TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

To:
Rod Sims
Chairman
Australian Competition and Consumer Commission
23 Marcus Clarke Street
Canberra, ACT 2601
Australia
platforminquiry@accc.gov.au

RE: Call for recommendations on "Digital Platform Inquiry Preliminary Report"

Dear Mr Sims,

In response to the ACCC's digital platforms inquiry report, we would like to share our feedback on the preliminary recommendation 8 - Amendments to the Privacy Act.

1.0 Amendments to the Privacy Act: Protecting kids' online data privacy

Australia is falling behind world economic powers in the protection of kids' data privacy.

Every day more than 175,000 kids go online for the first time internationally[1]. We estimate more than 1,000 kids go online in Australia for the first time everyday. Each of these new Internet users becomes a profile in a database (or many databases) against whom more data is collected every day.[2] Research published in 2017 estimates that by the time a child reaches the age of 12, more than 72m points of data have been collected about them.[3] These profiles are then used to target advertisements and product recommendations, tailor services, and increasingly lead to automated decisions about them that can have a life-changing impact, eg affect a credit score[4], school admission or job eligibility.

1.1 Kids Digital Data Privacy Laws

Since 1998 kids in the U.S. have benefited from explicit data privacy protections through the Children's Online Privacy Protection Act (COPPA, as amended in 2012), and more recently, in May 2018, the E.U. has followed suit by including specific protections for children under 16

[1] UNICEF, More than 175,000 Children Go Online for the First Time Every Day, Tapping into Great Opportunities, but Facing Grave Risks (February 2018).
[2] Children's Commissioner for England issues new report on extent of children's data collected online (8 Nov 2018)
[3] Adtech firms collecting 'vast amounts' of data on kids despite online regulations (The Drum, 13 Dec 2017)
[4] How Companies Turn Your Facebook Activity Into a Credit Score (The Nation, 27 May 2015)

years in its General Data Protection Regulation privacy law (GDPR). We call the sum of these E.U. provisions GDPR-K[5]. In 2017 China passed the Cyber Security Law and more recently published the accompanying Personal Information Security Standard, which explicitly seeks to protect the personal information of children aged 14 or younger[6]. As a result of these new laws—and further comparable initiatives underway in countries like India[7], Brazil and Argentina—the protection of children's personal information online has now become a global standard.

1.2 Consequences

The consequences of these laws being put in place is that content owners, technology platforms and advertisers have been compelled to adopt technologies and processes that protect the privacy and anonymity of children by:

- Preventing the profiling of children for marketing purposes, including restricting interest-based advertising, behavioural targeting and remarketing
- Removing social media plug-ins and third-party embedded code that collects data from child-directed sites and apps
- Stopping the collection and wide dissemination of kids' geo-location, images and video recordings, and persistent identifiers that could be used to locate, identify or profile children

[5] How GDPR-K Dramatically Changes the Landscape for Kids' Brands & Publishers in Europe (ExchangeWire, 19 Mar 2018)
[6] China rolls out data privacy law for children (SuperAwesome blog, 15 Jun 2018)
[7] India needs to acknowledge the gaps in data protection and rights of children (10 Aug 2018, Hindustan Times)

- Requiring publishers to obtain verifiable, opt-in, informed consent from parents prior to allowing children to share personal information, or be exposed to unmoderated chat or community forums

The oldest of these laws—COPPA in the U.S.—has led to numerous enforcement actions by the Federal Trade Commission (FTC) and Attorneys General[8] and has spawned civil lawsuits[9] and activist intervention[10] that has changed the behaviour of technology platforms and companies by forcing a focus on protecting kids' data privacy. The success of COPPA has also led to the rapid development of technologies to enable that privacy across all types of digital engagement, eg "kidtech".

2.0 Amendments to the Privacy Act: Parental Consent, Privacy Controls and Notification

2.1 No personal data collection from kids under 16

Children are not aware of the personal data that is routinely collected from them while they use digital services, whether the collection is passive (such as by advertising technologies) or active (such as games asking for permission to record location). The primary objective of any new regulation should be that no personal data is collected from kids under 16 years of age unless prior parental consent has been obtained.

2.1.1 Definition of Personal Information

Because much of the data that drives profiling is collected passively, it is critical to use a broad definition of personal information in any law protecting kids' data privacy. The technology industry has hugely benefited from being able to collect supposedly anonymous persistent identifiers on a vast scale and without regulatory oversight. The FTC and most regulators have come to the conclusion that such identifiers are not in fact anonymous[11], can be resolved to specific persons, and must therefore be reclassified as personally identifiable information or PII. For this reason, COPPA, the GDPR, and every new data privacy law currently in draft or discussion around the world, includes persistent identifiers (such as cookie ID, device ID, IP address, advertising ID, etc) in its definition of Personal Information.

---

[8] A.G. Schneiderman Announces Results Of "Operation Child Tracker," Ending Illegal Online Tracking Of Children At Some Of Nation's Most Popular Kids' Websites (13 Sep 2016)
VTech settlement cautions companies to keep COPPA-covered data secure (8 Jan 2018)
A.G. Underwood Announces Record COPPA Settlement With Oath – Formerly AOL – For Violating Children's Privacy (4 Dec 2018)
[9] Disney sued for allegedly spying on children through 42 gaming apps (The Verge, 9 Aug 2017)
Class Action Lawsuits over Alleged COPPA Violations Reinforce Importance of Compliance (FKKS, 22 Aug 2017)
Alleged misuse of children's data lands Subway Surfers studio in court (gamesindustry.biz, 9 Aug 2017)
[10] YouTube Is Improperly Collecting Children's Data, Consumer Groups Say (New York Times, 9 Apr 2018)
New COPPA Complaints Filed (KMT, 2014)
[11] FTC's Jessica Rich Argues IP Addresses and Other Persistent Identifiers Are "Personally Identifiable" (FTC, 29 Apr 2016)
PII, Cookies and de-ID (IAPP, 25 Apr 2016)
Beware the Persistent Identifier (Jenner & Block, 29 Apr 2016)

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

2.1.2 Scope of law & definition of child-directed service

Kids data privacy regulations are challenged to clearly define the scope of their applicability. Ideally, children would benefit from protections no matter which digital service (adult or kids' content) they are using. In practice, because current technologies do not allow us to know exactly who is a child and who is not, regulators have been forced to limit the scope of protections to services that are "child-directed" (COPPA) or "offered to children" (GDPR-K). Each of these approaches have merits and failings that we believe the ACCC can learn from. We analyse them below:

COPPA: "child-directed"

First, COPPA applies only to services that are "child-directed". The assessment of "child-directed" is subjective, eg if the subject matter is likely to appeal to children (eg, cartoon characters), the regulator will consider it child-directed. This approach has been fairly effective in that it includes in its scope websites and apps that are likely to be frequented by kids (and not just those that have provable kids' audiences). The definition was clarified by the landmark 2016 COPPA case against Viacom and others[12], where corporate websites (eg, nickelodeon.com) were declared to be child-directed by the nature of their content.

The drawback of the COPPA definition is that it allows many service providers whose content is not obviously appealing to children (or at least not *primarily* appealing to children) to avoid the scope of COPPA. Relevant examples of this are YouTube and other content distribution platforms, and popular casual games such as Angry Birds, Cut the Rope, Fruit Ninja, etc, which have millions of adult and child users. Millions of children using these services are treated fully as adults.

Second, the other element of the COPPA scope is the "actual knowledge" qualifier, which states that any service provider (child-directed or not) who becomes aware of a child using it must apply the protections of COPPA to that child. This provision was effectively used against non-kids service providers who were collecting data from children, such as in the Yelp case[13]. This concept is key to ensuring that those providers who can argue their services are not for children are still held to account when they become aware (as new technologies will increasingly enable them to be) that there are children.

The primary drawback to date has been the difficulty regulators face in proving "actual knowledge" in the case of providers who are actively seeking to avoid such knowledge. This issue is at the heart of the recent FTC complaints filed by consumer groups against YouTube, which continues to claim that COPPA does not apply, even though:

[12] Viacom, Hasbro, and others fined $835,000 for ad tracking on children's websites (The Verge, 13 Sep 2016)
[13] FTC case against Yelp shows that COPPA isn't just for kids' sites (FTC, 17 Sep 2014)

> YouTube also has actual knowledge that many children are on YouTube, as evidenced by disclosures from content providers, public statements by YouTube executives, and the creation of the YouTube Kids app, which provides additional access to many of the children's channels on YouTube. YouTube even encourages content creators to create children's programs for YouTube. Through the YouTube Partner Program, YouTube and creators split revenues from advertisements served on the creators' videos.[14]

Any concept of making service providers responsible on the basis of 'actual knowledge' must therefore include a robust mechanism for auditing them and a clear threshold for proving that such knowledge existed.

GDPR-K: "offered to children"

The GDPR opted for a broader definition for which services must protect children, and the most recent guidance from the ICO[15] expands the scope even further. In effect, any digital service accessible to children is considered "offered to children." This in principle captures every corporate website and nearly every service except those that are actively blocking child users (such as alcohol or gambling sites). Clearly this is far too broad. Numerous industry participants have made representations to E.U. regulators to seek clarification and to request that some sort of subjective qualifier be included—eg, that the service must also be *appealing to children*.

The benefit of the GDPR-K's broad approach has been to force many of the mixed audience services (such as popular casual games) to recognise the existence of children on their platforms and to implement mechanisms for segregating that audience, eg by age-gating or sign-posting clearly which sections are for kids and which are not.

A summary of the positives and negatives of these differing approaches is set out below:

Approach to scope	Positive	Negative
COPPA - "child-directed"	Subjective test means any service that appeals to kids is in scope.	Excludes services used by millions of kids that are not primarily for kids.
COPPA - "actual knowledge"	Forces non-kids providers to protect them if they become aware.	Hard to prove when providers seek to hide their 'actual knowledge'
GDPR - "offered to children"	Captures services that are not clearly directed to children but may have many child users.	Too broad without some subjective qualifier, eg onerous on non-kids services.

[14] Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating the Children's Online Privacy Protection Act (filing before the Federal Trade Commission, 9 Apr 2018)
[15] Children and the GDPR (ICO, March 2018)

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

2.1.3 Future of Age Verification

The focus of U.S. and E.U. regulators has been on protecting children when they are accessing *child-directed* online services. But the fact is that most kids' digital activity is on services that do not know whether their users are children, or believe that they are not children, or pretend that they are not children. It has been widely reported that age gates are frequently circumvented or ineffective, while most available methods of verifying a user's age are based on further data collection and hence incompatible with the principle of data minimisation.

The use of age gates in games and kids' services has proliferated in recent years, mainly because in the U.S., the Children's Online Privacy Protection Act (COPPA) allows services that consider themselves mixed-audience (as opposed to primarily child-directed) to segregate their audience into kids and adults by asking the users' age. Whilst well-intentioned, this approach has had three significant unhelpful effects that have made kids less secure online:

1. Having been exposed to dozens of age gates, most children have realised that '13' is a magic threshold that unlocks a grown-up experience. As a result they have learned to lie about their age in order to get access to those services, in particular to social media platforms. This has in many cases been exacerbated by parents who have become complicit in helping their kids set up profiles on 13+ platforms.[16]
2. The mixed-audience concept has allowed thousands of services (especially games) to avoid being categorised as child-directed, and hence to continue using data-driven monetisation strategies that end up profiling children on a vast scale.[17]
3. The application of age gates or—in the case of social media such as YouTube, the use of Terms of Service limiting use to those 13 or over—has effectively allowed service providers to absolve their legal responsibility regarding children and reduced their incentives to improve the way they protect child users.

Article 8 of the GDPR seeks to address this problem by requiring service providers to "make reasonable efforts to verify" a user is over the age of consent. But the guidance acknowledges that there is no clear methodology to achieve this and calls on the industry to develop new solutions.

We believe that, for the most common data processing activities, any age verification technique

[16] Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' (FirstMonday, 7 Nov 2011)
[17] This issue has been widely reported in 2018, starting with the publication of an academic research paper into the data collection practices of Android apps: Thousands of Android apps potentially violate child protection law (The Guardian, 16 Apr 2018); followed by a complaint filed in the U.S. under COPPA: How Game Apps That Captivate Kids Have Been Collecting Their Data (New York Times, 12 Sep 2018)

that requires the collection of more personal data—such as a national ID card, or a national insurance number—is overly intrusive. In addition, these types of verification can only really be implemented to gate a specific service, but it is not feasible, for example, for a website to conduct this level of verification before deciding whether to serve an advertising impression.

We believe that the next generation of age verification techniques must be based on automated, passive ways of detecting whether a user is likely a child or not, and providing that assessment, along with a confidence score, to the service provider so that they can implement appropriate policies. Our research team, is currently testing a number of promising solutions. These involve collecting multiple signals from user behaviour (locally, on the device, without tracking or data collection) to determine the probability of the device being, at that moment in time, operated by a child or an adult parent.

Such a dynamic score could then be passed to a service provider, who can use it to verify what the user provided via an age gate, or potentially avoid age-gating altogether and simply tailor the experience for the child to be safe. Due to its real-time nature, such a signal could be used by advertisers—for example those who specifically do not want to reach children—to stop the serving of (and data collection from) an impression if the 'child score' is positive.

Whilst this work is still in its early testing stages, we would welcome the opportunity to share our findings and proposed solutions with the ACCC in due course.

2.1.4 Parental Consent Verification

The GDPR has taken one of the core concepts of COPPA as the basis for its protection of children—the notion of verifiable parental consent. According to the GDPR's Article 8, where the legal basis is consent and the data subject a child:

> *you must make reasonable efforts, taking into consideration available technology, to verify that the person providing parental consent does, in fact, hold parental responsibility for the child.*

Whilst COPPA proscribes what methods of verification are acceptable to confirm the identity of the parent (most commonly, a credit card transaction), the GDPR puts the onus on the industry to determine an appropriate level of verification based on the risk of the processing activity for which consent is being sought. This 'proportionate approach' is welcome as it enables companies to minimise the amount of additional personal data collected in the verification effort (one of COPPA's main drawbacks).

In order to help the industry design appropriate user consent flows, we recommend that any new regulation along these lines include specific examples of how to match appropriate levels of verification to the actual risk of the data processing.

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

Based on our extensive experience of working with children's online services (as well as building Verified Parental Consent (VPC) workflows and technology for COPPA and GDPR-K compliance), we have developed a practical framework along the lines below (examples only, not exhaustive) as a guideline for what level of parental consent and verification would be appropriate for different data processing use cases:

Type of data being collected	**Sensitivity**	**Examples of sites or apps**	**Appropriate method to verify user is <u>over</u> age of consent**	**If not, parental consent required?** **Appropriate verification method**
Sensitive Personal Information (health, ethnicity, tied to a name or ID number, etc)	Very high	Ancestry or healthcare service that stores user profiles with identity information and demographic/ ethnic/health data.	Neutral age gate, plus Database check against national registry, or Copy of photo ID submitted	**Identity-Verified Parental Consent (<u>w/</u> database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Parent identity checked against national ID database, or by submitting copy of photo ID
Identifiable personal information, eg full name, address, national ID number; image/video uploads; free text content. Combination of online identifiers and profile information that can be used to identify a natural person	High	Social media app that allows use of real names, connections with strangers, free-text chat rooms Virtual assistant that records voice & stores it in cloud, builds useage profiles.	Double confirmation, eg Neutral age gate, plus Reconfirmation of birthyear; or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	**Identity-Verified parental consent (<u>no</u> database)** 1. Parent provides consent 2. Statement by parent that he is the holder of parental responsibility; 3. Identity is confirmed by requesting credit card details and matching them against information provided (no transaction). Credit card information is then immediately deleted.
Technical online identifiers that cannot easily be resolved to a	Medium	Websites that allow behavioral or profile-based	Double confirmation, eg Neutral age gate, plus	**Verified Parental Consent** 1. Parent provides consent;

natural person, but are (a) shared with third parties, and/or (b) used for behavioural advertising & profiling, including geo-location Creation of a unique username (not PII)		advertising. Virtual world, or games app that includes username registration, leaderboards	Reconfirmation of birthyear; or, Two-factor confirmation, eg Neutral age gate plus Confirmation provided by email or text message	2. Statement by parent that he is the holder of parental responsibility.
Enabling of notifications (eg, push) City-level geo-location information	Low	Apps that request permission to send push notifications; provide services based on city location (eg transport)	Confirmation that subject is over age of consent, via a simple, neutral age gate	**Direct Notice**. Opt-in, and direct notice sent to parent, stating type and purpose of collection and linking to Privacy Policy. No further verification of parental holder of responsibility
Technical online identifiers used for internal operations purposes only (analytics, contextual advertising, personalisation, security) Country-level geo-location information	Low	Casual games site with no registration, only contextual advertising	Processing on **Legitimate Interest** basis. No age check required.	Processing on **Legitimate Interest** basis. Parental consent not required. n/a
No data collection	None	Corporate website for marketing purposes, no advertising, no trackers	No age check required.	Parental consent not required. n/a

All of the above is of course subject to the prerequisite that the online service meet the transparency requirements, in particular when it comes to notices children can understand.

Example 1: educational website that finances itself primarily through advertising.

If advertising is delivered only contextually and no cross-domain tracking is allowed, then this represents Low sensitivity and would not require age verification or parental consent.

Publisher would have to ensure all technology and advertising partners are aware of child-directed nature of site and is responsible for guaranteeing that they are not collecting technical online identifiers that could be used to profile users. Social media plugins would not be allowed.

Example 2: mobile social application that enables chat, connecting with friends, sharing content under real names.

Use of real names, open text chat and the ability to connect with strangers make this High Sensitivity, eg a service that requires age verification and/or verified parental consent.

Example 3: virtual world that allows interactions between anonymous avatars.

Provided measures are in place to prevent disclosure of personal information (eg filtering out real names or phone numbers in unmoderated channels or chat rooms), then this represents Low sensitivity, with no verification or parental consent required.

Example 4: voice-based virtual assistant, or Internet-connected toy.

Given that audio files are likely to be stored and analysed in the cloud, and it is not technically feasible to filter out personal information in moderation, this represents High sensitivity and should require both age verification and Verified Parental Consent.

If the service provider can demonstrate that it is using any collected audio files solely for purposes of transcribing a command, and immediately deletes the audio files thereafter, we may consider this case Medium sensitivity, requiring only a simple opt-in + Direct Notice to parents.[18]

2.2 Privacy Controls & Notification

All new data privacy laws include the critical principles of transparency and informed consent. This reflects the widespread recognition that privacy notices have become (or always were) ineffective. Those on the most widely-used social platforms can run to 5,000 words of densely-written legalese. It was common for adults to have no idea how their data might be used by different service providers. Most sites require that you accept terms and conditions

[18] We recommend as a best practice following the recent guidance from the U.S. Federal Trade Commission (FTC) on how virtual digital assistants can comply with COPPA:
https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings

before you can use them, and many users will consent without reading or understanding what they are consenting to[19].

It is worth noting that the GDPR's strict requirements that consent be "freely given, unambiguous, specific and informed" has been one of the most controversial and difficult aspects of the law to implement. In particular, the large technology platforms have struggled to balance their vested interest in continued data collection with the new consent requirements, as evidenced by the multiple lawsuits currently working their way through the courts,[20] and the first fines to be issued by EU regulators.[21]

The GDPR's transparency requirement explicitly says that any child-directed site must have privacy notices that are easily read and understood by children. This is challenging, in particular across different age categories, and so we set out below our recommendations regarding the content and language of child-friendly privacy notices; how to design and 'layer' notices; easy-to-use privacy controls; and mechanisms for ensuring appropriate parental involvement.

2.2.1 Content

Notice requirements should be used for the most critical elements that are relevant to the child user, and then attempt to translate that disclosure into language the child can understand. We suggest the following sections (with examples of language):

Exactly what the online service's approach to data collection is

It's important for publishers to set out their data collection 'philosophy' in order to give context and comfort to the user.

For example: We'll never ask you for personal information, but our app needs to collect some data from the way you use it in order to work. We'll always tell you what we're collecting and why, and we'll do our best to keep your information safe. You can help by not sharing any personal information on the app!

Exactly what personal data is being collected

Within this section the types of data should be detailed, and explained in simple terms.

[19] Click to agree with what? No one reads terms of service, studies confirm (*The Guardian*, 3 March 2017)
You're not alone, no one reads terms of service agreements (*Business Insider UK*, 16 Nov 2017)
[20] Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR (The Verge, 25 May 2018)
Apple & other tech giants cited by Austrian group for failing to meet GDPR (AppleInsider, 18 Jan 2019)
[21] Google fined €50 million in France for GDPR violation (InsidePrivacy, 22 Jan 2019)

For example: We need to collect your email address and username to create your account, and information about your device so that we can make the app look great.

Why their personal data is being collected

The user should be able to identify the purpose of processing, whether it is required for the service to work, to improve features, or to deliver advertising, etc.

For example: We collect non-personal info to give you the best app ever, so it looks good, contains everything you love and we know how to help you with any bugs.

If and how their personal data may be shared with third parties

For example: If the police or government ask us to help stop or investigate a crime we may have to give them your username and internet address.

The rights of the user and how they can exercise them.

For example: You or your guardian can look at, change, correct or delete any information about you on the app. Just ask your parent or guardian to contact us.

2.2.2 Design of notices and 'layering'

It is important to consider how the information contained within a data privacy policy is presented.

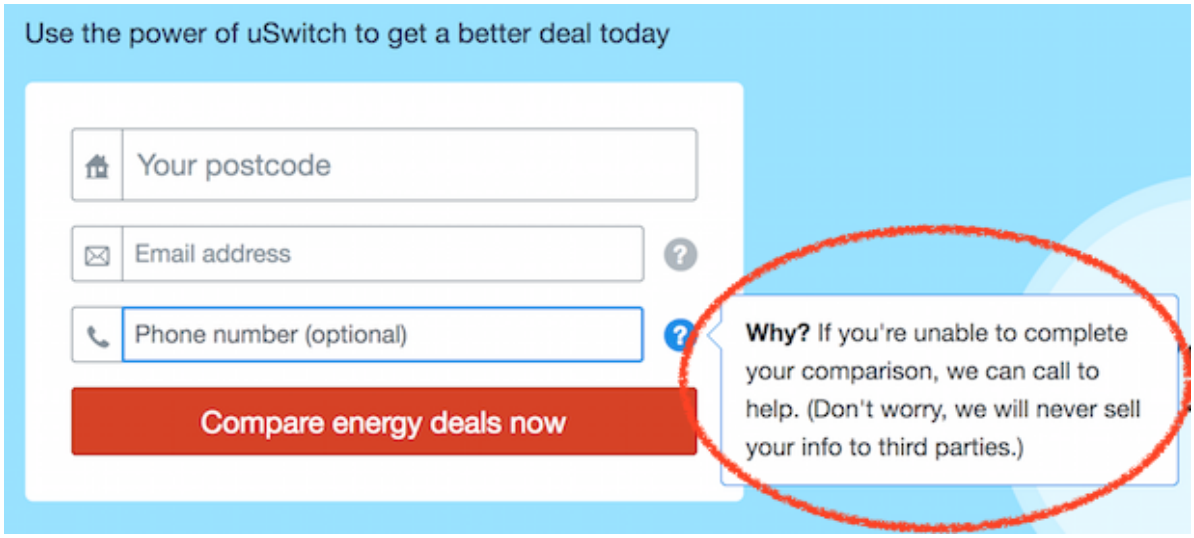
Consent needs to be informed, that is users need to know what they are consenting to and why. A balance needs to be struck between giving sufficient information and not overpowering the user with a 'wall of words' which could have an adverse impact on readability, particularly for younger readers.

For this reason layered privacy policies should be encouraged, whereby key statements or information are offered in a concise manner with the option for the user to review fuller text if desired. Layering could also be supported through images, video or other graphics

Topline information, such as that suggested above, can be linked using "hover" functionality, or click-throughs, to a more comprehensive document.

The UK's ICO has provided useful examples of layering, so we won't repeat them here, except to say that this approach works particularly well to address the challenge of communicating privacy notices to children.

Another good example is that applied by uSwitch:



In general, we are seeing more frequent attempts to innovate when it comes to bringing privacy to the attention of younger audiences, either by adding a separate child-friendly statement to a regular privacy policy (for example, Beano's Privacy Policy), or a specific child-facing information page such as the PopJam privacy policy re-written for kids. Other examples of child-friendly privacy policies are:

- TutoTOONS
- SuperCell

This remains an area that is challenging for publishers, in particular independent content owners who may have limited ability to work with legal teams to develop the best approach. This is a topic where we strongly encourage as much guidance, specific frameworks and comprehensive examples as possible.

2.2.3 Privacy Controls

Regardless of whether an app or website is general audience or child specific, clear labelling of privacy controls should be encouraged.

Most apps and websites offer some degree of user control comprising one or more of:

- user profile visibility

- user blocking
- search history deletion
- notification management
- ad enablement
- cookie management

In terms of design, there is no current uniformity among toggles, controls or dashboards for users to exercise personalisation or privacy controls. This creates an opportunity for a code of practice to offer a common interface so that children and parents can easily identify when a control is offered, what choices are available and whether a given choice has been made. Given that a child may have several apps on their device(s) with essentially the same control features in different manifestations across those apps, identifying and selecting those controls may be overwhelming or confusing, particularly at scale with different toggles, buttons, colours or sliders.

For example, if a user has exercised a choice to have a feature active or inactive, that choice should be clearly identifiable—we recommend clearly labelled large toggle switches (see example below from the BBC).

Using large bold titles and short descriptions coupled with symbols such as ticks and positive colours in familiar colours, (e.g. green for on, greyed out, red for off) should help children easily understand whether they have a choice, the selection options they have and (at a glance) understand what choices they have made.

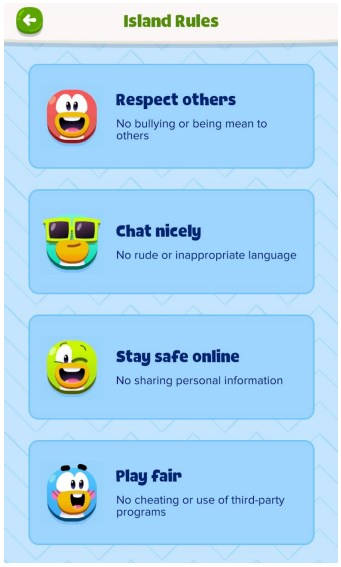
Each control should be clearly labelled. Plain, simple language such as ‘on or off’ should be used instead of adult-themed vocabulary such as ‘enabled’ and ‘disabled’. The label should be placed in close proximity to the control. An example of a child-directed application (Roblox) where the language is quite adult-oriented and the toggle controls distant from the description shown below:

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

The target audience of the service and the sophistication of general users should also be taken into consideration when designing interfaces. Toggles may be supported by additional visuals—such as a padlock or graphic to show that a feature has been unlocked or locked. For example, Animal Jam's controls visually explain some of the settings. Although in this example, the descriptions supporting each toggle are high level and may not provide sufficient information for a user to make an informed decision:

Even if there is no specific call to action for the user, the use of colour and graphics is a useful approach to express key messages, whether house rules or safety messages. For example see Club Penguin's approach to engaging users with regard to their house rules:

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602



Settings Options

There is a balance to be struck between offering granularity of choice and having a sufficiently clear dashboard to enable users to exercise their choices in a timely manner. There is no definitive approach whether a single page of controls (with simple descriptions), or several pages of more detailed controls is the right approach for younger audiences. For example, Animal Jam offers a clear but light set of controls:

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

Balancing the need to inform users of their choices with the age-based understanding of the audience is challenging, but we recommend the following best practice approach:

For all age ranges privacy controls should have clear bold titles and succinct descriptions. For pre-school users images may help illustrate their purpose. Toggles are a clear and familiar way to give control to all age groups. For 3-12 year olds they should be coupled with ticks and a positive green colour to clearly indicate that setting has been set to ‘On’. Plain, simple language such as ‘on or off’ should be used beside the toggle. These recommendations should help kids easily understand what state the settings is in and make it obvious if they adjust a setting.

TotallyAwesome Singapore Pte. Ltd.
137 Telok Ayer Street #06-04
Singapore 068602

About TotallyAwesome:

TotallyAwesome is the fastest-growing kids digital media company in the Asia-Pacific region, reaching over 170M kids monthly across desktop, mobile and online video. The company operates a kid-safe and compliant content and advertising platform. TotallyAwesome makes sure brand engagement with the youth market is safe, effective and entertaining.

TotallyAwesome was founded by SuperAwesome and Inspire Ventures and is led by a track-record management team responsible for some of the top games, advertising and digital content startups in the world. It is headquartered in Singapore with offices in Australia, India, Indonesia, Philippines and Vietnam.

About SuperAwesome:

SuperAwesome is the leading provider of 'kidtech', technology and services used by companies worldwide to enable safe, compliant (COPPA, GDPR) digital engagement with children. The company serves over 250 customers across industries including toy, film, entertainment and video games. From its London headquarters, SuperAwesome employs a team of 130+ employees, including more than 35 software engineers, to develop Privacy by Design technology focused on the needs of the childrens' digital media ecosystem. SuperAwesome also operates KidAware, the kids industry's education and certification programme, training digital media professionals around the world on kids' data privacy and digital best practices.

SuperAwesome is actively involved in working with the market and regulators in developing and implementing digital child safety policies, including contributing to ongoing consultations in relation to data privacy regulations.

https://www.superawesome.com