Comments provided to the Office of the Privacy Commissioner – Children and Young People's Privacy Project

30 November 2023

Thank you for the opportunity to provide comment on the Children and Young People's (CYP) Privacy Project. The Foundation's position statement on the Privacy Act 2020 dated 17 November 2020 supported the heightened attention paid to collecting information from children and young people, but also commented that further review, research and concerted action was needed by both the Privacy Commissioner and agencies, to give effect to this.

We welcome your Office reviewing this important area of privacy and the chance to contribute to the assessment of how the current laws and regulations are working with respect to the privacy of tamariki and rangatahi.

We note the significant developments overseas (e.g. UK, GDPR) regarding for children and believe we can be guided by their experiences, research, and legislative provisions. For example, we note the EU Kids Online research at the LSE/EU (with parallel projects focused on Latin America). From this research, the London School of Economics and Political Science published its report 'EU Kids online 2020', which surveyed 19 countries and mapped internet access, online practices, skills, and online risks and opportunities for children aged 9-16 years in the EU.

This, together with other international research provides valuable insights into children's online practices, risks and experiences, which Aotearoa can be guided by, while recognising the importance of overlaying our own unique New Zealand perspective and challenges, ensuring our own Te Ao Māori perspectives are accounted for.

We are mindful that in researching this issue, the OPC will need to ensure this is conducted with Treaty principles in mind and that Pākehā, other immigrants, Pasifika and Māori responses could well differ, necessitating particular consideration.

Concerns with respect to children's privacy

We acknowledge at the outset that there are many different areas concerning children and young people's privacy, and that what is important differs with regard to age and level of maturity. In 2022, the Privacy Foundation launched a concerted campaign focused on children's and young people's privacy. In this response document, we largely focus on our comments with respect to research and findings we have conducted on data collection and use by EdTech and the concerns raised, while bearing in mind that there are many other contexts of collection, processing and use of children's data that also engender privacy considerations.

We note for the OPC's information, that our working group also discusses other privacy-related issues concerning children and young people such as (i) 'sharenting', (ii) the potential profiling and commercialisation of children's data and (iii) the opportunities and potential risks of artificial intelligence (AI) for children, through to (iv) emerging issues related to children's use of home devices such as Alexa and other smart technologies. We are aware that rapid advances in AI (including collection and processing of biometric information) raises new challenges. For example, a recent

report by UNICEF (2023) points to opportunities (such as developing personalised learning systems) and risks (e.g. exposure to misinformation, illegal content e.g. creation of photo-realistic child sexual abuse material (CSAM), and manipulation of children's worldviews through microtargeting).

Current Situation

In our inquiries and research, we have found that there is a clear focus on safety issues concerning children's conduct in the digital space, including information and legislative provisions aimed at addressed concerns raised by issues such as online bullying, sextortion and inappropriate content. We commend the efforts of organisations such as NetSafe and other agencies in addressing such issues raised. We also acknowledge the role and importance of legislation such as the Harmful Digital Communications Act 2015, and amendments Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Act 2022) in supporting the work that these agencies do. At the same time, we would submit that while these are helpful, they do not go far enough in protecting children/ young people and their information.

In our responses we recognise children and young people as a vulnerable group whose right to privacy needs special protection. We are guided in our thinking and positioning of this response document by some of the tenets within the EU GDPR which include special provisions for children as well as the UN Convention on the Rights of the Child (UNCRC). We note that given increasing recognition by other jurisdictions coupled with technology advances that can threaten the privacy and dignity of children the time is right, indeed it is urgent, to address the gaps.

We are of the view, with the increasing presence of children and young people online, that Netsafe and other agencies need to expand their work on digital literacy for tamariki and rangatahi and stakeholders working with them. While digital citizenship is important, its focus is on children's conduct rather than on scrutinising the data practices of commercial digital service providers that children interact with. Particular concern is raised about systems that are embedded within digital products and services aimed at children and young people, especially those utilised in schools and other contexts where children, young people and their caregivers have little choice but to engage and share their information.

Our observation, for example in the Edtech space, suggests that the Ministry of Education and other stakeholders apply a rather narrow and static perspective on privacy within the digital environment that CYP engage with, which may increase their vulnerability to the commercial interests of EdTech providers. In our opinion, this approach does not put children's data privacy at the forefront. A strong stance is needed in the case of EdTech providers that ensures the protection of CYP information. Schools are not equipped to do this – leadership must come from the Ministry, the OPC, and other bodies charged with protecting our children and young people.

Children's privacy is commonly thought of as *protecting personal sensitive information from being shared without consent* of the child or their parent among their peers and communities (such as schools). However, children's data privacy in relation to commercial interests, must be given primacy. Though less visible the privacy risks to children are potentially greater and with long term consequences that cannot be easily foreseen. As such, our stance is that tamariki must be protected from third party and commercial influence. Their data should not be commercialised or monetised.

We believe that a position that gives primacy to the protection of children and which balances rights to privacy with innovation in ways that are proportional, ethically responsible and socially sustainable, is sorely needed.

OPC Consultation Document – Our responses

Below, we address selected questions posed in the OPC survey.

Question 1. Who are you?

Response:

Other (please specify) – Privacy Foundation New Zealand

Question 2. Do you know where to see what the rules/laws are and how they apply to children?

In this response we focus on what provisions are in place to protect children's privacy, as opposed to 'where we can find such information'. The aim is to briefly consider the landscape for protecting children and young people's privacy and to identify the gaps.

The UN Convention of the Rights of Children (UNCRC, Art. 16) speaks directly to a child's right to privacy, stating: *1. No child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation. [and] 2. The child has the right of protection of the law against such interference or attacks.* New Zealand, however does not have statutes that expressly protects a child's right to privacy, nor does it have legislations that give legal effect to the provisions of the UNCRC.

In New Zealand, the key legislative structures that give some protection regarding the privacy of an individual (so applies also to children) include NZ Bill of Rights Act, Privacy Act 2020, and the Official Information Act 2010. The Harassment Act 1997 does provide some protection in the case of harassment which can include online posts, email etc. The Harmful Digital Communications Act 2015 also has statutory protections that protect against online harms; although the Act does not mention children specifically, its remit includes protection of children. However, when we look closely at these different provisions, in general, we see limited mention of children specifically.

The key provision regarding children's privacy remains the Privacy Act 2020. Although this legislation makes little mention of children, of the 13 principles, when taken together, IPP4 and IPP6 seem to provide children under 16 years, with specific protections. IPP4 speaks specifically to the rights of the child, stipulating that where personal information is being collected from children or young persons), an agency can only collect that information by a means that, in the circumstances of the case, is fair and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned. IPP6 provides the right to access information.

The Official Information Act 1982 also provides right of access to information pertaining to children, though it does not speak specifically to this group. Other Acts may also make provisions that reflect underlying tenets in the Privacy Act, but the Privacy Act remains the key determining document. This makes it important to 'get it right' in relation to protection of Children and young people's information. It is also important to note that the Privacy Act applies only to agencies (with the exception of section 28(3) exposing a gap when it comes to domestic disclosure of children's information).

The Privacy Act 2020 remains the foremost document to support privacy rights in relation to the collection, processing and use of personal information, but lacks provisions that speak specifically to the privacy rights of a child or young person.

Moreover, there is a tendency for government agencies and organisations to summarise the Privacy Act Information Privacy Principles, for various bodies. While this has the advantage of ensuring understanding of the principles, there are often few if any, concrete details that indicate, for example, how the principles would apply.

In certain respects, this is reasonable as the Principles are intended to be flexible and the Act is technology-neutral. In other settings, there is the risk of exposure of personal information where the importance of privacy and privacy rights are overlooked. A good example where the OPC provided specific guidance on the application of the IPPs (which was immensely useful) regarding the use of cameras in school bathrooms.

Overall, the Privacy Act does not function as a form of data protection regulation such as the GDPR. We suggest that a fuller debate about establishing children's data privacy rights and how these might be enforced is needed.

Question 4. If No, where would you go to find out?

If seeking information about how to protect a child's privacy, the options provided in the answer underline the problem for the average person. Most people's understanding of privacy relates to information that is knowingly shared with others via social media or with organisations when using their services. In such cases, parents or young people may attempt to contact these organisations but in many cases it can be difficult to find appropriate channels to address concerns around consent and privacy breaches.

Netsafe is the organisation promoted most frequently in respect to children's safety on the internet and use of social media networks with harmful consequences. Safety is, however, different from privacy, therefore Netsafe is not always the most appropriate organisation to seek help from. This is particularly the case when wanting to understand what the rules are and what rights children or parents have in relation to digital services, and EdTech. Some people may think to contact a privacy related organisation, and that might be the OPC.

If an educator, or School Trustee, is unaware about privacy regulation, then their professional body and regulator has not provided clear guidance about the importance of a child's privacy. It is key that those who engage with children in a school environment, and in an extra-curricular environment such as sport or the arts, are aware and understand the impact of having access to a child's personal information.

The answer to this question also links to the later answer to question 9 about where someone might turn if they wanted to complain that a child's information had been used without parent/whānau's consent. If an individual does not know where to seek advice, they are unlikely to know where to complain.

Question 5. For those working with children or young people, do you feel that you have access to clear information about the privacy rules that apply to your profession?

We took from this question that there is a perception that there is a lack of clear guidance in a number of professions about the scope of the Information Privacy Principles and how they apply to children. Distilled from this question is that there needs to be improved privacy education in respect of children across a broad range of sectors with appropriate sector-specific guidance. We suggest that examples of the application of the IPPs would support clearer application of the law. Grouping also the OPC's

"AskUs" questions into a specific section related to tamariki, relevant to different sectors would be useful.

Question 6. For those providing services for children (health, education, etc) do you feel well supported in helping them use services and tools (online, government services, etc)?

In this response, we wish to raise a number of issues regarding the New Zealand Educational context. We feel that this is a particularly good example/context, within which to consider the implications for children's privacy given often:

-the lack of voluntariness and active, full consent being given regarding children's use of EdTech,

-the wide-reaching collection and use of children's data that use of such technology entails, and

-the blurring of the line between use of personal data for delivering services vs commercial uses of children's data for profit and uses that go beyond what is necessary to deliver EdTech products and services in ways that conserve children's rights and dignity.

The following points are noted:

- Schools manage personally identifiable and sensitive student data. This information is regularly shared with persons within the school, who may not need for that information. It can also be shared with external bodies and third parties including commercial entities. Much of this information sharing may not be required. Without the requirement for privacy impact assessments (PIAs) children's personal data can be unknowingly put at risk.
- In addition, even the sharing of anonymised data has potential for individuation and re-identification that exposes children to potential harms. This is exacerbated in the case of sensitive personal information, whether factual, inferred or derived.

  We recommend that schools are required to conduct privacy impact assessments (PIAs) to identify and assess the privacy risks of data collection, use, or handling of personal information, and find ways to mitigate or minimise those risks, including finding alternative ways of achieving goals while minimizing the privacy impacts. Schools need extra support to ensure these are carried out, with specialised training and resources being made available.

  We also recommend that schools are provided with appropriate sector specific guidelines to enable them to understand the scope and use of the information they hold about children.

- Commercial entities are collecting and using children's educational data with little or no oversight. This means personally identifiable data is obtained directly from children through EdTech products, which is highly problematic. The impact of the data collection means a child's privacy is compromised. If an EdTech product is collecting a child's data, this should not be for commercial gain. For most New Zealand schools, there is no explicit and free and full consent sought for the use of educational technologies, rather consent is often implied on enrolment. Most CYP and parents/guardians are unaware of the scope of data collected from children while using EdTech assuming that such use is limited to the learning purpose specific to the EdTech tool in question
- There is no regulatory framework that specifically protect children's rights to privacy from institutional data processing or commercial data processing within education. The sole framework governing collection of a child's data is the Privacy Act 2020. The issue which arises is the lack of meaningful consent provided for commercial data processing by the child and/or parent/guardian.

- Schools are in a position of a power imbalance. They do not have the ability, even as a collective, to negotiate privacy terms with commercial EdTech providers that are fair. To address requires support and action at the highest level. EdTech companies often require schools to consent to their privacy policies on behalf of children, but as we lack strong data protection policies to protect children's interests, review of data practices is rarely considered.
- It is not clear how and to what extent do government-endorsed contracts with large global EdTech companies address children's data privacy. Assurance that children's privacy is at the forefront is needed to address and allay concerns. The rights of a child should take precedence over any commercial reasons for the use of any particular EdTech.
- When the Privacy Act is discussed in relation to children, often the safety element is highlighted. There may be some further provisions for information-sharing provisions under Oranga Tamariki and Family Violence Act, but these do not speak more broadly (or may not apply) to the privacy concerns raised regarding collection and use of children's data, for example, by EdTech.

Question 7. What do you think should be done to better support children's privacy in the area you work in?

The following commentary speaks to strengthening the support for children's privacy in general. We have a number of recommendations drawn from developments both internationally and regionally which we feel can help inform the way forward. In summary our recommendations entail:

Further strengthening of the law with respect to tamariki and rangatahi is required. Internationally, there are far more regulations and provisions directed to children's privacy. These include:

- GDPR (Europe) and UK GDPR
- Privacy and Electronic Communications Regulations (UK)
- Digital Services Act (Europe)
- Age-Appropriate Design Code (UK) or Children's Code
- Children's Online Privacy Protection Act (US)
- California Age-Appropriate Design Code Act (US)
- Family Educational Rights and Privacy Act (FERPA)

The overseas environment may be challenging with multiple provisions and there is concern that as with for example, that the United States the end result is a 'patchwork' of regulations. We have an opportunity in New Zealand to develop provisions that avoid such patchwork measures and which can provide comprehensive protection for CYP.

Adopting a rights-based approach to provisioning of children's privacy. We consider that the kōrero and framing of children's privacy issues needs to be firmly centred on a rights-based focus. A rights-based approach also recognises provisions under the UNCRC (Art. 16) – that, "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, … The child has the right to the protection of the law against such interference or attacks." Adding this dimension both focuses and broadens attention. A rights-based focus means that the positive benefits and opportunities of digital technologies can be promoted and utilised, but also that children's vulnerabilities are recognised and protected, and not exploited.

A**ppointment of a Children's Privacy Commissioner** as someone who can advocate for the privacy rights of CYP.

Privacy Impact Assessments. We consider that requirements need to be strengthened, such that these must be done. We note by comparison, Article 35(1) of GDPR states that a DPIA must be done where the processing is likely to result in a high risk to the rights and freedoms of individuals.

Constraints on the use of biometric information for profiling children. We refer here to the parallel consultation regarding biometrics and privacy, which has particular relevance to the use of children's data.

Establishing an Age-Appropriate Design Code. This will address particular issues for this vulnerable group. Such a code should also consider provisions that increase awareness of and protect children's rights where the information sharing and use falls outside the remit of the Privacy Act's 2020 focus on agencies use of personal information to provide wider protections.

We make further comments on an age-appropriate design code below. In considering elements of age-appropriate design, we also note the Future of Privacy Forum's December 2022 Policy Brief, comparing the UK and California Age-Appropriate Design Codes.

We submit that having provisions similar to the Age-Appropriate Design Code (UK) managed and enforced by the Information Commissioner's Office; and the California Age Appropriate Design Code Act (US) is an important step. These Codes seek to protect children within the digital world, with a focus on providing privacy by default settings which ensure that children have access to online services, while minimising data collection. They also seek to ensure that when a choice is made to change default settings, relevant information is provided producing more meaningful consent.

As most digital services and technologies are provided by companies overseas such a Code would need to be enforced on companies selling into New Zealand. In the Edtech space in particular, where over 90% of EdTech are international companies, enforcement would supersede the current optional privacy and security risk assessment model that applies with ST4S (Safer Technology for Schools) and industry self-regulation. We note ST4S has an increasing number of New Zealand Edtech assessments, and we welcome and support this.

Our consideration of what needs to be included in an Age-Appropriate Design Code ties into the list of privacy concerns set out in Question 12 (below). We agree with all of the areas of concern that have been set out, as being important. We comment further as follows on what we consider needs to be addressed in the Code:

Transparency: We do, in particular, see the statement "*I want digital platforms to be more transparent around how they collect and use the information of people under 18*" as being critical, and that transparency should be a key provision of any Code.

Provide prominent and accessible tools to help children exercise their data protection rights and report concerns. The ability to exercise rights meaningfully stems from transparency. Platforms may offer privacy enhancing or protecting options in their settings around collection and use, but these cannot be meaningfully engaged with if there is no awareness or clear understanding upfront of the purposes for collecting, using and sharing of information.

We expect real adherence to Information Privacy Principle 3, regarding openness about why information is being collected and what will be done with it.

There is nothing new about layered and just in time privacy notices, and there should no reason why businesses cannot employ these. We suggest the Commissioner's Office adapts and further promote

its extremely useful 'Priv – o-matic" tool to assist organisations with their transparency obligations. This would assist smaller agencies in understanding their obligations.

Privacy by default: We suggest also that privacy enhancing concepts and techniques need to be given prominence, so that there is tangible implementation of privacy by design and privacy as the default in platforms and technologies.

Data Minimisation: This captures the principle to collect and retain only the minimum amount of personal data necessary to provide the elements of the service in which a child is actively and knowingly engaged.

Large global and international companies have complex ways in which they collect data and need more specific direction as to limits. We suggest firstly that emphasis should be placed on be on the principle of data minimisation, and that this should be clearly articulated, building upon Information Privacy Principle 1 obligations.

The starting point for additional data uses should be opt out by default, such that for any use and disclosure purposes that companies want to have in place beyond the primary purpose of delivery of the service/provision of the product, users have to explicitly and actively agree to.

It is our expectation that a rights-based approach would be founded on limits to what information can be collected from children without consent. When identifiable sensitive data is involved, this must have strong consent mechanisms in place.

Beyond stating that information collected has to be necessary to fulfil an agency's purpose, organisations need to be directed to identify the minimum amount of personal information that is needed, and only hold that. Organisations must then be held accountable and be transparent about the processes they use to ensure that only necessary information is collected, processed and held.

Restrictions on Data Sharing: Children's data should not be disclosed unless there is a compelling reason to do so.

Prohibit Geolocation tracking: Geolocation options should be off by default, and when turned on, there should be obvious signs for children.

Targeted Advertising: Prohibiting the use of children's data for commercial purposes such as targeted advertising.

Profiling: to prohibit or limit use of profiling and automated decision-making, especially within education. Profiling should be off by default and only allowed with appropriate measures to protect the child from harmful effects.

Nudge Techniques: Ban the use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

Right to Erasure: Such a right is not specific to children and may be considered in the broader context of privacy provisions (and alignment with international legislations, e.g. GDPR). However, we would argue that such an enactment be broadened to allow for the erasure of information that has been posted by others, recognising that children and young people with regard to age and maturity may not have had a say or understood the implications of the shared information (e.g. postings on social media).

Consent: Authorisation may be stated to be required, but not actively sought directly from children and parents. Instead, it may be oblique, sought indirectly or implied. In instances we have seen in the Edtech area, authorisation is simply passed on to schools to manage.

In schools, we see need for clarity around the issue of *who consents,* for example, to EdTech collection of data. At present schools vary in their approaches with most requiring parents and students to give a carte blanche consent to all technologies with little or no opportunity to be informed or to opt out. There is a risk that if blanket agreement is not provided, children may be excluded from participation and engagement.

We also note here the difficulties of consent and caution against making consent the foremost issue. For example, it is often complex to deal with age verification online, taking into account how that can be done meaningfully, and the risk that may be involved in collecting more information. However, solutions such as a *zero-knowledge proof* which help verify a claim without revealing any other information besides the veracity of the claim (e.g. whether a person is age 14 and over) may go some way in addressing these issues and support data minimisation principles. As more international law requires companies to adopt some form of age verification, there is also considerable research and discussion overseas as to the potential methods of verifying users' age online – though we recognise as yet there is no common stance on this.

Limitations:

An Age-Appropriate Design Code is a one step towards bolstering the privacy protections for children. However, it focuses only on agencies' collection, use and disclosure of individual's information. We therefore again emphasise that further protections are necessary in the case of children, who due their age and maturity may not be able to make informed decisions about their personal information. Domestic and personal context may be problematic when the data shared in question is potentially harmful, but outside the scope of the provisions under s28 of the Privacy Act 2020.

Question 8: What do you think should be done to better support parents and whānau to protect children's information?

We would support ongoing public awareness campaigns aimed at parents and whānau for ways to protect children's privacy in conjunction with the Office of the Privacy Commissioner and other agencies such as Netsafe.

Aside from the proposal made above for an Age-Appropriate Design Code, reflecting on our inquiries under the Foundation's Children's Privacy Campaign, we also recommend that greater support is provided to schools/kura so that they are cognisant of privacy issues around commercialisation of data.

Specific resources need to be provided to schools to ease the burden of the administrative time, resource and expertise required to assess Edtech for safety, privacy and authorisation/consent issues. Schools can then, in turn, have better informed conversations with parents and whanau concerning children's privacy.

Question 9. If you wanted to complain that a child's personal information had been taken without their or their parent's/whānau consent, what would you do?

The particular circumstances will influence the approach to be taken here, and we agree with the initial options set out around speaking directly to the child's parents/whānau/guardians, applicable

professional body in the specific context, or the OPC. Again, with the range of options presented here, this suggests that there may be a lack of clarity on where first to approach. We suggest that further supporting guidance and examples are required to raise public awareness.

Question 10. Are you ever worried about how a child's personal information is being used?

The example contexts and instances of using services online are all relevant and ones which we see as cause for concern. This question highlights the complexity of the issues in terms of responsibility, and the provision of assistance to address worries and concerns where there may be multiple vendors, entities and parties involved. There is often not a single contact point and the issues can require a multi-agency response or interaction. We link back to our comments made under Question 2 above.

Question 11. If you're worried about how their personal information is used, what worries you about this?

In this comment we address provisions and limitations regarding children's privacy for different areas of concern. In doing so we highlight areas of worry that need addressing.

(The following has been reorganised to align better with areas of concern and the IPPs to which they relate e.g. concerns about use, access, data collection etc).

Use: The mana/tapu/integrity of their information is not respected / You don't know how their personal details might be used after it is collected / The personal information may be used by companies to directly advertise to children/young people

We agree with the concerns noted here, and in particular-

- **Secondary use of information and data** - this leads to potential privacy harms including surveillance, aggregation, bias and discrimination, and increased accessibility of data, particularly by commercial interests.
- **Lack of transparency**, in relation to the full information lifecycle – privacy advocates are acutely aware that it is common to see privacy notices and terms that are lacking, difficult to comprehend or buried amongst legal provisions. At the same time, it is good to see that some agencies are starting to address this issue by presenting privacy policies aimed specifically at children and young people, so are presented in ways that can be more readily understood by these groups.

Access: You don't know who sees their personal information

It is often not clear when it comes to the sharing of children's information who is able to see what information. For example, staff can have access to student information including sensitive pastoral information through the Student Management Systems that may not have any or sufficient privacy thresholds, or teachers may have access to a student's vaccination status without ongoing just cause. Role based access and other controls such as break glass and a clear retention policy and process then become critical.

There are other situations where EdTech applications make global requests for student records which without review from a privacy perspective can expose children's personal information to third party commercial interests.

Collection: The way their personal details are collected / It has been collected without their consent / The app/service has geolocation on, so the service knows where the child is

IPP 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. IPP4 makes specific provisions for the collection of information from children. These principles collectively address data minimisation but lack sufficient clarity, direction and guardrails concerning what constitutes lawful and fair data processing within education. In the case of EdTech, in our view these may not go far enough to enable the separation of commercial interests and those of the individual in protecting the privacy of children.

We remain concerned about overcollection of data – vast amounts of data are collected on children that may not be adequately protected or is at risk of secondary use.

Question 12. What would be most important to you to better protect a child's personal information?

We agree with the matters presented and see these all as being of critical importance. We would also add here that it is imperative that there is focus and published commentary in relation to Māori Data Sovereignty and privacy within a Te Ao Māori and indigenous peoples' worldview.

Question 13. Do you have any ideas about how organisations, websites and businesses can be more transparent/clear about how they collect and use children's information?

We refer to our comments under Question 7 on transparency under the suggested Code, and confirm there should be consideration and implementation of standard privacy by design/UX design principles, including:

- Central location of privacy information that is easy to see and not hidden
- Portals or privacy centres
- Repeated/ongoing display of privacy information throughout the App/platform
- "Just in time" notices
- Layered privacy notices
- Privacy notices appropriate to the modality of the App/platform
- Age-appropriate language
- Accessibility considerations with respect to font and colours

We also see it as being critical to provide organisations and businesses with clear guidance as to the limits of data collection involving children. We need to view children as having rights rather than as being potential subjects of surveillance or commercialisation.

Question 14. Do you think parents/guardians/whānau should be able to ask to receive a copy of a child or young person's personal information? And

Question 16: If yes describe the situations you think parents/guardians/whānau/ hapū/iwi should get a copy of a child's personal data?

That children have a right to privacy is stipulated in many international regulatory frameworks. See UNCRC General Comment 25 for instance.

The exercise of this right should be viewed with consideration of the well-being of the child at the fore. This may necessitate in some circumstances restricting the information shared with parents. In

other circumstances the desire for privacy may be overruled where the information is necessary to ensure the well-being of the child. This requires careful consideration, and perhaps setting a high bar for determining circumstances under which the withholding of information may be put aside.

We see this as a broad and very nuanced question with many sublayers. It is insufficient not to consider different aspects, contexts and sensitivities of the information involved, e.g. a request for information about school attendance and performance vs health information held by the school's counsellor or nurse. Health information is particularly contentious. For instance, children who may be exploring their sexual identities or seeking help with contraception may not want this information to be shared with parents.

For children under 14 years, it likely generally accepted that there is a clear need for parental representation. Between 14 and 18 years this may vary with regard to age and maturity. We note the existing application of the exceptions that may apply under Rule 11(5) of the Health Information Privacy Code 2020 for the information of children who are under the age of 16. If we are to take the Gillick competency test as at common law, then professionals who may be making decisions as to minor's medical or mental health care may choose to act without parental consultation.

However, it may be that schools, counsellors and medical professionals could also harm family relationships by excluding parents. There should be avenues for parents to intervene or be consulted if they feel information is insufficient for 'others' to make decisions about what is in the best interests of the child.

Question 17. Do you think iwi/hapū should be able to ask to receive a copy of a child or young person's personal data? And

Question 18. If no, why not? And

Question 19. If yes, describe the circumstances you think hapū and/or iwi should receive a copy of a child's personal information?

Consideration should be given to what the sharing of children's information means in relation to tikanga and a rights-based approach for a child. It also necessitates a clear understanding of what a rights-based approach means and its application, especially where such may confer less rights to some groups.

We are mindful of the work undertaken by Te Mana Raraunga and others relating to Māori Data Sovereignty and a Te Ao Māori view. We consider that it is appropriate to consult with hapū and iwi to determine the appropriate context for sharing a child's data.

Question 20: What age do you think parents/guardians/whānau/hapū should stop being able to ask to see a child or young person's personal data?

This is a challenging question i.e. to provide a bright line test at which age parents should no longer be able to ask to see a child's personal data. Noting also in other contexts, rights and legislation relating to minors, children and young people differ- for example at 16 children can chose which parent to live with, and at 14 legally stop being a child are a young person.

We have stated that the Gillick test in healthcare empowers children to make decisions around their healthcare, and a similar approach could be adopted for children in respect to their personal

information. This is where an Age-Appropriate Design Code would support the design of services for children which would embed privacy by design and support children's autonomy.

Question 21: What might be some reasons where both the child/young person and their parents/guardians/whānau/hapū/iwi should have to jointly ask to see their personal information?

This again is a question that requires nuance and consideration of the different variables. We suggest that in instances where there may the potential for emotional harm to the child/young person, or exposure or intrusion (following Solove's taxonomy of privacy) then a joint approach should apply. There may be some topics or categories of personal information that can be jointly identified and agreed between children and their parents/guardians as being 'ok to discuss and release', with this consensus being revisited on a regular basis.

Question 22. Do you think there should be rules about how old a person should be before they can use a social media platform without needing parental consent? And

Question 23. If yes, what age should this be?

This is where further research is required to understand the appropriate age in the context for children of Aotearoa New Zealand. As noted in the EU Kids Online research, if children are educated and empowered, and further if the social media platform is designed in an age-appropriate way, then a number of the concerns we have highlighted could be minimised.

International legislation differs as to what age a child is considered a child. In the USA the Children's Online Privacy Protection Act considers a child under the age of 13. However, Article 8 of the GDPR considers a child under the age of 16, but individual Member States can lower the age to 13. We consider the overseas examples helpful, but again, research is required to identify the appropriate age whether this is relevant in a New Zealand context.

Concluding comments:

Once again thank you for the opportunity to contribute to this discussion. We are available for further feedback and dialogue, please do not hesitate to contact us further.

This submission has been prepared by the Privacy Foundation's Children's Privacy Working Group. The authors are: Rebecca Hawkins, Caroline Keen, Annette Mills, Sarah Butcher and Aya Yamaguchi Murray.

Contact:

Rebecca Hawkins

Children's Working Group convenor, Privacy Foundation New Zealand

Contact: rebeccaljhawkins@gmail.com