whereas the Banking Code is in part also threshold-based (e.g. 'age' vs. 'age-related impairment, or 'physical health condition' vs. 'serious illness'). Identifying vulnerability factors allows for a wider range of persons to be within the scope of protection but also introduces some uncertainty about how vulnerability is to be assessed. Furthermore, the situational factors in the Banking Code are of a more limited range, although this is in part addressed by the catch-all of 'any other personal, or financial, circumstance causing significant detriment'. Finally, it is significant that neither Code identifies lack of financial understanding or financial literacy, as such, as a vulnerability factor. Other vulnerability factors that are absent from the indicative lists relate broadly to other indicators of 'socioeconomic disadvantage' (which not infrequently crosses over with the groups identified above), such as homelessness,[523] refugee or uncertain resident status etc.

One problematic issue is how much of the onus should be placed on the online service provider to assess vulnerability. The Hayne Royal Commission criticised the previous Banking Code of Practice for putting much of the emphasis on self-disclosure.[524] Many providers of financial services have direct customer contact, and can train their front-line staff in appropriately identifying and responding to customers who may be in vulnerable circumstances.

In contrast, online services are by their very nature delivered remotely and often without direct human intermediation. Vulnerability will therefore often be much more difficult to recognise and address in online channels. In addition, it may raise privacy issues of its own if service providers were to request and collect additional information to assess 'vulnerability' that would not have been necessary for the particular service itself.

(vii) **Individual factors**

Individual characteristics affecting vulnerability should not be understood in a narrow sense of inherent traits of a person. Morgan et al developed a typology of vulnerability that distinguishes four areas of vulnerability: physical sensitivity, physical competency, mental competency, and level of sophistication.[525] In their classification, *physical sensitivity* arises through contact with harm-causing products. (In the context of online services, the factor of 'physical sensitivity' would probably be better described as *product sensitivity*, because the digital environment does not depend on physical proximity for exposure to harm.) *Physical competency* is associated with (physical) disabilities as well as diminished capacities, for example as a result of ageing. *Mental competency* can be affected by mental impairment, as well as cognitive and processing abnormality and linguistic and literacy issues. The *level of*

Coppack et al, *Consumer Vulnerability*, Occasional Paper No. 8 (Financial Conduct Authority, February 2015), 7 (emphasis added) ('Financial Conduct Authority, *Consumer Vulnerability*').

[523] This factor is recognised in Australian Competition and Consumer Commission, ***Don't take** advantage of disadvantage: A compliance guide for businesses dealing with disadvantaged or vulnerable consumers*, 2014, 2.

[524] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, *Final Report vol. 1* (February 2019) 89.

[525] Fred W Morgan, Drue K Schuler and Jeffrey J Stoltman, 'A Framework for Examining the Legal Status of Vulnerable Consumers' (1995) 14(2) *Journal of Public Policy & Marketing* 267, 272.

sophistication can depend on the consumer's educational attainment, socioeconomic factors, as well as their emotionality and gullibility.

In a recent paper, the UK Financial Conduct Authority has identified four key drivers of the risk of vulnerability that relate to individual circumstances. These are:

- health – disabilities or illnesses that affect the ability to carry out day-to-day tasks
- life events – major life events such as bereavement, job loss or relationship breakdown
- resilience – low ability to withstand financial or emotional shocks
- capability – low knowledge of financial matters or low confidence in managing money (financial capability) and low capability in other relevant areas such as literacy, or digital skills.[526]

Although these and similar[527] descriptions of the drivers of vulnerability vary slightly, they share the common understanding that vulnerability is not only the product of a consumer's inherent characteristics but also depends on their particular situation at a given time.

Vulnerability is rarely static; it can fluctuate and may affect a consumer in some situations but not others.[528] It is important to note that risk factors can compound to increase a person's vulnerability. For example, a person with a gambling addiction may be particularly prone to harm after an adverse life event, such as a relationship breakdown, which reduces their resilience to engaging in harmful gambling behaviour. Multi-layered vulnerabilities are regarded as particularly indicative of high risk.[529]

(viii) Situational factors

In addition to personal factors, there are also external or structural factors that make consumers vulnerable. These situational factors include the 'market environment', as referred to in the above definition of customer vulnerability developed in the European Union. Market-related factors can include that consumers do not have enough information to make informed decisions, that they have limited access to a range of services because they live in a remote area, or that they belong to a customer segment that is not adequately catered for.

The Irish Privacy Commissioner has added in the context of the GDPR that vulnerability can arise 'in any case where a power imbalance in the relationship between the position of the data subject and the controller can be identified'.[530] In these circumstances where a data processor has considerably more power, the data subject may be unable to freely exercise their right to consent to, or oppose, the processing of their data. This significantly widens the

---

[526] UK Financial Conduct Authority, 'Treating vulnerable consumers fairly', Web page (2 December 2020) <https://www.fca.org.uk/firms/treating-vulnerable-consumers-fairly>.
[527] See, for example, the list in Essential Services Commission, *Building a strategy to address consumer vulnerability*, Approach Paper (17 September 2020) App 4.
[528] Data & Marketing Association, *The vulnerable consumer: Recognising vulnerability and taking a customer-centric approach*, White Paper (September 2016) 4 ('CMA *Vulnerable Consumer*').
[529] Financial Conduct Authority, *Consumer Vulnerability* (n 522) 8.
[530] Data Protection Commission (Ireland), *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)* (2019) 7.

groups in which vulnerability can be experienced. It would include relationships between employers and employees, health care professionals and patients, in aged care and other care contexts, between school or universities and their students.

Vulnerability is not detached from the environment in which a person lives and makes their decisions. In an important article exploring the interaction between privacy and vulnerability, Calo highlights that a person, groups and society can *render* another person vulnerable, or that they can *exploit* an existing vulnerability.[531] It is also possible that actors simply *disregard* or *exacerbate* another person's existing vulnerability – for example, when a business interacts with a consumer using a channel of communication, language or visuals that do not correspond to their needs.[532]

(ix) Vulnerability to privacy invasions

As explained above, vulnerability is generally associated with a heightened susceptibility to harm. A definition of who is vulnerable in relation to privacy must therefore take into account the harms that a person may be exposed to if their privacy is not sufficiently protected.

In our discussion at 1(b) above, in relation to the privacy harms that can affect children we drew a distinction between intrinsic privacy-related risks and harms, and consequential risks and harms. This categorisation is also relevant here. *Intrinsic* harms include dignitary and autonomy harms that results from loss of control over one's personal information, the potential reduction in a person's capacity to maintain anonymity and harm to health and well-being. *Consequential* harms include increased exposure to unsolicited targeted advertising and other online marketing, the risk of exclusion from services as a result of profiling, as well as increased exposure to e-safety harms including scams and data breaches. Other consequential harms can be economic in nature, such as the risk of price discrimination or result from the purchase of unsuitable products and services due to manipulation or misinformation.[533]

(x) Conclusion on identifying vulnerability to privacy harm

The local and overseas developments discussed above, including the work of industry bodies in the financial sector in seeking to improve their treatment of vulnerable individuals and of regulators which have increased their focus on vulnerability, contain important information on the types of approaches that can usefully be adopted to assist vulnerable individuals.

The literature on this issue makes clear the importance of adopting a sophisticated and broad understanding of vulnerability. If a definition is used, it must not be rigid and should be cognisant of the full range of drivers that can contribute to vulnerability. It is simplistic to associate vulnerability with belonging to a particular group. Vulnerability is not a fixed trait with an easily identifiable threshold; it can improve or worsen over time, depending on

---

[531] Ryan Calo, 'Privacy, Vulnerability, and Affordance' (2017) 66(2) *DePaul Law Review* 591, 594.
[532] CMA *Vulnerable Consumer* (n 528) 4.
[533] See also ACCC *DPI Final Report* (n 3) 447.

personal circumstances, as well as external factors. Furthermore, the causes of vulnerability are complex and can intersect with one another.

Identification of specific groups as particularly vulnerable bears the risk of paternalism, alienation and potentially discrimination. Therefore, it is preferable to adopt a factor-based approach to vulnerability that relies on listed risk factors of vulnerability but remains responsive to non- identified risk factors. The approaches adopted by the eSafety Commissioner and in recent codes in the financial services industry provide useful models that are worth considering.

An unresolved issue relates to the issue of identifying vulnerability, in particular in an online environment. Obligations on online service providers to identify at risk groups can cause practical problems and carry the risk of privacy invasion or potential discrimination or exclusion from services. Self-identification is more likely to work in case of those with static conditions or with groups that are used to self-declaring, such as persons with disability or older persons, and may work less well with individuals who do not wish to disclose their vulnerability, or are unaware of it.

Recommendation 22

The Code should adopt a factor-based definition of vulnerability that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020.

We support this also as an economy-wide measure.

Question 3c — What makes each of these groups vulnerable? This will include consideration of whether an existing vulnerability (e.g. a disability) is compounded when engaging with a digital platform or other online organisations, or whether a vulnerability arises where an individual engages or transacts in the online environment.

Key findings:

Vulnerability in an online context can arise where an individual faces greater difficulty than others in protecting themselves from harm. This can be the technical or cognitive skill and experience to use digital platforms and other applications safely.

Individuals can also be vulnerable because they have particular characteristics that expose them to greater or different harm than other people. Such harm can arise from being exposed to or targeted with inappropriate products or services, from unlawful discrimination or inappropriate exclusion from a market.

Digital platforms can exacerbate the risks for people with a range of 'vulnerability factors' and can compound the risks that are experienced by these individuals.

The approaches of other agencies and organisations suggest that is advisable to engage in detailed qualitative and quantitative research into the vulnerability experience of specific customer groups and to adopt a multi-stage approach to identifying and addressing vulnerability.

As explained above, our recommendation is to regard vulnerability not as a status associated with a particular group but as a product of risk factors. Risk factors can also intersect and compound, or – conversely – be compensated for by other characteristics of a person. For example, an individual may be affected by more than one risk factor, such as a child with disability,[534] or an older person from a non-English speaking background. This makes it less fruitful to identify vulnerability in relation to each group separately, or to consider vulnerability in the abstract, but rather in the context of a particular person, relationship or situation.

Nonetheless, it is possible to describe the variety of ways in which the risk factors identified above can operate on an individual.

(i) Vulnerabilities arising from difficulty to self-protect

In some cases, vulnerability arises because an individual faces greater difficulty than others in protecting themselves from harm. The ACCC referred in its Digital Platforms Report to the

[534] On these intersectional risk factors, see eSafety Commissioner, *Online safety for young people with intellectual disability*, Report (December 2020) <https://www.esafety.gov.au/sites/default/files/2020-12/Online safety for young people with intellectual disability report.pdf>.

fact that 'certain groups of consumers may lack the technical, critical and social skills to engage with the internet in a safe and beneficial manner'.[535] This may be the case in particular for individuals from disadvantaged backgrounds, who have limited access to electronic devices or services, and have therefore gained less experience in identifying risk and guarding against harm.

Vulnerabilities that can arise at an older age have been described as follows:

> Some aging consumers are faced with declining cognitive, biological and physiological abilities which heighten the feelings of vulnerability, especially in health-related service encounters that require informed consent. Evidence exists that in problem solving, some aging consumers may deliberate less, others may have less memory capacity for short-term recall, and some may lack speed in information processing.[536]

Similar difficulties may arise for younger individuals with disability[537] or illness. In addition to these risks that may affect an older person or persons with health conditions or disabilities generally, older individuals may be at a particular disadvantage in the digital environment if they lack familiarity with online systems. A report prepared for the eSafety Commissioner found that older Australians have a high level of concern around digital privacy and security,[538] and that about four-in-ten wanted to improve their skills in adjusting privacy settings.[539]

Some features of online applications also create the risk of harm for users with reduced levels of resilience or self-control. For example, elements of 'persuasive design',[540] such as infinite scrolls and cumulative features such as 'friends' and 'likes' that are intended to keep users engaged online for longer, have been said to exacerbate addictive behaviours of some users.[541]

(ii) Vulnerabilities arising from disadvantage

Individuals can also be vulnerable because they have particular characteristics that expose them to greater or different harm than other people. The eSafety Commissioner's Report suggests that some of the concerns about internet safety by older Australians were well-founded, because 'respondents who were over 70 years old were more likely to experience a security breach, for example have contact details stolen, experience a virus attack, or to be

---

[535] ACCC *DPI Final Report* (n 3) 448. While the reference relating to this statement was concerned with children under nine, some adults may also lack the requisite skills to use the internet safely.
[536] Merlyn A Griffiths and Tracy R Harmon, 'Aging Consumer Vulnerabilities Influencing Factors of Acquiescence to Informed Consent' (2011) 45(3) *The Journal of Consumer Affairs* 445, 446 (references omitted).
[537] See eSafety Commissioner*, Online safety for young people with intellectual disability*, Report (December 2020).
[538] Ipsos Pty Ltd, *Understanding Digital Behaviours of Older Australians – Full Report: A Report for the eSafety Commissioner* (2017), 103.
[539] Ibid, 110.
[540] 5Rights, *Disrupted Childhood: The Cost of Persuasive Design* (2018).
[541] UK Government, *Online Harms*, White Paper (April 2019), 27.

a victim of a scam'.[542] It is possible that the lack of proficiency with electronic devices and less developed protective skills are not only a cause of the higher incidence rates but also make older individuals a more attractive target for malicious actors.

Other privacy risks may also disproportionately affect people in disadvantaged positions. For example, the ACCC stated in its Preliminary Report of the Digital Platforms Inquiry that some vulnerable consumers are 'at risk of being targeted with inappropriate products or scams, discriminated against, or inappropriately excluded from markets'.[543] There is evidence that the potential for discrimination often disproportionately affects those who are already in a weaker economic or social position, with the consequence that 'statistical discrimination compounds the disadvantages […] we readily associate with race, class, gender and cultural identity'.[544]

Privacy harms can also arise through excessive collection and use of personal information relating to vulnerability. This includes cases where consumers are treated differently because they are inappropriately assessed as 'vulnerable'.

(iii) The need for further research and user engagement

Finally, it is important to point out potential shortcomings of this desk-based analysis. Other organisations and regulators that aimed to improve the situation of vulnerable consumers often adopt a multi-pronged, multi-stage approach to identifying and addressing vulnerability. These projects include qualitative and quantitative research into vulnerability experience of their specific customer groups, internal and external engagement with stakeholders, including with consumer representatives and groups, collection of examples of good practice, and capacity-building activities.[545]

Recommendation 23

We recommend that the OAIC engage in further engagement and analysis to ensure that its protective measures are appropriately targeted, have the buy-in and support of affected groups and are tested for effectiveness.

[542] Ipsos Pty Ltd, *Understanding Digital Behaviours of Older Australians – Full Report: A Report for the eSafety Commissioner* (2017) 102.
[543] ACCC *DPI Final Report* (n 3) 447.
[544] Oscar H Gandy Jr, 'Consumer Protection in Cyberspace' (2011) 9(2) tripleC 175, 176.
[545] See, eg, Essential Services Commission, *Building a strategy to address consumer vulnerability*, Approach Paper (17 September 2020); see also UK Financial Conduct Authority, 'Treating vulnerable consumers fairly', Web Page (2 December 2020) <https://www.fca.org.uk/firms/treating-vulnerable-consumers-fairly#4>.

Question 3d — Do digital platforms have any existing restrictions or other measures designed to mitigate risks/harms relating to the collection, use and disclosure of the personal information of individuals physically or legally incapable of providing consent or other vulnerable groups/individuals?

Key findings:

All digital platforms have a range of policies and controls in place to help protect vulnerable people, and to facilitate independent access to products and services.

The major platforms have detailed advertising policies that are intended to protect users from harm by imposing restrictions and prohibitions on advertising various types of potentially harmful products or services, and on certain advertising content.

In addition to restricting advertising content that may be potentially harmful to users, the major platforms further protect vulnerable users by imposing restrictions in relation to their personalisation and targeting tools.

Some platforms also impose restrictions on the collection of data relating to vulnerable groups through their advertising products.

Community guidelines and accessibility aids also operate to enhance the participation of vulnerable groups.

These policies can improve the experience and protection from discrimination and targeting. But they currently only operate on a voluntary basis through the platforms' terms and conditions of use.

As we observed with respect to the protection of children's privacy, none of the platforms present a single, consolidated approach to addressing vulnerability. In some ways, this might be as expected, given the complex nature and varied causes of vulnerability discussed above. We also observe a high degree of variability in policy and approach between platforms, making comparison difficult.

What follows is a survey of the range of existing restrictions and other measures that provide some mitigation with respect to risks and harms faced by vulnerable groups online. In general, these are applied for commercial actors via advertising policies and for all users (commercial and non-commercial) via community guidelines. Other measures, such as access controls and accessibility features are also discussed. We have sought to highlight equivalent or comparable standards of protection, even where these may be applied in different ways through different mechanisms.

We observe very few measures from platforms directed at limiting the volume or type of personal information that they collect about vulnerable people. Digital platforms cannot realistically (and consistently with the service they provide and the business model they are based on) avoid collecting information about their users that may indicate vulnerabilities. Instead controls focus on limiting the use of personal information or minimising foreseeable harms that may arise from the use of that information. So, for example, rather than refraining

from collecting information about a user's age, gender, racial or ethnic origin or other protected characteristic, platforms must instead have robust measures in place to ensure that that information is not misused in a way that causes harm (for example, in targeted advertising or recommending content). However, there is a substantial and growing body of evidence that measures currently in place and outlined below are ineffective in preventing harms (for example, by targeting housing and employment ads in ways that display age, gender or racial bias).[546]

All platforms enforce general standards of behaviour that apply to protect all users but disproportionately benefit vulnerable groups. These include prohibitions on misleading advertising or hateful content. Platforms also enforce more specific requirements to protect groups that are less able to defend themselves (such as restrictions on exploitative targeting and data collection) or are more exposed to harm (such as discrimination and violence).

Very broadly, this reflects the general approach to addressing vulnerability proposed below, whereby vulnerable groups are protected first by high baseline protections for everybody, and second by specific measures targeting key harms.

(i) Advertising Policies

In relation to advertising, platforms generally offer three means for protecting vulnerable groups: (i) general advertising policy prohibitions and restrictions, which prohibit advertisements containing potentially harmful content and products; (ii) technical advertising constraints on the use of targeting tools to exploit (for example, by targeting) and discriminate against (for example, by exclusion from target audiences) vulnerable groups; and (iii) additional data collection restrictions for advertisers in relation to vulnerable groups.

Content restrictions

Google, Apple, Facebook, Twitter and Snapchat's advertising policies protect users from potentially harmful advertising by imposing restrictions and prohibitions on various types of potentially harmful products and content. While such policies are formulated so as to afford general protection to all users, the protections covered in advertising policies are of increased value to vulnerable consumers. Notably, Facebook, Google and Twitter supplement these policies by further targeting restrictions.

The nature of advertising restrictions and prohibitions differs across platforms, but potentially harmful products and services commonly subject to such restrictions include; gambling, tobacco, alcohol. certain financial products, and misleading products; as well as harmful content such as discriminatory content, hateful content, and misleading content.

While advertising for gambling may have increased potential to cause harm to vulnerable groups, platforms still generally allow it subject to restrictions. Twitter is the only platform evaluated which prohibits rather than restricts gambling-related advertising,[547] while

---

[546] Kofman and Tobin (n 458). See generally Pro Publica, 'Machine Bias', Web page <https://www.propublica.org/series/machine-bias>.
[547] Twitter Business, 'Gambling content', Web page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/gambling-content.html>.

Facebook[548], Google[549] and Snapchat [550] impose additional safeguards, by requiring advertisers to gain pre-approval for gambling-related ads. Additional safeguards are commonly imposed promoting responsible gambling. The means by which this is achieved differs per platform and include the requirement to have a landing page that displays information about responsible gambling, [551] or further advertising content stipulations, such as not glorifying gambling or encouraging users to play beyond their means[552]; Apple's advertising policy for its advertising arm, Apple Search Ads, provides the least protection in relation to gambling content, and merely imposes jurisdiction-related restrictions.[553]

Similarly, advertising for alcohol has increased potential to harm certain vulnerable groups and is subject to varying restrictions by platforms. Google,[554] Twitter[555] and Snapchat[556] impose additional content restrictions on alcohol-related ads, such as not glamorizing alcohol or encouraging the consumption of alcohol in excess. Snapchat requires that advertisers add warning labels encouraging responsible consumption. Both Apple[557] and Facebook[558] seemingly offer the least protection to vulnerable groups, merely requiring that advertisers comply with related regulations and target alcohol-related ads age-appropriately.

All platforms prohibit advertising of certain financial products and services which may be potentially harmful to all users and vulnerable groups. This includes short term-loans, deceptive financial offers such as 'get-rich quick schemes' and cryptocurrency initial coin offerings. While Apple does not prohibit advertising for financial products, Apple does cover this under 'deceptive messaging', which includes get-rich-quick schemes.[559] Apple also requires pricing claims to be true-to-nature. Additional financial products and services commonly prohibited among the platforms evaluated include bail bonds (Facebook,[560]

---

[548] Facebook, 'Online gambling and gaming', Web page <https://www.facebook.com/policies/ads/restricted_content/gambling>.
[549] Google Support, 'Gambling and games', Web page <https://support.google.com/adspolicy/answer/6018017>.
[550] Snap Inc, 'Snap Advertising Policies', Web page <https://www.snap.com/en-US/ad-policies/ -gambling-services>.
[551] Google Support, 'Gambling and games', Web page <https://support.google.com/adspolicy/answer/6018017>.
[552] Snap Inc., 'Snap Advertising Policies' (n 550).
[553] Apple, 'Ad content policies', Web page <https://searchads.apple.com/policies/>.
[554] Google Support, 'Alcohol', Web page <https://support.google.com/adspolicy/answer/6012382>.
[555] Twitter Business, 'Alcohol content', Web page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/alcohol-content.html>.
[556] Snap Inc., 'Snap Advertising Policies' (n 550) 4.1.
[557] Apple, 'Ad content policies' (n 553).
[558] Facebook, 'Alcohol', Web page <https://www.facebook.com/policies/ads/restricted_content/alcohol>.
[559] Apple, 'Ad content policies' (n 553).
[560] Facebook, 'Payday loans, payslip advances and bail bonds', Web page <https://www.facebook.com/policies/ads/prohibited_content/short_term_loans?ref=fbb_blog>.

Twitter[561]); binary options (Google[562], Twitter,[563] Facebook[564]) and cryptocurrency token sales (Google[565], Facebook,[566] Twitter,[567] Snapchat[568]).

In order to protect consumers from deceptive and harmful practices in relation to permissible financial ads, all platforms evaluated impose additional requirements relating to transparency and disclosure.

In addition to advertising restrictions which apply to certain products, further content restrictions apply relating to the advertisement itself. Relevant content restrictions include prohibitions on ads that are false or misleading in terms of product claims; pricing and payment terms; functionality and landing pages as well as broader prohibitions on inappropriate and unacceptable business practices such as scamming. While all the platforms evaluated prohibit misleading and inappropriate conduct, only Twitter[569] and Google[570] prohibit exploitative advertising content more broadly.

In relation to advertising content, common prohibitions apply to 'discriminatory content' and 'hate speech' or the promotion of discrimination, hate, harassment, or violence within ads in relation to personal attributes such as race, sex, national origin, disability, religious affiliation, age, sexual orientation or gender identity.

The above protected attributes are common to every platform evaluated but are often supplemented by additional attributes. Google takes a broad approach to its prohibition, adding personal attributes such as veteran status and 'any other characteristic that is associated with systemic discrimination or marginalisation'.[571] Facebook prohibits ads that discriminate or encourage discrimination on the basis of personal attributes, referring to the examples in the above list and adding attributes such as family status and medical and genetic conditions.[572] Apple Search Ads also explicitly prohibits discrimination based on financial status, language and creed.[573] Twitter deals with discrimination within their hateful content policy. While this does not prohibit discrimination more broadly, Twitter prohibits hate speech and advocacy against a protected group, individual or organisation on the basis of the above personal attributes, as well as in relation to veteran status, refugee status and

---

[561] Twitter Business, 'Financial products and services', Web page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/financial-services.html>.
[562] Google Support, 'Financial products and services', Web page <https://support.google.com/adspolicy/answer/2464998>.
[563] Facebook, 'Payday loans, payslip advances and bail bonds' (n 560).
[564] Apple, 'Ad content policies' (n 553).
[565] Google Support, 'Financial products and services' (n 562).
[566] Facebook, 'Cryptocurrency products and services', Web page <https://www.facebook.com/policies/ads/restricted_content/cryptocurrency_products_and_services>.
[567] 'Financial products and services', *Twitter Business*, Web page < https://business.twitter.com/en/help/ads-policies/ads-content-policies/financial-services.html>.
[568] Snap Inc., 'Snap Advertising Policies' (n 550) 4.5.
[569] Twitter Business, 'Inappropriate content', Web page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/inappropriate-content.html>.
[570] Google Support, 'Inappropriate content', Web page <https://support.google.com/adspolicy/answer/6015406>.
[571] Ibid.
[572] Facebook, 'Discriminatory practices', Web page <https://www.facebook.com/policies/ads/prohibited_content/discriminatory_practices>.
[573] Apple, 'Ad content policies' (n 553).

immigrant status. In addition, Twitter prohibits degrading, mocking, or harassing references to events or practices that negatively affected a protected group.[574]

Targeting restrictions

In addition to restricting advertising content that may be potentially harmful to users, Twitter, Google and Facebook further protect vulnerable users by imposing additional restrictions in relation to their personalisation and targeting tools. This limits the ability of advertisers to exploit vulnerable users by targeting them based on vulnerabilities, or discriminate against vulnerable users, by excluding them from target audiences. Notably, Snapchat and Apple do not offer further targeting restrictions in Australia that are of relevance to vulnerable groups.

Among the platforms evaluated, Google offers the most robust targeting restrictions. Google restricts advertisers from taking advantage of its targeting functionality in relation to certain products, such as alcohol, gambling, clinical trial recruitment and prescription medications, which may be of increased harm when targeted to vulnerable users.

Google offers further protections for vulnerable groups by prohibiting advertisers from targeting advertising for certain products to users based on sensitive categories.[575] Google adopts a broad definition of sensitive categories which include: Personal hardships, including health conditions, treatments, procedures, personal failings, struggles or traumatic personal experiences; identity and belief including sexual orientation, political affiliation, race and ethnicity, religious belief, marginalised or vulnerable social groups; sexual interests; and access to opportunities.

Whilst the above definition of sensitive categories extends beyond vulnerability, Google's stated aim in restricting targeting within these categories explicitly cites vulnerability (ie preventing exploitation of the user, preventing stigmatising effects for users, and preventing the entrenchment of exclusionary societal biases).[576] Google provides instructive examples of violative content. It cites, for example, targeting bankruptcy services to users in financial distress; targeting advertising for gender transitioning based on transgender identification; and targeting advertising for legal services for refugees to marginalised groups.

Twitter's Anti-Discriminatory Targeting Policy prohibits advertisers from wrongfully discriminating against legally protected categories of users when using Twitter Ad's targeting tool. Twitter similarly makes reference to the concept of 'Sensitive Categories' of personal user data and prohibits advertisers across all Twitter products from targeting and excluding users from targeting based on any of the sensitive categories or using key words to this effect.[577] In contrast to Google, Twitter's definition of 'sensitive categories' focuses more on traditional notions of vulnerability and prohibits targeting on the basis of: the alleged or actual commission of a crime; health; negative financial status or condition; racial or ethnic origin;

---

[574] Twitter Business, 'Hateful content', Web page <https://business.twitter.com/en/help/ads-policies/ads-content-policies/hate-content.html>.
[575] Google, Advertising Policies Help, 'Personalized advertising', Web page <https://support.google.com/adspolicy/answer/143465 - 547>.
[576] Ibid.
[577] Twitter Business, 'Targeting of Sensitive Categories', Web page <https://business.twitter.com/en/help/ads-policies/campaign-considerations/targeting-of-sensitive-categories.html>.

religious or philosophical affiliation and/or beliefs; sexual orientation; gender identities other than cisgender; political affiliation and/or beliefs; trade union membership; and genetic and/or biometric data. The effect of this difference is that while targeting based on a key word such as 'divorce', may be prohibited on Google, advertisers may be able to do so on Twitter.

Facebook also prohibits the use of targeting options for discriminatory or predatory purposes. In addition, in 2018 Facebook began focusing on restricted advertisers' ability to target or exclude vulnerable groups by removing thousands of advertising categories and keywords relating to potentially sensitive attributes from its exclusion targeting offering.[578]

While not applicable in Australia, all platforms maintain policies relating to access to opportunities. These impose further restrictions on advertising in relation to housing, lending, and employment opportunities for users in the US and Canada.

Data Collection restrictions

Google and Facebook also restrict advertisers from collecting information relating to vulnerability through their personalised advertising products. Notably, Twitter, Snapchat and Apple do not have similar restrictions in place. These prohibitions apply to the collection of such data by advertisers and do not apply to data collection by Google and Facebook themselves.

Google prohibits advertisers from collecting information based on the sensitive interest categories outlined above in relation to its targeting features including audience targeting, location targeting and keyword contextual targeting.[579] Facebook's prohibition is more limited and prohibits advertisers collecting information through creating lead adverts questions, a specific form of collection, to request information, that may relate to vulnerable groups. Questions prohibited include questions about criminal history, financial information, health information, race or ethnicity, religion and sexual orientation.[580]

(ii) Community guidelines

In addition to policies relating to advertising content, Facebook, Google, Apple, Twitter and Snapchat all maintain community guidelines which govern user-generated content on platforms. While such policies apply broadly to all users, community guidelines offer specific protections that again may be of heightened importance to vulnerable groups. Of particular relevance, all platforms evaluated maintain prohibitions on hateful conduct as well as requirements of integrity and authenticity, and prohibitions of deceptive practices.

Platforms adopt a fairly consistent approach to defining hateful conduct as encouraging discriminatory conduct, demeaning conduct, or the promotion of violence in relation to protected characteristics. Facebook defines hateful conduct as a 'direct attack' but also

---

[578] Facebook for Business, *Reviewing Targeting to Ensure Advertising is Safe and Civil* (25 April 2018) <https://www.facebook.com/business/news/reviewing-targeting-to-ensure-advertising-is-safe-and-civil?ref=fbb_blog>.
[579] Google Support, 'Personalised advertising', Web page <https://support.google.com/adspolicy/answer/143465?hl=en-AU>.
[580] Facebook, 'Overview', Web page <https://www.facebook.com/policies/ads/>.

includes the promotion of violence and threats.[581] Google similarly adopts the notion of the promotion of violence and hatred on the basis of protected characteristics,[582] whilst Twitter adopts a broader approach towards defining hateful conduct as any conduct that promotes violence or discrimination, or demeans and defames, on the basis of protected characteristics.[583]

There is also, broadly, a consistency of approach among platforms in defining protected characteristics. Among all platforms evaluated, protected characteristics include caste, serious disease or disability, gender identity and expression, nationality, race, immigration status, religion, gender and sexual orientation. Additionally, all platforms cite age as a protected category, with the exception of Facebook, which only protects against attacks on the basis of age when paired with another protected characteristic.[584] Snapchat lists additional protected characteristics – namely, socio-economic status, weight and pregnancy.[585]

In addition to prohibiting hateful conduct, Facebook discourages cruel and insensitive conduct, which it defines as content that targets victims of serious physical or emotional harm.[586]

(iii) Controls

Facebook, Google and Twitter offer controls for to users who are physically or mentally incapacitated, allowing family members and friends of incapacitated users to remove accounts. Facebook allows requests for account removals and special requests through a form-based submission. Similarly, Twitter requires users to request such action through filing a form-based request, but management is limited to account removal. Google offers more substantial account management for such users through its 'Inactive Account Manager Tool', which allows trusted contacts previously designated by the account owner access to account data.

Of relevance to vulnerable users, all platforms evaluated provide controls which allow all users to turn off personalisation and targeting for advertising. This gives vulnerable users the opportunity to protect themselves against viewing ads which, to the extent possible in light of the restrictions discussed above, have been directly targeted to them based on a perceived vulnerability. However, these controls do not prevent vulnerable users from seeing contextual, non-targeted ads which they may deem to be sensitive. Notably, Facebook goes further in this regard by enabling users to hide ads from particular advertisers, elect to see

---

[581] Facebook, 'Hate speech', Web page <https://www.facebook.com/communitystandards/hate_speech>.
[582] Google Support, 'Hate speech policy', Web page <https://support.google.com/youtube/answer/2801939?hl=en>.
[583] Twitter, 'Hateful conduct policy', Web page <https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy>.
[584] Facebook, 'Hate speech' (n 581).
[585] Snap Inc., 'Community Guidelines', Web page <https://www.snap.com/en-US/community-guidelines>.
[586] Facebook, 'Cruel and insensitive', Web page <https://www.facebook.com/communitystandards/cruel_insensitive>.

fewer ads about a predetermined topic and manage the attributes on which they can be targeted.

(iv) **Accessibility**

All platforms evaluated, except for Snapchat, offer a variety accessibility tools and products for vulnerable users. These are generally aimed at users who are blind or have low vision, or who are deaf or hard of hearing, although Apple offers broader accessibility solutions for users with disabilities and attentional disorders.

As producers of underlying technologies (hardware, operating systems, and browsers) through which digital platforms are accessed, Apple and Google are positioned differently. Because content is consumed through these products, the importance of accessibility options and assistive technologies in these products is greater — accessibility options implemented in a website will not be effective unless supported by the browser, operating system and hardware through which it is consumed. Among all platforms evaluated, Apple seems to offer the most comprehensive accessibility tools and features.[587] Apple's 'voiceover' feature provides a verbal description of iPhone activity for users who are blind or have low vision and assists them with tasks through verbal cues.[588] The camera on Apple products also has a 'magnifier' option, which allows users to increase the size of real-world objects. Apple also allows users to enlarge content displayed on Apple products through its 'Zoom' feature and also provides for the upsizing of text in apps.

Apple's accessibility features for the deaf or hard of hearing include closed captioning, 'live listen' which enhances hearing quality on AirPods and Made for iPhone hearing aids, and hearing health tracking through its 'Health' offering.[589]

Apple offers additional accessibility features for other vulnerable groups. Apple includes comprehensive 'Voice Control' to navigate through Apple products by using voice commands; 'Switch Control', which allows for interoperability with assistive technologies such as joysticks and 'Assistive Touch' for users who have trouble using standard gestures such as pinching or typing. Apple also identifies and offers accessibility solutions for users with learning impairments, offering features such as 'Speak Screen' to narrate text, 'Typing Feedback' for typing suggestions and 'Guided Access' which enables parents, teachers and therapists to restrict user's view of Apple products to one app at a time.

Similarly, Google's accessibility offering is substantial.[590] Android products include a designated 'Accessibility Suite', offering a large-screen accessibility menu, voice descriptions of screen content activity, screen reader compatibility for users who are blind or have low vision and Switch Access for compatibility with switches for users with disabilities. As is the case with Apple, Google Chrome supports low-vision features such as

---

[587] Apple, 'Accessibility', Web page <https://www.apple.com/au/accessibility/>.
[588] Apple, 'Vision, For every point of view.', Web page <https://www.apple.com/au/accessibility/vision/>.
[589] Apple, 'Hearing, Catch every word, sign or signal.', Web page <https://www.apple.com/au/accessibility/hearing/>.
[590] Google, 'Products and Features', Web page <https://www.google.com/accessibility/products-features/>.

magnifiers.[591] In addition to imposing accessibility requirements on Android apps, Google's 'Accessibility Scanner' assists app developers in identifying opportunities to improve apps for their users.

Facebook also offers a variety of accessibility features for users who are blind or have low vision, or who are deaf or hard of hearing. Facebook's automatic-alt-text (AAT) feature allows users using screen readers to identify what is displayed on Facebook, including images, using AI.[592] Facebook's facial recognition products enable users who are blind or have low vision to discover who is in their photos, even when untagged.[593] In relation to users who are deaf or hard of hearing, Facebook offers closed caption across Facebook products including videos, ads and Facebook Live.

While Twitter has not always succeeded in accounting for accessibility in its product design, Twitter has recently increased its accessibility efforts and has pledged to add automated captions to audio and video by early 2021.[594]

[591] Ibid.
[592] Shaomei Wu, 'Using AI to help people with visual impairments share images on Facebook', *Facebook Research* (2 November 2018) <https://research.fb.com/blog/2018/11/using-ai-to-help-people-with-visual-impairments-share-images-on-facebook/>.
[593] Joaquin Quiñonero Candela, 'Managing Your Identity on Facebook With Face Recognition Technology', *About Facebook* (19 December 2017) <https://about.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/>.
[594] Dalana Brand and Kayvon Beykpour, 'Making Twitter more accessible', *Twitter* (2 September 2020) <https://blog.twitter.com/en_us/topics/company/2020/making-twitter-more-accessible.html>.

Question 4 — What additional protections/requirements could be put in place to mitigate the risks and potential harms faced by vulnerable groups online?

Question 4a — How have other international jurisdictions and data protection authorities addressed privacy risks and harms faced by vulnerable groups online?

Key finding:

Overseas jurisdictions have adopted a broad range of regulatory measures that directly or indirectly protect vulnerable individuals.

These include requirements for accessibility to respond to vulnerabilities that affect individuals' ability to access and interact with content.

The consent requirements are modified where a data subject lacks capacity to providing consent.

In the EU, the requirement for *free* consent operates to protect individuals whose vulnerabilities put them at risk of coercion, such as where there is an imbalance of power.

Many jurisdictions, including Canada, the EU, Brazil and South Korea, adopt special restrictions on data handling where individuals are particularly exposed to harmful effects. These restrictions, which include fairness and non-discrimination requirements, purpose limitations and restrictions on the use of sensitive data, have special relevance for people in vulnerable positions.

Overseas jurisdictions have addressed the privacy risks and harms faced by vulnerable groups online via various direct and indirect means, as outlined below. The following discussion explores these measures with reference to specific aspects of vulnerability.

(i) Vulnerabilities which affect capacity for informed consent

An example of a law that expressly deals with the situation where an individual is unable to consent is the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), which does so by creating an exception to the requirement for informed consent. Principle 3 states: 'The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information *except where inappropriate'*.[595] A note to the principle further specifies that: 'Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated'. A significant shortcoming of this approach is that the Act does not provide clear guidance on the applicable safeguards where this occurs.

[595] PIPEDA, sch 1, cl. 4.3.

The Netherlands' General Data Protection Regulation Implementation Act[596] makes specific provision for the circumstance where an individual has been placed under guardianship, or is the subject of an administration or protection order. In that case consent must be given by the legal representative, in so far as the data subject has no legal capacity or authorisation to act in the matter, and that person also has authority to revoke the consent.[597]

The GDPR itself deals with the issue more obliquely via the inclusion in its definition of consent that the consent must be informed. For this requirement, the UK ICO's Guide to the General Data Protection Regulation (ICO Guide)[598] states that organisations can generally assume that adults have the capacity to consent unless they have reason to believe the contrary. For the latter case, it states that 'a third party with the legal right to make decisions on behalf of an individual (eg under a Power of Attorney)' can provide consent.

(ii) Vulnerabilities that affect individuals' ability to access and interact with content

A good example of a law which deals with this issue directly is the California Consumer Privacy Protection Act (CCPA). The regulations under the CCPA provide that the notice required at the point of collection of personal information must be 'be designed and presented in a way that is easy to read and understandable to consumers'.[599] Specifically, the notice must be:

- available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California,[600] and
- reasonably accessible to consumers with disabilities. The regulations require in particular: 'For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.'[601]

The Web Content Accessibility Guidelines aim to 'make content more accessible to a wider range of people with disabilities, including accommodations for blindness and low vision, deafness and hearing loss, limited movement, speech disabilities, photosensitivity, and combinations of these, and some accommodation for learning disabilities and cognitive

---

[596] *General Data Protection Implementation Act* 2018 (Netherlands). Unofficial English translation at https://www.dataguidance.com/sites/default/files/dutch_general_general_data_protection_regulation_implemention_act.pdf; Original (in Dutch) at https://wetten.overheid.nl/BWBR0040940/2020-01-01.
[597] Ibid art 5.
[598] Information Commissioner Office UK, *Guide to the General Data Protection Regulation* (22 May 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.
[599] California Consumer Privacy Protection Regulations, California Code § 999.305(a)(2).
[600] California Consumer Privacy Protection Regulations, California Code § 999.305(a)(2)c.
[601] California Consumer Privacy Protection Regulations, California Code § 999.305(a)(2)d.

limitations'.[602] They are based on ensuring compliance with four Principles of Accessibility; that the web content is perceivable, operable, understandable, and robust.

For content to be perceivable it must be presented to users in ways they can perceive. This principle is elaborated in guidelines that relate to:

- providing text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language
- providing alternatives for time-based media (including audio and video)
- creating content that can be presented in different ways (for example simpler layout) without losing information or structure
- making it easier for users to see and hear content, including separating foreground from background.

The second requirement is designed to ensure that user interface components and navigation are operable. This principle is detailed in guidelines that relate to:

- ensuring accessibility via keyboard
- providing users with enough time to read and use content
- not designing content in a way that is known to cause seizures or physical reactions (eg via use of multiple flashes)
- providing ways to help users navigate, find content, and determine where they are
- making it easier for users to operate functionality through various inputs beyond keyboard.

The third requirement is designed to ensure that the information and operation of the user interface is understandable. This principle is set out in guidelines that relate to:

- making text content readable and understandable
- making Web pages appear and operate in predictable ways
- helping users avoid and correct mistakes.

Finally, the requirement for robustness is designed to ensure that content is sufficiently robust to enable it to be interpreted by a wide variety of user agents, including assistive technologies. This principle is implemented by guidelines that aim to maximise compatibility for current and future user agents, including assistive technologies.

The GDPR is less prescriptive and requires that for consent to be valid 'in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an

[602] Web Content Accessibility Guidelines (WCAG) 2.1, W3C Recommendation 05 June 2018, Abstract <https://www.w3.org/TR/WCAG21/#compatible>.

intelligible and easily accessible form, using clear and plain language'.[603] It further specifies that '[a]ny part of such a declaration which constitutes an infringement of this Regulation shall not be binding'.[604]

There is also a guidance document issued by the Irish Data Protection Commissioner, which discusses user interfaces in the context of consent to cookies and other tracking technologies.[605] This contains the following advice:

> Take accessibility into account in designing your interfaces. If you use colour schemes for your cookie banners or your sliders and checkboxes that blend into the overall background of your site, these settings can be hard to navigate, particularly for people with vision impairments or colour blindness. While binary, colour-coded sliders or buttons may purport to signify a YES and NO option or an ON and OFF option, these colour schemes are not always accessible or self-explanatory to users who do not see colours the same way as other people. Consider testing your interface with users who have vision or reading impairments to make them as accessible as possible to all users.[606]

(iii) Vulnerabilities that expose individuals to risk of coercion

The GDPR responds to vulnerabilities that expose individuals to a risk of coercion in two ways.

First, it deals with it via its requirements for the data protection impact statements (DPIAs). As explained below DPIAs are required where processing operation is "likely to result in a high risk". A relevant criterion for making this assessment is whether the processing involves the data of vulnerable data subjects, which been explained on the following basis.

> the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include … employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.[607]

Second, it deals with this issue indirectly by requiring that consent to processing is 'freely given […] by a statement or by a clear affirmative action, signifying] agreement to the processing of personal data'.[608] Consent has been interpreted as requiring 'active behaviour

---

[603] GDPR art 7(2).
[604] Ibid.
[605] Data Protection Commission (Ireland), *Guidance Note, Cookies and other tracking technologies* (April 2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance note on cookies and other tracking technologies.pdf>.
[606] Ibid, p 13.
[607] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making* (n 459) 10.
[608] GDPR art 4(11).

on the part of the data subject with a view to giving his or her consent'.[609] If this is lacking the data controller must rely on some other ground to justify the processing activities. Alternative grounds are available under art 6, which provides that processing is lawful if and to the extent that:

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The European Data Protection Board's guidelines on consent under the GDPR[610] state that:

> As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[611] … Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.[612]

These guidelines mention that there is likely to be an imbalance of power in the relationship between the controller and the data subject in the case of public authorities[613] and also in the employment context.[614]

The ICO Guidance takes a similar approach, also highlighting these two specific instances:

---

[609] Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, Case C-673/17 (1 October 2019) ECLI:EU:C:2019:801, [54].
[610] European Data Protection Board, *Guidelines on consent under Regulation 2016/679* (Version 1.1, adopted on 1 May 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
[611] Ibid, [13], citing Article 29 Working Party, *Opinion 15/2011 on the definition of consent* (WP187), 12.
[612] Ibid, citing GDPR Recitals 42, 43 and Article 29 Working Party, *Opinion 15/2011 on the definition of consent* (ibid) [12].
[613] Ibid, [16].
[614] Ibid, [21].

> Freely given consent will also be more difficult to obtain in the context of a relationship where there is an imbalance of power – particularly for public authorities and employers.[615]

However, it is clear that the situations where there may be power imbalances extend more broadly. It follows that this requirement may also address the issues of coercion that may arise in the context of individuals in residential aged care and students, including tertiary students.

(iv) Vulnerabilities that expose individuals to harmful effects

Canadian 'no-go' zones under the purpose limitation clause

The Canadian Personal Information Protection and Electronic Documents Act[616] contains an important **purpose limitation clause** that applies to collection, use and disclosure of personal information. Subsection 5(3) states that:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

In applying subsection 5(3), Canadian courts have generally taken into consideration whether the collection, use or disclosure of personal information is directed to a bona fide business interest, and whether the loss of privacy is proportional to any benefit gained.[617] The following factors have been stated to determine whether an organisation's purpose complies with subsection 5(3):

- the degree of sensitivity of the personal information at issue;
- whether the organization's purpose represents a legitimate need / bona fide business interest;
- whether the collection, use and disclosure would be effective in meeting the organisation's need;
- whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- whether the loss of privacy is proportional to the benefits.[618]

The OPC has published an interpretation of subsection 5(3) that includes certain so-called 'no-go zones'. These include: 'Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law' and 'Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual'.

---

[615] Information Commissioner's Office UK, *Guide to the General Data Protection Regulation (GDPR)* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ - what2>.
[616] Ibid, 7.
[617] See, for example, *A.T. v Globe24h.com*, 2017 FC 114.
[618] *A.T. v Globe24h.com*, 2017 FC 114, [74]; *Turner v Telus Communications Inc*., 2005 FC 1601, [39], aff'd 2007 FCA 21, [48].

Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law

The OPC Guidance contextualises this issue with reference to big data and emphasises the need to understand the collection between upstream data processing practices and downstream discrimination. It comments that:

> Data analytics—or any other type of profiling or categorization—that results in inferences being made about individuals or groups, with a view to profiling them in ways that could lead to discrimination based on prohibited grounds contrary to human rights law would not be considered appropriate under subsection 5(3)'s 'appropriate purpose' test.[619]

It further explains that determining whether a result in 'unfair or unethical' requires a case-by-case assessment.

Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual

The OPC Guidance acknowledges that individuals make privacy trade-offs to exercise their freedom as consumers in the digital marketplace, but goes on to express the OPC's belief that:

> a reasonable person would not consider it appropriate for organizations to require an individual to undergo significant privacy harm as a known or probable cost for products or services. By 'significant harm', we mean 'bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property'.[620]

A commentary on this guidance has interpreted it as follows:

> The OPC's premise is that if an organization identifies potential harms that may arise from the collection, use or disclosure of personal information, PIPEDA's accountability principle[621] will require that the organization will seek to minimize this risk. In some cases, mitigation efforts will reduce the risk significantly. In other cases the risk will remain meaningful. Only meaningful residual risks of significant harm must be notified to individuals.[622]

---

[619] Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices* (n 272).
[620] Ibid, under heading "3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual".
[621] Citing OPC, *PIPEDA Fair Information Principle 1 – Accountability* (August 2020) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/>.
[622] Derek Lackey, *PIPEDA: Guidelines for obtaining meaningful consent* (26 April 2020) <https://bestofprivacy.com/guidance/pipeda-guidelines-for-obtaining-meaningful-consent/>.

Protections of vulnerable people under the GDPR

The GDPR contains a number of provisions that are of assistance in protecting individuals who fall in the category of vulnerable persons.

Article 5, which sets out the principles governing processing, requires that **processing must be fair**.[623] The Article 29 Data Protection Working Party's Guidelines on Automated individual decision-making and Profiling[624] state that:

> Profiling may be unfair and create discrimination, for example by denying people access to employment opportunities, credit or insurance, or targeting them with excessively risky or costly financial products.[625]

The Article 29 Guidelines also give the following example of a situation where processing would not meet this requirement:

> A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as 'Rural and Barely Making It', 'Ethnic Second-City Strugglers', 'Tough Start: Young Single Parents') or 'score' them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other 'non-traditional' financial services (high-cost loans and other financially risky products).[626]

The GDPR also contains special rules which **limit the circumstances in which it is permissible to process special categories of data**. The Article 29 Guidelines mention the situation where processing creates 'special category data' by inference from data which is itself not special category but becomes so when combined with other data. They comment that this would occur, for example, where correlations 'indicate something about individuals' health, political convictions, religious beliefs or sexual orientation'.[627] In that case the processing must not be incompatible with the original purpose and there must be a lawful basis for the processing of the special category data.[628] The grounds for lawful processing of special categories of data are set out in Article 9(2) and are narrower than those for the processing of other personal data under art 6 (specifically they do not include the legitimate interests of the controller[629]).

Another feature of the GDPR's lawfulness constraints is the requirement for **compatibility with the purpose of collection** in cases where some ground for processing other than

---

[623] GDPR art 5(1)(a).
[624] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making* (n 459).
[625] Ibid, 10.
[626] Ibid. A footnote explains that this example is taken from: United States Senate, Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, Staff Report for Chairman Rockefeller (18 December 2013) <https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-ondata-broker-industry.pdf>.
[627] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making* (n 459) 15.
[628] Ibid.
[629] See GDPR art 6(1)(f).

consent is relied upon.[630] It further requires that in assessing compatibility the controller must take into account specified matters, including whether the processing of types of data that qualify for additional safeguards (ie as special categories of personal data or personal data related to criminal convictions and offences[631]) and consideration of 'the possible consequences of the intended further processing for data subjects'.

A final relevant feature of the GDPR is that it requires the preparation of Data Protection Impact Assessments (DPIAs) when processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.[632] The Spanish Data Protection Agency has published guidance outlining the processing activities that require a DPIA. This includes provides the category of vulnerable data subjects, the processing of whose data is considered to increase the need to carry out a DPIA. Consistently with the WP29 Guidelines, it takes the view that when a processing operation meets two or more of the criteria included in the Blacklist, it will be necessary in most cases to carry out a DPIA. These include:

> Data processing regarding vulnerable subjects or those who are at risk of social exclusion, including the data of persons aged under 14, older people with any kind of disability, the disabled, persons who access social services, and the victims of gender-related violence, as well as their descendants and persons who are in their guardianship or custody.[633]

Protections of vulnerable people in other jurisdictions

An alternative approach taken in Brazil is to directly **prohibit processing data for discriminatory, unlawful or abusive purposes**. Article 6 of the General Data Protection Law requires personal data processing activities to observe good faith and comply with specified principles, including the non-discrimination principle, which prohibits the processing data for 'unlawful or abusive discriminatory purposes'.[634]

South Korea uses a similar approach but leaves the specific harms to be prescribed by Presidential decree. It **prohibits the processing of data that qualifies as 'sensitive data' subject to exceptions** where consent is provided[635] or where other statutes require or permit it. Sensitive data includes data concerning ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information

---

[630] GDPR art 6(4).
[631] These are protected under Articles 9 and 10, respectively, and generally equate with the categories of 'sensitive data' as defined in *Privacy Act 1988* (Cth) s6(1).
[632] GDPR art 35(1). See further Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01) (4 October 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.
[633] Spanish Data Protection Agency (Agencia Española de Protección de Datos), *List of the Types Of Data Processing that Require a Data Protection Impact Assessment Under Art 35.4*, 3, <https://www.aepd.es/media/criterios/listas-dpia-en-35-4.pdf>.
[634] Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais), as translated by iAPP <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/>.
[635] *Personal Data Protection Act* (South Korea) 2020, art 23, <https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG>. If consent is relied upon, the controller must inform that data subject of specific matters as spelt out in art 15(2) (information required to be disclosed in relation to the collection and use of personal Information) and art 17(2) (information required to be disclosed in relation to the disclosure of personal information to others).

which is likely to harm the privacy of data subjects as prescribed by the Presidential Decree.[636]

The right to erasure as a safety net

Finally, it should be noted that the mechanism of a right to erasure, which exists in the GDPR and the CCPA, as discussed above at 2(a) in relation to children, can likewise function as a safety net that allows (at least partially) for the retrieval of information that may result in harmful effects for vulnerable individuals.

[636] Ibid.

Question 4b — How can meaningful consent be obtained on behalf of individuals who are physically or legally incapable of making their own privacy decisions? If possible, provide examples of best practice models or mechanisms in the online environment including consideration of effective parental/guardian consent models.

Key findings:

The capacity to provide consent needs to be assessed issue-by-issue. Capacity to make one's own privacy decisions may depend on the complexity of the practice in question and the risk involved in the data collection, use and disclosure.

It is essential to ensure that individuals who have difficulty making their own privacy decisions are supported as much as possible.

Overreliance on guardian-consent models runs the risk of infringing on vulnerable persons' autonomy and their right to make decisions that affect their lives.

Before changes the current requirements are proposed, there should be further consultation with stakeholders and further research to ascertain the extent to which inability to provide meaningful consent presents issues for data processing by platforms and commercial websites.

Capacity is an attribute that is unique to the individual context. It follows that assessment of capacity requires some knowledge about the individual and their personal circumstances. In the case of transactions with platforms and online websites, the fact that an individual is participating online makes it unlikely that they lack the physical ability to communicate consent. The issue of lack of factual incapacity to make decisions with understanding of their effect is therefore likely to be the predominant one. This may not be known, or reasonably expected to be known by the entity seeking consent, unless the entity holds information that reveals or raises a strong inference that the individual is unable to provide meaningful consent (eg. because it provides a service or product directed at persons likely to have a factual incapacity to make decisions with understanding of their effect).

In cases where an individual is both incapable of giving meaningful consent and lacks a legal representative, and those facts are known to the entity seeking consent, there are two possible solutions available. The first is to require a processor to make use of any informal arrangements available to the individual of which they are aware; that would enable the individual to provide consent, albeit that it supported by the informal arrangement. As observed by the ALRC, '[d]ecision-making arrangements for persons with disability take many forms along a spectrum, including: informal arrangements – usually involving family members, friends or other supporters…'.[637]

[637] ALRC Equality Report (n 483) [2.52].

The NSW IPC's guide expands on this issue as follows:

> It is not always possible to use substitute decision-making. In some cases a person may not have a close relative, friend or other representative who can act on their behalf. In other cases, the views or interests of the person's representative may conflict with the person's current opinions or with a wish or opinion previously expressed by the person when they had capacity. In this situation, the views of the person's representative should not automatically override the person's views. A further limit to using substitute consent is where there are irreconcilable differences between family members about what is in the best interests of their relative.[638]

(i) Where the processor has actual or constructive knowledge that an individual lacks capacity to give meaningful consent

In cases where an individual is both incapable of giving meaningful consent and lacks a legal representative, and those facts are known to the entity seeking consent, there are two possible solutions available. The first is to ascertain and make use of any informal arrangements available to the individual. As observed by the ALRC, '[d]ecision-making arrangements for persons with disability take many forms along a spectrum, including: informal arrangements – usually involving family members, friends or other supporters…'.[639]

The NSW IPC guide suggests that:

> Generally, the more privacy-intrusive the proposed conduct or use of personal information, the greater the care required to provide appropriate information and support to enable a person to exercise their capacity to the greatest possible extent.
>
> For example, a person with a mild intellectual disability may be able to understand a simple notification form advising about the routine collection of personal information. However, if consent is sought in relation to the collection, use and disclosure of sensitive personal information for research purposes, the same person may need a support person to help explain the effects of a decision to consent to or refuse the conduct.[640]

The other possible solution is to require reliance on some ground other than consent to authorise processing of their information. Grounds of this type already exist in item 1 of 'permitted general situations' in s16A of the Privacy Act and the 'permitted health situations' provision in s 16B, which are applicable to health data.

(ii) Where the processor has no reason to be aware that an individual lacks capacity to give meaningful consent

That still leaves the situation where an entity has no reason to be aware that an individual lacks the capacity to give meaningful consent. The current law starts with a presumption of capacity, which can be rebutted by proving a lack of the required level of understanding. Any processing by an entity that relies for its validity on consent is an 'interference with the

---

[638] IPC NSW Guide (n 488) 13.
[639] ALRC Equality Report (n 483) [2.52].
[640] IPC NSW Guide (n 488) 8.

privacy of an individual'[641] to the extent that lack of capacity is proven and there is no other lawful basis, as discussed above. However, the issue of capacity is unlikely to be pursued in most instances, which leaves unaddressed any harms that may have already been caused. Any changes that increase the requirements for processors are likely to be onerous for them and/or expose them to regulatory action; the also run the risk of exposing information subjects to more privacy invasive activities.

This is not an issue that lends itself to any obvious solutions. In these circumstances it would be useful to consult further with disability support groups and industry representatives and also to carry out further research to ascertain the extent to which inability to provide meaningful consent presents issues in the context of processing by platforms and commercial websites.

There is also a case for ensuring the Code does not rely solely on consent as basis for protecting the interests of consumers and that it contains additional restrictions directed at any processing activities that are likely to be harmful to them, as discussed below.

Recommendation 24

Before any specific measures are considered for decision-making arrangements for individuals lacking capacity to give meaningful consent, there should be:

- consultation with both disability support groups and industry representatives, and
- further research to ascertain the extent to which inability to provide meaningful consent presents issues in the context of processing by platforms and commercial websites.

[641] Privacy Act, s 13.

Question 4c – Consider whether particular measures or requirements should apply to privacy policies and notification practices in relation to individuals physically or legally incapable of providing consent.

Key findings:

The best way to improve consent process for people who have limited capacity to provide consent is to improve the transparency and accessibility of privacy notices/policies and to reduce their complexity.

Where an individual is supported or represented in their decision-making, it should be a requirement that notice is also to be provided to the supporter or decision make.

(i) Supported decision making and enhancing capacity

As discussed in section 3a above, questions of capacity require an individualised assessment that also has regard to the context and decision in question. They should be approached through the lens of the National Decision-Making Principles, and from the understanding that:

> [a]ll adults, except in very limited circumstances, have some level of decision-making ability and should be entitled to make decisions expressing their will and preferences, but may require varying levels of support to do so.[642]

The preferable approach is not to adopt a static or binary view of capacity and decision-making based on particular characteristics, but to focus on what level of support, or what mechanisms are necessary, to enable people to express their will and preferences.

So, as for children, privacy transparency should aim not only for the disclosure of material facts about the handling of personal information, but also to educate and empower users and enable privacy self-management, accounting for their varying needs and capabilities.

As discussed in section 2d and 2e above, almost two in three (63%) Australians are not confident that they understand privacy policies (when they read them).[643] However, there is extensive literature and broad agreement that privacy transparency can be improved through:

- using the most effective tools and strategies for clear communication
- taking into account individuals' specific needs, vulnerabilities and contexts, and
- adopting design practices around privacy disclosures that involve children and vulnerable persons to ensure effectiveness.

---

[642] ALRC Equality Report (n 483) [4.12].
[643] OAIC Community Attitudes Survey (n 310) 70.

Recommendations 4 to 8 are directed at reducing the barriers that all individuals face in accessing and understanding information about what is being done with their personal information. A greater degree of organisational accountability for designing less complex and more accessible privacy transparency measures, combined with a higher baseline for formal notifications as recommended by the ACCC would enhance capacity, enabling more people to make more meaningful decisions about their privacy with less support.

Requiring platforms to design the content, style, mode of delivery and timing of privacy notifications to account for the varying needs, capabilities and behaviours of users serves to ensure that there are explanatory materials appropriate for individuals (and their supporters or representatives) across the spectrum of ability.

(ii) Universal design

The goal should be to encourage more universal and user-centric design around transparency measures so that they are more responsive to users' needs. Many of the tools and strategies for clear communication that are outlined in response to questions 2d and 2e assist all users – not just children, but also those with disabilities or other vulnerable groups. However, in some cases, measures aimed at supporting one group will be unhelpful or counterproductive for another. Individual needs are diverse, and designing to meet them is complex. For example, an adult may suffer from loss of specific functions, such as language or memory, and may be alienated by explanatory content designed to resonate with a young child. Though there is already a substantial body of literature, standards and guidelines in this space,[644] as the ACCC observes, ongoing research and development is required to understand the most effective ways of communicating privacy information to individuals with diverse needs.

Our recommendations focus on the organisational processes and factors considered in the design, maintenance, and improvement of transparency measures, rather than prescribing the nature of notifications themselves. This is in keeping with the technologically neutral and principles-based approach of the Privacy Act, and supports a move away from once-off notification towards a more holistic approach to privacy transparency embedded throughout a product or service. Additionally, this approach gives organisations more flexibility to determine the best mechanisms for transparency, and avoids a proliferation of privacy notices pitched for different audiences that could increase compliance costs as well as generate more complexity and confusion for users.

Recognising that the needs, capabilities and behaviours of individuals with cognitive disabilities or other limitations to capacity do not map directly on to the developmental stages for children, and recognising the need for further research and consultation in this area, it is still possible to adopt a high-level approach to privacy notifications that would meet the support needs of adults with cognitive disabilities and children. Building on the discussion

---

[644] See, eg, Lisa Seeman et al, 'Making Content Usable for People with Cognitive and Learning Disabilities', W3C Web Accessibility Initiative (17 July 2020) <https://www.w3.org/TR/coga-usable/>; Scott Hollier, *Cognitive Disability Digital Accessibility Guide* (Media Access Australia, April 2020) <https://centreforinclusivedesign.org.au//wp-content/uploads/2020/04/cognitive-disability-digital-accessibility-guide.pdf>; 'ICT Guidelines for Practice', Centre for Universal Design Australia <http://universaldesignaustralia.net.au/category/ud-and-ict/ict-guidelines-for-practice/>.

under questions 2d and 2e above, and on the varying levels of decision making support an individual might need as outlined in the ALRC Equality, Capacity and Disability in Commonwealth Laws report,[645] we can provide high level guidance for how privacy notices and policies should be deployed for best effect:

Support needs	**Notice guidance**
Full support — a person may choose someone else to make decisions for them, or it may be necessary to appoint someone to do so.	Privacy notifications and policies should be targeted at parents/supporters/representatives and provided at sign-up and on demand. Reliance on contextual notifications and prompts to alter privacy settings during use should be limited.
High support — for example, a person may require support to obtain information, have the information explained to them in an appropriate way, receive advice about the possible decisions they might make, communicate their decision, and follow through to ensure their decision is given effect.	Privacy notifications and policies should be targeted at parents/supporters/representatives and provided at sign-up and on demand. Reliance on contextual notifications and prompts to alter privacy settings during use should be limited. Appropriately pitched, explanatory materials should be provided for users in context. Services could also provide materials to assist supporters to explain privacy concepts and risks.
Low to medium support — for example, a person may require support to obtain information, have the information explained to them in an appropriate way, and receive advice about the possible decisions they might make.	Privacy notifications and policies should be targeted at users (appropriately pitched) as well as parents/supporters/representatives. Contextual notifications and prompts for privacy decisions may be appropriate, but users should be encouraged to discuss with a parent or supporter.
Minimal support — for example, a person may require no support, or require some assistance obtaining information, but when provided with the information is then able to make the necessary decision. Similarly, the person may only	Privacy notifications and policies should be targeted at users (appropriately pitched) as well as parents/supporters/representatives.

[645] ALRC Equality Report (n 483).

require support to communicate their decision to a third party.	

(iii) APP 5 and substituted decision-makers

Under APP 5, notice of the collection of personal information must be provided to the individual about whom the personal information is, regardless of that individual's capacity. No provision is made for notice to supporters, representatives or substituted decision-makers.

As a result, even where a nominated representative has been appointed, or a parent or guardian provides consent on behalf of an individual, APP 5 does not require any notification to be directed at that decision maker.

In our view, it is appropriate for APP 5 to continue to apply to the individual to whom the personal information relates. However, where an individual is supported or represented in decision-making, APP 5 should also require that notice be provided to the supporter or decision maker.

Recommendation 25

The Code should extend APP 5 to require that any privacy notices required to be provided to an individual also be provided to a nominated supporter or decision maker, where one exists.

We recommend this also as an economy-wide measure.

Question 4d — What additional protections could be imposed to mitigate the privacy risks and harms faced by individuals physically or legally incapable of providing consent in the online environment?

Key findings:

Individuals who lack capacity or require support in their privacy decision-making would benefit from any protections introduced to protect vulnerable individuals more broadly.

As has been discussed above, individuals physically or legally incapable of providing consent in the online environment are a very limited group. Wherever possible, adults who have some level of decision-making ability should be supported to make their own decisions and express their own preferences.

We do not recommend any additional protections be imposed directed solely towards individuals physically or legally incapable of providing consent in an online environment. However, many of the recommendations below for vulnerable groups more broadly would provide meaningful protection to individuals who may lack capacity or require support.

Question 4e — Any additional requirements or protections to ensure the privacy of vulnerable groups is protected online

Key findings:

Implementing requirements that protect people's privacy generally will help protect vulnerable people. There is also a close relationship between particular measures for children and measures for other vulnerable individuals.

There would be significant benefits in introducing a 'fair, lawful and reasonable information handling' requirement, requiring mandatory PIAs, privacy-default settings, and transparency about profiling, banning nudge techniques, and introducing the right to erasure.

There would also be benefits in mandating complete or partial compliance with accepted standards for accessibility, such as currently the Web Content Accessibility Guidelines 2.0 (WCAG).

We have established above that vulnerability is best understood as arising from the totality of the circumstances affecting an individual, rather than from a single characteristic (or set of characteristics) that can be identified in advance. This makes it difficult to target specific protections to members of particular groups. Additionally, care should be taken when considering any requirements which may require platforms to proactively identify members of the protected group, as this may in itself negatively impact on their privacy.

As a starting point, we consider that the best way to secure the privacy of vulnerable adults online is through strong baselines protections for all adults, combined with flexible obligations to take greater care or apply additional protections or provide greater support where vulnerabilities are disclosed or detected. Where individuals are at risk that their specific privacy needs that are not met by these general protections, additional requirements could be considered, in consultation with the affected individuals and representative organisations.

(i) General protections

Many of the recommendations made in response to question 2f above apply equally to other vulnerable groups. We repeat those recommendations for the following general protections:

Fair, lawful and reasonable information handling

Recommendation 26

In addition to the matters listed under Recommendation 10, the Code should include the following factors to be considered in determining whether a collection, use or disclosure is fair and reasonable in the circumstances:

- any information the APP entity has, or ought to have, about the likely vulnerabilities of their users
- the appropriateness in the circumstances of enquiring about or verifying whether a user is vulnerable in a particular way before processing their information

- any privacy harms that could result from processing and any measures that could be taken to prevent them.

As discussed above, we consider that a general duty to handle personal information in a manner that is lawful, fair and reasonable presents the most efficient and effective means of establishing a balance between organisational and individual interests, and also allows for a variable standard of protection to be applied for children and other vulnerable groups.

An obligation of this type would require organisations to examine whether their information processing is appropriate in all the circumstances. Additional provisions in the Code, or in guidance, could outline the range of factors that may indicate or contribute to a person's vulnerability, and what makes each of those groups vulnerable.[646] Guidance could also clarify the range of matters that APP entities should take into account when assessing whether processing is fair and reasonable. For the protection of vulnerable users, these could include:

- any information the APP entity has, or ought to have, about the likely vulnerabilities of their users
- the appropriateness in the circumstances of enquiring about or verifying whether a user is vulnerable in a particular way before processing their information
- any foreseeable privacy harms that could result from processing and any measures that could be taken to prevent them.

Consideration of the overall lawfulness, fairness and reasonableness of processing could be included in a PIA process (discussed below).

Privacy Impact assessments

Recommendation 11 is that the Code require digital platforms to conduct a PIA for all online products and services, and for all new products and services prior to launch.[647] In addition to considering the best interests of children, PIAs should include consideration of the ways in which customers may be vulnerable to harm as a result of the project, and whether the information handling is lawful, fair and reasonable in the circumstances. This requirement will increase the likelihood that risks to vulnerable people are identified and mitigated prior to the launch of a service.

Nudging, default settings

Recommendations 12 and 13 prohibit 'nudge' techniques and require platforms and services to be pre-configured with the highest privacy settings by default. This will help protect individuals at greater risk of harm from misuse or disclosure of personal information (eg. a survivor of family violence). It will also support individuals with more limited technical, critical and social skills to start from a safer base and exercise greater control and autonomy over their settings.

---

[646] See sections 3b and 3c above.
[647] And that an economy-wide requirement to conduct a PIA for all 'high privacy risk projects' be introduced.

Transparency regarding profiling

Recommendation 14 is that wherever a person is profiled, they must be provided with information explaining the process and its implications for them, and they must be able to express their point of view about their profile. This is particularly important for groups that are vulnerable to greater or different harms than others by virtue of certain characteristics. This would include profiling that may put individuals at risk of being targeted with inappropriate products or scams, discriminated against, or inappropriately excluded from markets.[648]

Right to erasure

Recommendation 15 is that a right to withdraw consent be formalised as part of the Code, pending the establishment of a full right to erasure as part of the broader Privacy Act reforms. This would further enhance control for individuals at greater risk of harm from misuse or disclosure of personal information, and also provide greater opportunity for those less able to consistently engage with the internet in a safe and beneficial manner to recover from mistakes.

(ii) Specific protections

Where individuals have a persistent need that is not addressed by the general protections, additional requirements should be considered, in consultation with the affected individuals and their representative organisations.

Accessibility of privacy information and controls

Recommendation 27

The Code should require that privacy policies and privacy controls be provided in formats that are accessible, according to current, generally accepted accessibility standards or guidelines.

Many digital platforms do not deliver privacy information or privacy controls in a manner that is accessible.[649] As a result, people who are blind or have low vision, or who have other disabilities and rely on assistive technologies to interact with the web, do not have the same access to information about privacy, or to the same degree of choice and control as the rest of the community. The Web Content Accessibility Guidelines 2.0 (WCAG), are widely accepted as a shared standard for accessibility. As discussed above,[650] the WCAG are adopted as the accessibility standard under CCPA. Vision Australia states that, in general, digital content will not be accessible unless it complies with WCAG. Further consultation would be required to establish the level of conformance to WCAG or other standards that

---

[648] ACCC *DPI Final Report* (n 3) 447.
[649] Bruce Maguire and Karen Knight, 'Vision Australia Submission to the Digital Platforms Inquiry Issues Paper' (29 March 2018) <https://www.accc.gov.au/system/files/Vision Australia %28April 2018%29.pdf>.
[650] See section 4a(ii) above.

should be required. For example, the Consumer Experience Standards for the Consumer Data Right specify certain elements of WCAG that the Consent Model must comply with.[651]

This requirement should also be considered as an economy-wide measure, though this may give rise to concerns about compliance costs for smaller businesses, as WCAG compliance can be an expensive exercise (particularly if the small business exemption were removed). These concerns may be addressed by prioritising a subset of the WCAG rules that must be complied with. It may well be that technical or market-based solutions would bring the cost of WCAG compliance down as well, should it be mandated. In any case, we consider the benefit in terms of accessibility would outweigh the cost to business.

[651] Consumer Data Standards, *Consumer Experience Standards* (17 July 2020) <https://consumerdatastandardsaustralia.github.io/standards/pdfs/CX-Standards-v1.4.0.pdf> 15.