Consultation with young people about the Children's Online Privacy Code; especially Transparency, Geolocation, Advertising & EdTech

Reset.Tech Australia
March, 2025

This consultation was organised and moderated by Reset.Tech Australia, and we are hugely grateful for assistance from PROJECT ROCKIT, the Australian Youth Affairs Council, UNICEF Australia, ChildFund Australia and Southern Cross University. All errors and omissions rest with Reset,Tech Australia.

With many thanks to the Internet Society Foundation for the support for this research.

Contents

Introduction

This paper documents notes taken from a workshop with 37 young people aged 13-17 on March 29th, 2025. It reflects the young people's perspectives and words as much as possible. It is a briefing given to the Office of the Australian Privacy Commission, to support their work drafting the Children's Online Privacy Code.

During the workshop, participants worked in small groups to discuss four considerations in around online privacy:

1. Transparency and notices: This group addressed how young people want to be informed about what data is being collected, used or sold about them online, and interrogated the adequacy of privacy and cookies notices.
2. Geolocation data. This group explored what young people thought the rules around the collection, use and sharing of geolocation data should be, and if geolocation data should have 'special' protections.
3. Using data for targeted advertising. This group discussed if young people's data should be allowed to be used to deliver targeted advertising, and what the rules around this should be.
4. Software and apps used for learning. This group explored EdTech as a case study, and discussed what the rules should be for EdTech providers who collect, use and share young people's data. They unpacked how consent "works" when young people have to use these products in school or out of school.

Participants were asked to develop a summary of 'key insights' from each small group discussion to share with the Commission, to share their ideas around idea enhancements to their privacy if they had a 'magic wand' and also provided the opportunity to leave a postcard (or note) to the Privacy Commissioner.

This report documents the thoughts and words of young people themselves, and some observations from adult moderators of each group.

Transparency & notices working group

Key insights

The group agreed that the key insights they wanted to share with the Privacy Commissioner as they draft the code was around the need for:

1. Youth friendly policies. There needs to be a youth accessible version of what we are agreeing to, and ensuring young people have an understanding of what they are agreeing to. Summaries of policies- we have to know what we are signing up to.

2. Genuine choice and easy opt out. An easy way to opt out of having data collected - if your only choice is to have your data collected or not use a service at all that is not really a choice. Without digging through settings or getting a VPN.

3. Service access that is not tied to data extraction. Access to services should not be restricted as a way to extract unnecessary data. Privacy policies and cookie notices shouldn't be used to pressure users into sharing more information than is needed.

Summary of the discussion

This working group discussion was prompted with two key questions. Below we have included the adult moderator's summary of the group's discussion, with notes that—as far as is possible with live note-taking—reflect the language from young people.

1. *Australia's Privacy laws say that people should know when their data is being collected, used, shared or sold. This is meant to happen online through privacy policies, or cookie notices for example. Does anyone read the privacy policies, or cookie notices when they are online? Why or why not? Should they be made better? How?*

Not all young people read notices, describing various barriers, including difficulties with the documents themselves. This included complicated jargon:

- I recently only first read a privacy policy. What I found out was that it's unnecessarily complicated, legal terms and complicated language. Any reasonable young person would give up. It's ridiculously long — 80 pages. It serves to stop young people from knowing what's going on. My friends give throw away comments like "oh yep they're stealing my data again". Reading the policy felt like such an intrusion, all the data they actually take.

- I don't read them — they're really long. Some companies have a summary at the bottom before you accept or reject the cookies, there is a risk of agreeing to some things that haven't been listed but this is better. You can have an idea, rather than none and I think that is more ethical

But also the length of the documents were often raised as an issue, and often felt disproportionate to the online task young people were trying to achieve:

- I don't read anything either, because it's not efficient and like people want to move on with the world and not waste time reading a whole essay.
- I have never read one personally, but I think a big issue is that young people are one of the most online generations — when we are googling or downloading apps we just do so much of it it just diminishes the point of these cookies (policies), we're not going to take the extra half hour to read the document when what we're looking at or researching only takes 5 minutes. We just wouldn't have enough hours in the day — I'm only shopping for one thing, but this huge cookie thing comes up and it takes me half an hour to read it.
- It's time consuming, I haven't read it, it's an inconvenience — I just click accept. It does concern me, but I don't think we bother to spend time looking further. Is it always clear? No it's not clear, it looks intimidating , the language is complicated.
- I don't read them most of the time, once I did, I only got half way through. They are so long. I think there should be a mandatory summary or something visual to get their attention. Privacy is so important and we get desensitized to it.

But there was also a feeling that reading the policies did not help to advance 'privacy' anyhow:

- If you don't agree to have your data be used, then you can't use the service. It feels like that isn't even a choice. They just say here is the deal, if you want to use the service, even if you don't have the capability to sign you just do anyway. It's a pretense of a choice when really there isn't a choice at all.

Two young people spoke about not reading the policies because alongside the general normalisation of just clicking 'accept' or there wasn't much meaning to the policies:

- I trust it's reasonable, so I don't always bother to read the notices. I honestly don't think that young people are able to consent to those contracts at all. I don't see the point of them there, if clicking to accept doesn't hold meaning.
- Personally, I do not read online notices, mostly because it takes so much more time than just clicking 'accept' to get to the content/service. Since I always just accept, I feel like I am desensitised to clicking the button and actually thinking.

There were discussions around the ability for the 'fine print' to hide important details:

- I think there can be malicious things in the privacy notices. I don't know how these things work or where my data goes, I'm asked to accept cookies for the 'best experience' - but what does that mean?

The ability for younger children to understand notices was generally refuted by the group:

- I don't think a 10 year old can click accept, and know what that means.
- I have friends with siblings, I want to know, isn't there a law that says you can't sign up to a legal document? It's really concerning that 10 year olds are asked to do this, even with this law in place

Lastly, there was also some discussion about if reading policies mattered, since you needed to 'click accept' anyhow to use them:

- I personally don't read any of them because they're just too long and I've tried rejecting them sometimes and then it doesn't let me use the service or website.
- It (the reason young people don't read notices) could also be the stress of having a subpar experience if you choose not to agree to it. With social media for example, if you're creating an account it's most likely because your friends are on it and a privacy policy wouldn't be in any way a deterrence to using the platform. The fear of missing out or losing out on features that all your friends are using is stronger than your desire to read the privacy policy
- Isn't it still within the providers right to deny service if the user doesn't agree to set terms and conditions?

2. *How should young people be told when their data is being collected, used, shared or sold? What should the rules around this be?*

There was general agreement that young people ought to know when and how their data is being processed:

- I think that young people should be told when their data is used, collected or sold. It's their data, even though it's the services of the company. It should be very regulated for the companies — if they use it and don't say they're going to sell it to another party who are using it to influence you, that's not ok. There should be enough rules because your data is *your* data.
- You got to engage with it in some way, not scroll all the way to the bottom and accept. It should be kept concise - a list of things that are happening and presented to young people in a way they can engage with/understand it. Like a clip - like what is on social media. Think about accessibility - not hidden behind legalese just the facts.

- I think companies of websites should share when they're collecting our data - should be at the front, like even in the app store. Some apps do that but either the info is limited or vague - so more information before we even hit the install button and mandatory.

There was also discussion around the importance of notice in youth accessible ways:

- Something useful could be visual aids or mandatory summaries to actually grab attention and make us think before accepting
- I like the video idea. What about 2 sentences max about what they are doing with your privacy and a 15 second timer before you hit accept, you can't accept before that so you have to read it - what else are you going to do while you're sitting there.
- A youth accessible version that comes along with that set of conditions - simple language and key points is more enticing to read. So many stakeholders, difficult to regulate, each provider needs time and money to do that. Legal side of thing requires the use of that language - making that clear, so there it it not vague in the case of an incidence a someone goes to court- no grey on what was there and who had what responsibility
- A clear, concise list or maybe notification that is easy to understand at a glance, uses terminology and vocabulary that is understood by anyone

Geolocation data working group

Key insights

The group agreed that the key insights they wanted to share with the Privacy Commissioner as they draft the code was around;

1. Data retention: the duration of time that data is allowed to be stored should be specified, limited and clearly articulated in any app-use agreement.

2. The need to understand: The young person who is sharing their data should fully understand what information they are sharing and why it is required. Clear terms and conditions are required in age appropriate language!

3. Data security: How securely data is being stored and managed is paramount. How can the code ensure that any data that is stored by apps or companies is hack-proof?

Summary of the discussion

This working group discussion was prompted with two key questions. Below we have included the adult moderator's summary of the group's discussion, with notes that—as far as is possible with live note-taking—reflect the language from young people

1. *Lots of data gets collected about all of us online, but geolocation data for some young people can 'feel' different, but not for other young people. What do you think? Does data about where you are feel more sensitive to you, what do you think about collecting it?*

Young people said that geolocation data didn't feel especially sensitive, although they were still worried about misuse:

- People often forget about geolocation data, so we don't think it is so important. But if devices can share your location then advertisers can target you and this can be misused
- Snapmaps collects data and me and my friends don't think about it or read the fine print in the agreement for using the apps
- I think, more than apps knowing your location, what's scarier is where that data is going… we never actually know who has access to it.

When it came to why geolocation data was collected, and if it was necessary, there was often a general sense of 'mistrust' in the justifications for collecting it:

- Whenever we use apps like Google maps etc I feel safe, but not so when an app doesn't 'require' your data but take it anyway. The app is collecting, rather than providing data!
- There's a general concern about *why* apps who don't need your location still collect it, and may not allow you to continue using the app unless you accept the collection of this data.
- The line is 'blurred' with some apps still requiring geo consent. Some might lie and pretend they actually *need* such info to function, but how would we know.
- I think if an app purpose requires location it's normalised for us to just trust it. Whereas if it's an app that doesn't require it, it does feel like telling a stranger where you are at all times.

Concerns were also expressed about the security of geolocation data:

- How stable is the storage of geolocation data? Even if the app itself is trustworthy, hacking can expose that data to outside parties who may not be trustworthy.
- If the data is collected then it is vulnerable to being stolen.
- I think, more than apps knowing your location, what's scarier is where that data is going… we never actually know who has access to it.
- Young people could imagine scenarios where geolocation data could be used to 'harm'. For example, a scenario was discussed where someone wins a lottery ticket and a nefarious app collects that intel and targets or even steals from the winner.
- Other young people talked about 'commonplace scams', like getting a text claiming that data has been stolen and you must 'click on link' to help 'recover' that data.

There was also a discussion about what the potential uses of geolocation young people felt comfortable with, and what they did not feel comfortable with:

- An example of an okay use was shared around using Snapmaps. They used Snapchat to organise a birthday party. All invitees shared geolocation data to help find each other at a large hotel, which was useful and reassuring…
- Another example of an okay use was around Life360. One young person talked about how it was is always on for them but they trust the app because their parents share the data as well
- I share my location with my mother but it's purely so she can know the timing to pick me up. but I've turned most location services off except for Pokemon go.

2. *What do you think the rules should be in the Code for apps and websites that want to collect young people's live location data?*

Suggestions included:

- Explicit consent:
  - If an app wants to use a young person's location then *the company* should have that request approved. Apps won't be allowed to collect that data on default without justification
- The right to change your mind:
  - Should be an easy way to revoke consent on change of mind, for any app. The app is then required to delete any stored data.
- Clear information:
  - Apps should describe what the data being stored *is* and *why* they need it in clear understandable ways, and time-impermanent terms.
  - Companies need to tell us that they are storing our data. The *way* they tell is important - not endless paragraphs but short clear language that explains *what* you are consenting to
  - Terms and conditions should be tailored to the audience - e.g., if the target group is young, then terms and conditions should be clear and simple for that demographic!
- Stronger data security:
  - A rule about *how* the data is used and stored. How can companies be sure that the data they collect is invulnerable?
- Data retention:
  - Companies should have to *renew* approvals of data collection periodically, e.g. every 6 months, to allow young people to rethink their decisions around consent of data collection
  - Data should have an expiration date. It should then be deleted automatically and reset, regardless of renewal confirmation of consent
  - I don't think location should be stored for more than a short period of time, especially if they are susceptible to security breaches and cyber attacks
  - Noting some good examples around this, they outlined that Apple asks if you have it sharing constantly for more than 3 days I believe

When it came to parental consent for geolocation data, the group also noted:

- I think there is an element of maturity, kids who are younger shouldn't be allowed to consent for themselves for sharing their geolocation data. Parents need to be involved.
- Apple permissions can need parents' consent. How about a similar rule in the code?

Targeted advertising working group

Key insights

The group agreed that the key insights they wanted to share with the Privacy Commissioner as they draft the code was around the need for greater:

1. Transparency: Being clear about the methods used to target advertising and why companies are are doing it

2. Accessibility: Being clear about the methods and what data is being taken from young people in the process

3. Autonomy: Being able to make our own decisions as young people, whilst introducing informed consent so we know how our information is being handled

4. Protection for vulnerable people: There should be stronger rules to stop manipulative ads targeting children, people with mental issues or who are going through tough times.

5. Specifications about hard limits on what advertising companies can collect: That is, they should legally be prohibited from collecting sensitive data

Summary of the discussion

This working group discussion was prompted with two key questions. Below we have included the adult moderator's summary of the group's discussion, with notes that—as far as is possible with live note-taking—reflect the language from young people

1. So I think everyone will have had an experience where their data is used to deliver them a targeted ad. You'll get an ad that is just on point, or something you were just thinking about. How do we feel about this? Is it helpful to you as a shopper or creepy or somewhere in between?

There was some unease with the way targeted ads seem to be so accurate, and the desire for more transparency about how the data is collected and used to drive these:

- I think it's a bit creepy with targeted ads specifically. There's been times when I have looked something up on another device and I got a query ad about that topic. It's creepy how it has an impact on what ads come to me.

- I talk about random recommendations with my friends - books, movies etc and then it pops up on Amazon. It's quite creepy if it pops up, but it's quite useful if it gets me a discount or something else.
- Honestly, I feel the same vibe as what everyone else is saying. Talking to my classmates, there's some familiar ads a lot of the time, but we don't get a lot of insight into the algorithms and what the purpose is. We get asked 'would you like your data used' but we don't get insight into what it is used for.
- A while ago I was having a Zoom call with my friends, talking about going on holiday with my family, a week later, I was scrolling and I got travel hacks and travel blogs, etc. It was a little creepy bc I never imagined my phone would be listening to what I was talking about with my family.
- It is helpful but also really shows that your phone seems to always be listening
- Ads can affect how I or we feel, but especially for young people, by creating pressure to buy things or follow trends they see online. It makes me stressed. I have a younger sister, and she gets crazy to buy things.

2. *What do you think the rules should be in the Code for advertisers that want to collect, use or sell young people's data to deliver target ads?*

Young people spoke of the need for greater protections for young people in general, given their age and stage of life, and for young people facing particular vulnerabilities:

- As young people, our circumstances tend to be less stable and we crave entertainment from social media. We want to watch videos on TikTok. When we get a pop-up, we just click it because we want to watch the video. That gets taken advantage of. It should be explained to us more
- Protect vulnerable people , there should be stronger rules to stop manipulative ads targeting children, people with mental issues or who are going through tough times.
- (The role of parental consent was also noted as a potential protective factor) Advertisers should get parental consent before collecting or using kids' data, and never be allowed to sell it.

This was balanced against the need for advertising processes to recognise young people's agency in the process of data collection, and the role of consent in ensuring this:

- (what's important is) the concept of autonomy or being able to make our own decisions as young people, whilst introducing informed consent so we know how our information's being handled

The need for informed consent connected to the need for greater transparency around targeted advertising:

- I think for me, it would be transparency about what methods of collection they have - are they actually listening to our phones? What data are they collecting and why? We can't give consent if we don't know what we are consenting to and why.
- Ads must be age-appropriate, honest, and easy for young people to understand.
- Companies use terms and conditions as a never-ending list of information. They could use AI to summarise it, to help young people be more aware of what they are doing.

Lastly, the importance of limiting data flows was discussed:

- Confidentiality also plays a huge factor in this. whether our data gets shared with other third-party apps is important to us, and misuse may also result in disturbingly accurate advertisements - which we aim to avoid at an extent

EdTech working group

Key insights

The group agreed that the key insights they wanted to share with the Privacy Commissioner as they draft the Code was around:

1. The illusion of choice: We think we are able to give consent, but there are no alternatives to be able to access learning opportunities at school.

2. The importance of digital literacy: the ability to have autonomy to consent to information that can be at risk of breach of privacy. Students have a lack of knowledge about how their data is being used online; sometimes they don't care, because they don't know how their data is being used (and because consent is given by parents on their behalf).

3. The nature of surveillance at schools: For example, data collected online on digital platforms or CCTV cameras. This is a compromise between individual privacy and safety.

Summary of the discussion

This working group discussion was prompted with two key questions. Below we have included the adult moderator's summary of the group's discussion, with notes that—as far as is possible with live note-taking—reflect the language from young people

1. *What sorts of apps and websites does your school or you use for learning? Has anyone thought before about what data they collect about you and where it goes?*

A range of digital products and services were mentioned, and young people felt they did not always have visibility about their data practices:

- (My school uses) Compass, which is used for a variety of things, likedDaily timetables, reports, key documents, such as VCE forms, birthdays, parents' information, key contacts. It is vital in schools, and it might be collecting our data and using it for other things, but we haven't seen any privacy notices!

Or have reason to trust that their data was handled safely:

- My school uses Compass too. It keeps a lengthy record of just about everything about you. Most of it is used for safety, for example, medical records. But when I was in Year 10, we had a security breach on Compass. My school was very transparent and emailed us. While it's pretty secure, but I know there has been more than one (breach). A little bit concerning, because it's not just data that might be insignificant, like. shopping habits, it's your date of birth, address, full name, all grades, whole school career in that one app. It's concerning when you're giving so much data continuously to the school.

Some of this was described as feeling unnecessary, without excessive data collection occurring even when they are doing 'nothing wrong':

- (My school uses) 'Landschool / Livewire' Monitoring system. I'm unsure if it is an app, but it uses AI. It takes a screenshot of the laptop every 7 seconds and stores them. This has created a weird sense of paranoia in the school. Nobody is really sure what it is, and they (the company) don't have to ask us for permission. When we signed up to the school, we had to give permission (to everything). Even though it's not anything malicious, you're allowed to be doing it, but I would prefer them not to read my screen. So strange that they're allowed to do that.
- My school has their own internet and Wifi. Every day we have to log on. The school uses and tracks the websites we use and potentially our data. Sometimes it's daunting to know that even if you're not doing something bad, they can control and see everything that you're doing online.
- It's really hard, there's a lack of privacy for young people already and there's a broader picture around a lack of independence too. I have friends who have been forced to stay in school as the teacher marks the roll through Compass, because if you haven't been marked as present within the class or late, a parent receives an automatic message, and you get a call over the loud speaker.
- My school is a public school, we use EduStar wifi that can track your online activity.it has Firewalls for certain websites, like social media sites. It used to be (block) for Chat GPT and Netflix too

These mechanisms don't always work, and can have implications for intra-family conflicts:

- All of these mechanisms are meant to make sure you are in class, but there are ways around it. Some children have their parents' Compass login — so if they were going to skip class, they can login and record approved absence and circumvent it. Young people are able to take advantage of that.
- My peers, one of my friends, is very independent and doesn't have a close relationship with parents, but if he skips class (as noted by Compass), it turns into a bigger fight and escalation.

2. *I want to ask about consent here. How do we 'consent' or say okay to the way learning products collect or use your data? Can you do that in the classroom?*

There was a general agreement that consent was not meaningfully collected at present, and that it was more often forced or illusionary consent:

- It's the illusion of choice that gives the school all the rights they need for the rest of their school journey. The justification that they're doing this is for our interests, but does that still make it right or okay? At our school we had CCTV cameras everywhere for our safety, but did I want them knowing where I was around the school at all times?
- Some people get the legal stuff, like schools always have their legal basis sorted. So sometimes we say we haven't received privacy stuff and it turns out we did. Because it's heavy documents, those privacy documents are very heavy, it's very detailed. What would be great, especially for those with disability or multicultural backgrounds, is to have a concise version, for example a Year 3 level or Year 5 level. Something very low and easy to understand. It would be beneficial for young people to read the documents and really understand it. When I was in Year 7 or lower, I wouldn't know anything about what I was reading, I'd just say 'yeah sure, whatever' and just give consent. Opportunities of consent ,it's like forced to consent, because if you don't, you miss out on these opportunities, for example. to go to something or access resources for school. There's no other alternative to that consent.
- Some things you just have to consent to whether you like it or not, that's what it feels like for me. But you can't opt out of it because of the 'no phone' policy, I can't use your own mobile. For example, I can opt out of media consent, such as photos on school social media (but not EdTech). There is a personal risk of leaking info to third parties, you don't have control over, otherwise that would hinder your learning opportunities. It feels like there are some things we consent to because it's simply because it is what the school uses. What can you do? It's either that or you're not really able to access those platforms for learning.
- When it comes to consent, especially with using the various apps we use at school, it's always been implied that if you do go to school, the school has the right to gain any data through the apps you use. I can't remember reading a privacy notice about any particular app. School is using AI and apps for almost everything. There is concern that our consent hasn't been there from the beginning.
- (The rapid adoption of AI raised additional concerns around meaningful consent). I always trust my school if they would use AI, they would use it for the right purposes, but it's always the idea that AI is rapidly evolving and we're uncertain about. Will our school be able to deal with this quick movement, but also that we consent to our data being used by AI?

There was a sense that parental consent, or ‘school based consent’ was often sought instead of young people’s. This affects their autonomy now, but also their ability to ‘learn’ and prepare for a digital future:

- In my experience, there has been an opportunity for consent, but that consent is not mine - parents consent on my behalf. Literacy and data security isn’t that common, especially among young people. Young people should have the opportunity to consent on their own behalf.
- Because our schools have been really ‘protective’ of our online safety, I don’t feel personally that prepared to navigate the online world as I’m older and exposed to new things. Digital literacy, making sure young people have these experiences, is really important.

In general, privacy seemed lacking for young people in all settings:

- There’s a misconception that because you have more freedom as you get older in the world, that you have more freedom online. This isn't the case with surveillance, for example workplaces, shops online, participating in online forums. Surveillance is still quite high and used in a way that breaches your data and security.

What young people would change if they had a magic wand:

We also asked the whole group at a later point in the event what they would like to see changed if they had a magic wand. Suggestions included:

- Improvements around privacy notices:
  - Easy to read contracts. I think if some of the contracts were translated into readable or lower level language it would be better, they are full of legalese. They get in the way, for example a multicultural family might not have the capacity to understand it. Their parents will just sign it, children are only developing their language, they don't understand what their parents are signing, they don't understand their rights. Plain English or lower level English would be better.
  - Shorter contracts in dot-point form of what *actually* are you agreeing to. Make these short synthesised agreements instead of 80,00 words, what is the most necessary and basic information that you are agreeing to when you click ok — synthesise this for us.

- Improvement to young people's agency and digital literacy
  - Digital literacy and empowering young people to understand and make decisions about privacy, rather than spoon feeding. Young people can make informed decisions for themselves!
  - (This included a balance or blend of young people and parental consents) Just a thought - I love those joint consent forms where the young person and their parent sign the forms. It's great for students in Year 7-12 I guess, as it includes the young person in this decision making. And prepares them for reading contracts in the future 😬
  - Like I said before, I think presentations and excursions at school to first learn about the risks and rights of online privacy would be really helpful
  - I would add more education on data and what it really is, also mentioning where data is stored and the purpose of it.
  - Ideally, young people would grow up learning in schools, in my opinion starting from like year 3 or 4, knowing about privacy rules and regulations and grow into learners who can make well-discerned decisions about their own privacy rights.
  - For how youth should be informed on data sharing: I would add on that there should be presentation at schools so students can understand in general how their data is used online (since many platforms have similar uses of data). Maybe posters/little booklets outlining how personal data is used online and what you can do to stay safe 🙂

- Stronger enforcement of privacy rules:
  - Greater legal enforceability of breaches of privacy and more accountability!

- Change the business model:
  - I know it's silly but make all tech companies non-for-profit - they would have no incentive to collect our data. 😅

Messages to the Privacy Commissioner

At the close of the event, each young person was asked to share a message about the Code with the Privacy Commissioner and her team. These messages are included below, and addressed four key themes:

- The need to engage, educate and empower children and young people. This includes further engagement as the code is developed, especially with a diversity of young people and primary school students. But also, there was discussion around the need to educate young people about their privacy rights in general, and what the Code offers them when it is released. Young people need to know about their rights under the Code to ensure they can protect their own privacy and autonomy.

- Responsibility resting with companies that collect and use personal data. While education and empowerment are important, a number of young people also noted that companies have a central role in creating privacy too. They described how responsibility should also be on the companies to keep young people's data safe and private, and the Code needs to make sure young people are and feel safe about how their data is used.

- A call to improve transparency and accountability from companies, as a way to realise their responsibility. This included especially making sure that privacy notices are accessible to young people, but also making sure that they are short, jargon-free and age appropriate. But it also meant making sure that companies complied with these requirements and were accountable under the Code where they failed to be transparent.

- A call for better data processes in general. There were many comments that spoke to the need to protect personal information from being misused through better data processes in general, such as data minimisation, privacy-by-design, the ability to opt out, and 'hard limits' preventing potentially harmful uses of personal data.

Below, we have included all of the messages divided by 'category'. Please note, many comments address more than one area.

<u>Engaging, educating and empowering young people</u>

- Clear communication with youth about their rights and autonomy. I feel a lot of people our age feel pressure to agree to all of these 'privacy' agreements and such because they feel like they have no other choice especially when told to by an adult. Having clear

communication and education around youth's rights to privacy in the online space is imperative. This law will be almost completely useless if youth don't know how to protect themselves with it if needed

- Young people also need to be aware of the power of their data and why it is important to protect their privacy in the first place.
- Make sure you constantly involve children/youth as you write this privacy code. No tokenistic engagement or involvement in only one stage of the drafting process, but consistent, meaningful engagement instead.
- When your collecting data during the next year, I think it's really great to hear from a. range of young people who also may be not connected to these youth organizations, so really ensuring youth from diverse backgrounds are heard and consulted with
- Keep young people engaged throughout the creation process
- 1) Make sure that a wide range of students are consulted and at different stages of writing the code

  2) Working groups with students to go through the code and outline feedback once it is complete

  3) Also, it is vital to consult younger primary school students as well since many of them would have recently started using technology and as the future young people of our nation, this code will really impact them and they should have a voice as well

  4) I'm not sure if this is relevant but quotes from students/examples of data sharing within the code?
- Ensuring that children and young people are involved in further discussions while drafting and finalising the Code.
- More education on how read these contracts—and what to get out of it—what info should I get
- I think that if we're going to put young people in a situation where they have to sign legal documents, then in school we should actually teach them what legal documents mean and are
- First of all, this is such a great initiative! I think that the main issue here is education - in school we learn a lot about cyberbullying, phishing, etc, but never about issues pertaining to privacy and data. If we learnt about this then we wouldn't have people vulnerable to hacking because they don't know what setting they should change or randomly agreeing to thing since they don't understand the terms and conditions. If this was incorporated into the curriculum, I feel like we would be better equipped to navigate the online world.
- Stronger protections are needed to stop harmful or manipulative ads targeting vulnerable groups. Young people want clear control over how their data is collected and used in targeted ads.
- (This includes making sure the Code itself is accessible). It is important for me the way that the code that is formed is formatted. For example making sure not only the way it is formatted so it is clear and easy for young people to understand but also states the reason why these apps are taking out data. Allowing us young people to then make a decision on whether they would agree for companies to use their data or not

- Ensure that the opportunity of consent is in the hands of young people, not just their parents (and) teach young people appropriate media literacy
- I think it's important that more young people are being educated about digital privacy and digital literacy being the superficial level that is usually, if any at all, covered in schools. Children will have to deal with increasing risks and/or incidents of privacy breaches as they grow up in an ever-technologically-developing world anyway, so being informed on their rights and ways to safeguards such rights are extremely important. In the education sector, schools and the Dept. of Education should work with EdTech companies to ensure that personal information of students are not compromised in trying to access learning opportunities, because in reality, students don't really have a choice in opting OUT of those educational platforms/apps despite the ability to give/withdrawal consent.

<u>The responsibility rests with companies, not young people, and they should protect children</u>

- That the responsibility should be on the companies to keep OUR data safe and private. That we have a choice to use the websites and they should respect whether we want our data to be used. They should also make it clear when they sell our data to other companies and if we dont want that let us be. It's our choice. But make it still possible to use some of the services and functions on the websites.
- Young people and their privacy should always be the priority over the profitability of tech companies or whatever political or monetary clout they can throw about
- Young people need to have autonomy over their data and what is being shared with companies/schools/people. I know this isn't viable in some cases though, so for those cases I think not scaring young people is good. To have the message that our data is sacred and all sorts of terrible people may have it is all well and good if we have access to change these things... But if we don't it's just fear for fear if that makes sense, which is never ever fun. I also want it to be very much on the adults and never take away benefits that are currently there for kids.
- Making sure the code includes something that makes the children feel safe
- This should include:
    - Clear and easy to understand rules
    - Stronger privacy settings by default
    - Limit or completely wipe out tracking and selling data
    - Age appropriate content and safety
    - Easy and more convenient ways to delete data.

  Furthermore, kids should be able to access and explore the internet without having a feeling of their personal information being misused.

  It's so important to me that young people, particularly those under the age of 18, are not unfairly targeted with ads that are potentially harmful to their self-esteem! Overmarketing beauty products and diet related products to young people can be so detrimental not only in that moment, but can have lasting impacts in the long term!

Better transparency measures, notices and accountability for this

- To have these privacy consent forms in plain english, in a lower level english so it is easy for anyone to understand and comprehend the necessary info. It might be an additional document that is made with the original form, for if the consenter would like to understand more.
- More joint forms for students and parents that are over the age of 14
- Confidentiality, autonomy, and transparency/informed consent.
- Transparency and accountability: Companies gotta be transparent about their data practices, with clear, child-friendly explanations about what information is being collected and how it is used. There should also be strict accountability measures for non-compliance.
- The most important thing for a Children's Online Privacy Code would be for companies to make it clear when they are using our data and location and also how they are using it.
- To make sure that everything that is done is done ensuring that the themes of transparency and accessibility are at the forefront of what is written in the code
- It should be concise and should be to the point
- Platforms should have privacy policies that are in clear and simple terms - that even you children can understand because sometimes they are the ones who have to agree/disagree to things like data information being collected. By creating a code that enforces strict protections and encourages ethical behaviour a safe environment for youth can be built online.
- In an ideal world, each and every time I access a website, app or other service, I should be able to understand what I am agreeing to. How can I give informed consent when what I am agreeing to is in language that I don't understand? I feel like I am being forced into accepting so I can continue accessing the service- the system is stacked against me. It would be great to have a mandated Youth Accessible version with simple language and summarised points to all Ts and Cs in regards to privacy.
- I think that in contracts, there shouldn’t be any asterisks which makes the information not so visible to the readers, thus possibly causing them to miss out on key information that might affect their decisions
- 1. Terms and conditions are short, and we have to type it out/say it out loud to agree to it.
  2. Companies MUST outline the duration of time they are keeping the consumer's information for
  3. Consumers should be able to take back any information they gave to an app/company. And it must be easy, accessible and obvious.
- Transparency and clarity are two things I believe are important for the privacy code. When drafting the code, please consider the benefits and values of young people
- Utilising key technologies such as AI to summarise T&C’s, as they are quite often lengthy — simplifying it into a readable paragraph or points, thus making young people informed about the details surrounding their privacy.

Better data handling practices

- Minimal Data Collection: ONLY the essential information should be collected, and nothing more. The code should enforce strict limits on what can be gathered from young people.
- Privacy by Design: Online services and platforms should build privacy into their systems from the ground up, ensuring that data protection is an integral part of the design process rather than an afterthought.
- Make geo-data localized to zip codes. This is a way to bypass apps that "require" location sharing. Along with this re-draft of privacy rights, engage young people and educate them through short form video content. For example, a reel or small video that can be shared both on social media and in schools. To consent you must be able to understand. Expiration date on data, companies are legally obligated to delete and let go of information that is no longer relevant due to a period of time passing, eg 6 months. This would protect data footprints and mitigate the ability for people to manipulate young people.
- That data being collected from young people under 18 should not be heavily monetised and should be minimised, especially with regards to location and advertising towards people under 18. Would love to see more transparency from companies about what data is being collected and how it's being used.
- To me, I think there are quite a few things to take into account for the Children's Online Privacy Code:
  1. Transparency and Accessibility (this was mentioned twice but I still think this cannot be emphasized enough): Making the T&C's easier to read and interpret would be a great first step, because (especially in the case of young people), it's not easy to scroll through 2 pages worth of text written in language that can often at times be hard to understand.
  2. Hard limits: Advertising companies should face strict consequences if they breach the hard limits set by the government about the amount of information they can collect.
  3. Easy opt out: Especially in the case of cookies, if you choose to opt out, you often cannot use the application/website, which is really unfair, so I feel like this is a critical issue that should be addressed.
  4. Data retention