5Rights' interim comments on the draft Age Appropriate Design Code
May 2019

We very much welcome the Information Commissioner's draft Code, which represents an important first step towards giving children and their data the specific protection that they require in the digital environment. Since the draft Code was published, we have engaged with a diversity of stakeholders in our network, including children themselves, all of whom have contributed to the comments and recommendations that are set out in this document. We hope it is useful for those who intend to respond to the ICO's consultation, and we would welcome any thoughts and feedback on it.

For the avoidance of doubt, this is not the formal response that we will be submitting to the ICO as part of the consultation. We will publish that in due course.

About 5Rights Foundation

The digital world was imagined as one in which all users would be equal, yet a third of internet users are children.[1] Nearly one billion children are growing up in an environment that systematically fails to recognise their age, and in so doing, fails to uphold the protections, privileges, legal frameworks and rights that together constitute the concept of childhood.

Working closely with children, 5Rights Foundation operates in the engine room of the digital world: supporting enforceable regulation and international agreements; developing policy in data protection and child online protection practice; with our network of engineers building technical standards and protocols; and helping businesses re-imagine the design of their digital services.

5Rights Foundation believes that all children need to inhabit a digital environment that anticipates their presence and meets their needs, so they can access it *knowledgeably, creatively, and fearlessly*.

Table of Contents

Overview

The draft Age Appropriate Design Code (the Code) was published by the Information Commissioner's Office (ICO) on 15th April 2019. It is a standalone, statutory data protection code for children under the age of 18, but it sits within a broader policy/media context that is informed by the Government's Online Harms White Paper, the Digital Economy Act 2017, statements made by Secretaries of States from the Home Office, the Department for Digital, Culture, Media, and Sport, and the Department of Health, and a constant flow of media headlines. In this context, the Code offers a systemic and proportionate first step to addressing some of the issues faced by children online, where they intersect with the collection and use of their personal data.

Data protection is a crucial part of a multi-faceted approach to making the digital environment a positive and rights-respecting environment for children. The use of children's data determines the content they see, the people they can be contacted by, the adverts they're targeted and bombarded with, and the amount of time they spend online. It can shape their perspectives, co-author their opinions, influence their identities, mediate their relationships, nudge their behaviour and affect their mood. In sum, data protection is a high priority area if we are to support children in the digital environment.

We have been delighted by the response of civil society, many in business, academia, the health sector and the engineering community, as well as many national and international bodies. We have been disappointed by the initial response of a small but powerful lobby within the technology sector, who continue to see protecting children's data as an affront to their business model, rather than simply a requirement of doing business.

Finally, we wish to commend the ICO for its interpretation of section 123 of the Data Protection Act 2018 and we hope that our comments provide useful additions and clarifications for the final draft.

General comments

Intent of the Code

The Commissioner could usefully state that she will consider intent when assessing compliance with the Code. The Code is broad - it covers a range of areas, applies to a range of services, and will apply to a range of emerging technologies.

We recommend: that the Code state that services *must have regard to the intent of the Code, rather than simply the strict letter* as this will promote good practice and serve to future-proof the Code.

Proportionality

In its Regulatory Action Policy,[i] the ICO makes clear that its approach to both regulation and enforcement will be fair, targeted, and proportionate. This includes reserving the right to consider 'aggravating or mitigating factors' in all its work, including:

- the vulnerability, if any, of the individuals affected
- the state and nature of any protective or preventative measures and technology available, including by design
- whether the attitude and conduct of the individual or organisation concerned suggests an intention, wilful or negligent approach to compliance; and
- the relevant individual or organisation's prior regulatory history.

[i] The Regulatory Action Policy is currently subject to Parliamentary consultation and approval, though it is unlikely to change significantly.

The policy also sets out that the ICO will use its fining powers in an 'effective, proportionate and dissuasive' way, and that it will consider the 'risk of harm to individuals or the level of intrusion into their privacy' when issuing information notices.[2]

Whilst this approach is clearly set out here, we have received a great many inquiries on this point and it would be useful for the Information Commissioner to make clear that the nature of the data, the extent to which the data is collected, processed, or shared, the purpose for which the data is used, and the risk that children are exposed to, will each be taken into account in coming to a judgement in relation to the Code. This overarching statement, twinned with the commitment to the best interests of children being a primary consideration, would allow all parties to assess their own practice.

We recommend: that it is made clear in the text of the Code itself that the ICO intends to be proportionate, and that the Code spells out the criteria that the Information Commissioner will be applying.

Supporting innovation

We note that some of the larger tech players are suggesting that the Code could damage innovation and will hit smaller firms the hardest. We have consulted widely with engineers and computer scientists working across many sectors, and to a person they do not agree. Rather, they suggest the Code is a greater challenge to the incumbents who have poor practice, but that many of those bringing new products and services to market will be able to embody their commitment to child safety and data protection from the start. Indeed, we have received a number of comments from businesses – keen to treat children fairly – that welcome the guidance and clarity the Code provides, and which suggest the approach a company takes to data ethics is increasingly becoming a competitive differentiator.[3]

We recommend: that the Information Commissioner makes clear that, while innovation and child protection are almost never mutually exclusive, if the two do conflict, child protection must always take priority.

Upholding the rights of children

Section 123 of the Data Protection Act 2018 states that 'in preparing a code or amendments under this section, the Commissioner must have regard to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child'. We feel the convention could permeate the Code more thoroughly. This would serve to guard against a narrow focus on a list of known harms and would serve to future proof the code. Taking a rights-based approach embodies the fact that children have rights *irrespective* of any harm that may result and would underline the overarching nature of the 'best interests' provision.

For instance, 'age-appropriate application' supports a child's right under Article 5 to be treated in accordance with their evolving capacities. 'Nudge techniques' impact on a child's freedom of thought under Article 14 and their right to rest and leisure under Article 31. The provision on 'profiling' supports their right to protection from information or material injurious to their wellbeing under Article 17(e).

We recommend: that the Code is more consistent in referring to the Convention on the Rights of the Child.

Inferred data

The Information Commissioner has made clear on numerous occasions that inferred data *is* personal data, most recently in her evidence to the House of Commons Digital, Culture, Media, and Sport Committee in April 2019:

> "Inferred data is personal data… If inferred data is not personal data, it is completely unregulated."[4]

We strongly endorse this important clarification. The impact that the processing of inferred data has on children is indivisible from personal data gathered more directly.

We recommend: that the Code makes clear overall, or within each provision of the Code, that data inferred or derived from a child's personal data *is* personal data and is therefore subject to the Code.

Purpose and storage limitation

Article 5(1)(b) of the GDPR states that personal data shall be:

> 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.

This is referred to as the 'purpose limitation' principle and interconnects with the 'data minimisation' principle set out in Article 5(1)(c) (as well as the 'storage limitation' principles under Article 5(1)(e)). These principles are all overarched by the principle of 'accountability', which a service provider needs to implement in order to demonstrate their compliance with the GDPR. Therefore, what service providers do with children's data once it is collected requires as much scrutiny and limitation as whether the data is collected in the first place.

We recommend: that the Code places more emphasis on purpose limitation throughout and, given the importance of this principle, we urge the Commissioner to add an additional provision relating to purpose limitation, or amend the current 'data minimisation' provision to give purpose limitation equal prominence.

'Core service'

We recognise the concept of 'core service' but are concerned that more clarity is needed as to what can be considered a core service. For example; many social networks rely on advertising for their revenue, so one such service might describe 'advertising' as its core service rather than 'social network' and therefore serving users with adverts could meet the 'core service' test.

The concept of 'core service' should be clarified to mean the service that *a child could reasonably be expected to have believed* as the core service, and limited to the purpose for which they are accessing it. Engineers in particular say that 'purpose limitation' and the doctrine of 'reasonable expectations'[ii] are more useful concepts than 'core service', since a company may seek to define its core service in a way that contravenes the spirit of the Code (for instance by freeing it from certain regulatory obligations or benefiting it commercially to the detriment of its users).

In a similar vein, any moves towards 'feature bloat', whereby unnecessary 'core' features are added to a product or service despite not being of value to most users, should also be explicitly constrained by the Code.

[ii] As established in various areas of law, particularly contract and consumer rights law, as well as other related areas including insurance law and administrative law.

We recommend: that the Code provides a definition of core service that incorporates the principle of purpose limitation and the doctrine of 'reasonable expectations'.

'Compelling reason'

The term 'compelling reason' is used throughout the Code, particularly in relation to the provisions on default settings, data sharing, geolocation, and profiling. We support the ICO in requiring online services to justify their use of children's data but feel that the Code could usefully clarify that what constitutes a 'compelling reason' should be from the point of view of the child, should provide examples of compelling reasons in different contexts and should outline the criteria by which it will be judged.

We recommend: that the Code clarify that 'compelling' relates first and foremost to the best interests of the child and to the strength of the evidence presented.

Screen-centricity

The Code references non-screen-based services and we welcome the ground-breaking provision relating to connected devices. However, future technology will be increasingly embedded and 'environmental', rather than simply screen-based. The Code should make clear that the nature of the user interface or interaction pattern is not an excuse for failing to comply with its provisions.

We recommend: that the Code include additional, non-screen-based examples in the 'transparency', 'nudge techniques', 'default settings', and 'online tools' sections, among others, to underline the fact that the Code's provisions apply to interactions that may not be screen based.

Online gaming

We are concerned that there is an absence of examples and language relevant to online games. Online games have tended to be under-associated with data processing, despite the collection of significant and diverse amounts of data from voice recordings and video footage, to user messaging and spending habits.[5]

We recommend: that the Code offers further direction of best practice to help providers of online games to fully understand their obligations under the Code.

Vulnerable groups of children

There is a growing body of evidence that children with special educational needs or disabilities, children in care, young carers, and children with mental health issues face specific challenges online.[6]

We recommend: that the Code explicitly requires online services to properly consider the additional vulnerabilities and needs that such children may have in their Data Impact Assessments and take steps to meet those needs.

'Services covered by this code'

We welcome the Commissioner's important assertion that the Code 'applies to services that aren't specifically aimed or targeted at children, but are nonetheless likely to be used by under-18s.'

Greater clarity on 'likely to be accessed by children'

The section headed *When are services 'likely to be accessed by children'?* would benefit from greater clarity and the addition of some examples. For instance, the Code states that services must be able 'to point to specific documented evidence to demonstrate that children are not likely to access the service in practice' but it would be helpful to provide some detail on the threshold for this evidence. Similarly, the Code states that it applies to services 'even if [children are] only a small proportion of the overall user base' but does not offer a threshold. Additionally, 'proportion' may be an unhelpful metric since some services are used by huge numbers of people, where even a small *proportion* of children may amount to a large *number* of children.

Ofcom's Broadcasting Code may be useful here in its definition of content 'likely to be accessed by children'. It refers to factors such as 'the nature of the content' and 'the nature of access to the content e.g. ***whether there are measures in place that are intended to prevent children from viewing and/or listening to the content'*** (our emphasis).[7]

Additionally, it would be helpful to clarify that services whose own terms (rather than the law) prohibit under-18s, but which are nonetheless 'likely to be accessed' by children, are in scope of the Code. For example Amazon, states:

> 'We do not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18 you may use the Amazon Services only with the involvement of a parent or guardian.'[8]

Similarly, Netflix states:

> 'You must be 18 years of age or older to subscribe to the Netflix service…While individuals under the age of 18 may utilize the service, they may do so only with the involvement, supervision, and approval of a parent or legal guardian.'[9]

However, both Amazon and Netflix clearly fall within scope of the Code given that children are likely to access – and be accessed by – these services. Further clarification should be provided to make clear that parental involvement does not exempt services from the Code or lessen the protections they are required to provide to children under the Code.

We recommend:

- The Code should provide more detail setting out the criteria by which a service will be judged as "likely to be accessed" by children, including what steps they might take in their Data Protection Impact Assessments to establish if they meet these criteria.
- Services should be required to include estimations of the age-breakdown of their user-base (and how such estimations were made).

Comments on the summary provisions

1. **Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.**

We welcome the inclusion of the 'best interests' test in this Code, which focuses the design of service on the needs of the child, and sets an appropriately high bar for the processing of children's data.

2. Age-appropriate application: Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

This provision tackles a fundamental flaw in current practice where online services routinely fail to identify which of their users are children. This is despite many such services having a minimum joining age. Allowing a failed system of age verification to be a norm, even where the need has already been established, creates a lack of trust in the sector overall.

The Code strikes the right balance here, requiring online services to give children's data specific protection, without stipulating the mechanism of verification. Rather, the Code simply requires that this is done in a robust and effective way. This allows for the use of a number of existing options as well as for future innovation. It also allows companies who do not wish to establish which of the users are children to apply by default the Code's standards to *all users,* thereby ensuring the standards are applied to *all children*.

The ICO is also right to state that data may be collected for age verification purposes but must not then be used for any other purpose.

Proportionality
This provision would benefit from a statement about proportionality of both compliance and enforcement.

We support an approach that requires online services to implement demonstrably robust age verification mechanisms if they do or have any of the following; a) a large numbers of child users, b) pose a particular risk to children, c) process significant amounts of personal data, d) process particularly sensitive personal data, or e) make sensitive or impactful judgments on the basis of children's data. Services that do not process a child's data in these ways or for these reasons, or services that are demonstrably in the best interests of a child, many not require the same level of or any age verification, but must still comply with the other provisions of the Code.

Self-declared age
We welcome the Code's move to address the failed system of self-declared age. In the UK, three out of every five children have a social media account by the age of 12, despite a minimum age limit of 13-years-old.[10] In a recent appearance before the House of Commons Digital, Culture, Media and Sport Committee, a representative of Snapchat (which allows users to self-declare their age) conceded its age verification processes do not work.[11]

However, we are concerned that the drafting of the section '*Tailor the measures in this code to the age range of your users'*, appears to undermine the stated position by allowing and encouraging services to tailor services to 'the declared age of each user'. This contradiction could be usefully clarified.

Technical feasibility
It is already possible and practical to establish the age or age range of users in a robust, privacy-friendly and low-friction way. The fact that this is not done widely across the digital ecosphere has to do with commercial interests, lack of investment and, crucially, no statutory requirement to do so. In many cases it is even possible to allow users to take their proof of age with them as they access different services, in much the same way that Facebook and Google account-holders can use those accounts to log-in to other services seamlessly. Such mechanisms would need to comply with the

Code's requirements on data minimisation, data sharing, and others, but there is no technical reason they could not be reconfigured to offer solutions to the portability of age verification.

Many online services have a clear understanding of the age or development stage of their users from the way they interact with the services and devices they use. This includes data points such as their use of language, the way they type, 'pinch' a screen or scroll, as well as more 'traditional' data points such as their browsing history and the information they have chosen to share about themselves. In 2013, researchers found that a user's age could be discerned with 75% accuracy on the basis of their Facebook likes ***alone***.[12] These contextual assessments are already widely used by industry for the purposes of commercial profiling.[iii] Assessing age or the development stage of a child using the same technical infrastructure is just one of a variety of emerging approaches (though in deploying it, services must have regard to the Code's requirement that data taken to establish the age of the child may not be used for other purposes).

We recommend:

- The Code should provide greater clarity about the proportionate responsibilities of different online services, and what factors the ICO will take into account in enforcing this provision.
- The Code should make clear that, while wide-spread age verification and assessment is not yet a norm, there are mechanisms available and the Commissioner will expect companies to either implement them or innovate in order to comply with this provision.
- The ICO should periodically consider the need to update or clarify its guidance on age-appropriate application of the Code in light of developments in the technology available.

3. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

Transparency is fundamental to fairness and we welcome the careful consideration the Code gives to the needs of children at different stages of development. Given the extent to which so many children's rights are mediated online – free expression, free association, access to information, privacy – children must be empowered to understand the consequences of using online services and to play an active role in balancing the risks and benefits. It is essential, therefore, that the information is presented in ways they can understand and at times that do not take advantage of their desire to participate immediately.

Greater clarity on what services must be transparent about

Online services must take the minimum amount of data for the shortest amount of time, use it in the least invasive and most purpose-specific ways and share it only when manifestly in a child's best interests. In the small number of cases where this is not happening, it should be clear why they are taking which data, what the potential impact will be on the child, who (specifically) has access to the data, for what purpose, and for how long that data will be held and/or used.

[iii] For example, in 2018 various gambling and alcohol advertisers pulled their ad spend from Snapchat citing concerns about Snapchat's ability to prevent these ads being served to minors. Snapchat was quick to refute the concerns, stating that it 'offers amongst the most sophisticated targeting in the industry and by introducing new tools…and incorporating additional signals into our targeting, advertisers have a reliable and flexible way to ensure their ads reach the right audience.' If Snapchat and similar companies are confident that the age verification mechanisms they use to target advertising are effective, we see no reason why they can't be similarly applied to complying with this Code.

We note that the Code signposts services to Articles 13 and 14 of the GDPR, but believe it should also direct them to the additional transparency provisions set out in Recitals 60 and 61. These are vital and include the following:

- 'The data subject should be informed of the existence of profiling and the consequences of such profiling.'
- 'Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data.'
- 'Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient'
- 'Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information.'

The Commissioner should require that a child should have a reasonable chance of understanding how their data will be used or impact on them.

Fair terms

Given this, the provision would be strengthened by including reference to the well-established consumer rights law principles of 'fair terms'. Guidance supporting The Consumer Rights Act (2015) states:[13]

> 'As indicated, openness is not enough on its own, since good faith relates to the content of terms as well as the way they are expressed. Fair dealing has been authoritatively said to require that, in drafting and using contract terms, a trader 'should not, whether deliberately or unconsciously, take advantage' of the consumers' circumstances to their detriment.'

And that:

> 'Businesses need to take particular care in communicating key terms to consumers who may have greater difficulty than others in collecting, processing and acting upon information and this in exercising choice effectively…for example, young consumers.'

The guidance makes clear that: 'Businesses are not ignorant of how consumers are likely to behave' and must acknowledge the 'inherent biases affecting consumers' behaviour generally' - 'Concerns to fairness are likely to arise where businesses…exploit such biases to their advantage.'

This has implications for the transparency of online services, their use of nudge techniques, the default settings they provide to users, and the content of their terms and policies themselves.

In addition, the guidance usefully sets out the idea of 'blacklisted' terms, which must never be used and are not binding or enforceable if they are, and a 'grey list' of terms, which may also be regarded as unfair. We would urge the Commissioner to consider the relevance of these terms to children's relationship with online services, and whether similar guidance might be necessary under the Code.

Children with specific needs in relation to transparency

Consideration should be given to children who may have specific needs in relation to the transparency of published terms. Children who are visually impaired, for instance, or who have

special educational needs or disabilities, are equally entitled to a high level of transparency in relation to their data, and we would like to see these further reflected in the Code.

We recommend:

- The Code should be more specific about what information online services must be transparent about. However, the onus to ensure that online services communicate to users the information that is important to and impactful on them – without recourse to an exhaustive list – must remain with those services.
- The Code should include reference to established consumer rights law principles relating to fair and unfair contract terms, and consider the benefits of producing similar guidance
- The Code should outline its expectation that online services consider those children with specific needs in relation to transparency as part of their Data Protection Impact Assessment.

4. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

We welcome the safety-by-design requirement implicit in this provision and the ICO's approach of referencing existing codes of practice and formal advice, including the 'precautionary principle' where none exist. Personal data is processed in so many different contexts that no Code should seek to address or anticipate every case of detriment that may arise. Providers are in a far better position to consider anything that is relevant to their processing, and be able to justify their processing in light of any relevant guidance. However, there are some very clear areas of risk and it might be useful for the ICO to indicate a broader set of sources that online services could consult in complying with this provision. For instance:

- UK Centre for Internet Safety (UKCIS)
- The European Data Protection Board (formerly the Article 29 Working Party)
- ICT Coalition for Children Online
- The Centre for Data Ethics and Innovation (CDEI)
- Alliance to Better Protect Minors Online
- The Office of Fair Trading's Principles for online and app-based games
- Code of Practice on Disinformation (European Commission)
- Internet Watch Foundation's FC Code of Practice
- Consumer rights guidance, including guidance on unfair contract terms
- The UNCRC and forthcoming General Comment children's rights in relation to the digital environment
- Any Codes introduced following the UK Government's Online Harms White Paper.

Behavioural advertising

This section could note to a greater extent the impact of behavioural advertising on children. We cover this in more detail in the section on profiling.

We recommend:

- The Code should include a greater range of sources of guidance to assist online services with compliance.

5. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

We welcome this provision and commend the ICO for recognising that processing personal data cannot be 'fair' if online services fail to uphold the rules and policies users have signed up to. It is fundamental to users' expectations of the services they access that the agreement will be upheld on both sides. In relation to children specifically, published terms allow children, or the adults responsible for them, to decide if the service is age-appropriate and to anticipate any risks it might pose.

We note that this provision brings the Code in line with the Government's Online Harms white paper, which sets out that:

> 'Relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action.'[14]

This is the least we should expect of online services, and – if meaningfully enforced – this provision would significantly improve the experiences of children in the digital environment.

Fair terms
As stated earlier, under the transparency provision the Code should align itself with established consumer rights law principles of 'fair terms', 'good faith', and 'fair dealing'. That statement is worth repeating here, and would serve to mitigate the risk of online services responding to this provision by amending policies and standards to reduce their obligations to users.

In addition to drawing on 'fair terms' principles, the Code should signpost other relevant guidance. For instance, the Office of Fair Trading has produced 'Principles for online and app-based games', which specifically relate to children.[15] The principles address the following concerns:

- 'misleading commercial practices, including failing to differentiate clearly between commercial messages and gameplay
- exploiting children's inexperience, vulnerability and credulity, including by aggressive commercial practices
- including direct exhortations to children to buy advertised products or persuade their parents, carers or other adults to buy advertised products for them
- payments taken from account holders without their knowledge, express authorisation or informed consent.'

For absence of doubt these principles would not be sufficient in-and-of themselves, but applied in conjunction with the other provisions of the Code, they offer helpful further detail to relevant online services.

We recommend:

- In addition to requiring services to uphold their own published rules, the Code should require services to meet fairness principles under consumer rights law
- The ICO should consider inserting an appendix, signposting principles of fair, child-friendly terms from other sectors and bodies (whilst making clear they are additional to the requirements of the Code).

6. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

This is a significant provision. Default settings are the starting point for children when they first access an online service and are the gateway to giving children the specific protections they are entitled to under the GDPR and this Code.

Using default settings as a nudge technique
We welcome that the Code makes clear that high privacy default settings must not be used to block or restrict the access of children to services that do not rely on lower privacy settings. Doing so amounts to a 'nudge' to encourage a child to lower their settings.

The provision is an invitation to the sector to introduce new norms, and the Commissioner could usefully state that she will consider intent when assessing compliance. For example: should an online service use its default settings to get children to behave in ways that are clearly not in their best interests, it will be deemed as non-compliant with the Code.

Appropriateness of settings made available to children
The Code is right to say that 'many children will never change their privacy settings from the default position'. This is because most online services have favoured data collection and default settings have been deliberately onerous to change as a result.[16] As the Norwegian Consumer Council puts it in its report *Deceived by Design*, 'default settings are often sticky', because 'having users opt in to things such as personalised advertising could affect a company's bottom line.'[17]

The Code should make clear that some settings or options are never appropriate for children, irrespective of their default setting or whether those other settings or options are appropriate for older users. For example, in an online game or a social network that has both adult and child users, it may never be appropriate to allow older users to identify and view the profile of child users or to contact them unsolicited.

If an online service wishes to provide its adult users with features or settings that are not appropriate for children, it can do this by either age-verifying upfront or offering all users high privacy by default (many adults would be very happy with that) and then allowing users to prove their age to access any additional feature or settings. We note that adults are likely to have many pre-existing proof points that could easily establish they are over 18 and make this process seamless.

We recommend:

- The Code should make clear that default settings must not be used as a means of encouraging children to make decisions that are not in their best interests
- The Code should clarify that services must consider the appropriateness of making different settings available to children over and above the defaults, having regard to the developing capacities of children and their best interests.
- That the Code must explicitly state that default settings that are designed to encourage, or have the effect of encouraging, children towards adopting lower privacy settings will be deemed non-compliant.

7. Data minimisation: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

This provision flows directly from Article 5(1)(c) of the GDPR and is a vital protective measure for children. We endorse the addition of 'actively and knowingly engaged', given the rise in passive collection of data, as well as the widespread practice of online services processing children's data

even when they have navigated away, logged off, or closed a service or app. Clear guidance on what 'actively and knowingly engaged' means would be useful.

'Processing' not just 'collecting'
Article 5(1)(c) of the GDPR relates to the processing of personal data – as defined under Article 4(2) of the GDPR – and not simply the collection of personal data. Despite this, data minimisation is defined in this section as '*collecting* the minimum amount of personal data…', and the rest of the text reflects this narrower understanding. The Code should make clear that the data minimisation provision is based on GDPR and relates to any processing of personal data, not just its collection. Data inferred or derived from children's personal data must be explicitly included in the scope of the data minimisation provision.

This would require adjustment throughout the text, including (by way of example), an addition to the first example on page 49, which states: 'It is not acceptable to continue to track [a child's] location after they have closed the map or reached their destination'. The data minimisation provision should limit not just the 'tracking' (or collection) of a child's location data but also any other use of that data, including storing, disclosing, or making available that data, or the processing of it for profiling purposes.

Purpose limitation and storage limitation
We have made clear in our general comments that these two important principles receive insufficient attention in the Code, but are fundamental to its effectiveness.

Bundled permissions
The Code's requirement that online services refrain from bundling permissions for processing that is required for enhancements, with permissions for processing that is required for the core service (as well as bundling in processing required for different enhancements) is useful. However, the Code should explicitly prevent online services from bundling permissions – in general – unless there is a compelling reason to do so (having regard for the best interests of the child).

For example, if an online streaming service requires additional processing to make personalised recommendations to its users, permissions for that processing should not be bundled in with permissions to 'share your data with third parties' or 'show you ads from companies that might interest you' (subject, as ever, to the best interests test). Clarification on this point would be helpful.

As noted in the general comments section, the Code should also expect 'core services' to be defined in a manner that could be understood by the child and aligned with the reasonable expectations of the child accessing the service. Efforts to bundle permissions by defining the 'core service' in a way that doesn't reflect the child's active and knowing engagement with the service should be explicitly ruled out by the Code.

We recommend:

- The 'data minimisation' provision should be amended to give equal prominence to 'purpose limitation', and to pay greater attention to 'storage limitation'
- This section of the Code should be amended to make clear that data minimisation applies to all forms of processing, not simply to collection or retention
- The Code should provide greater clarity on bundling permissions, and explicitly prohibit the bundling of permissions unless there is an evidential reason to do so (having regard for the best interests of the child)

- The concept of core service should be clarified to mean the service that a child should reasonably be expected to have understood as the core service, limited to the purpose for which they are accessing it.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

We fully support this provision which shifts the status quo from one in which children's data is available to anyone and everyone, to one in which children are protected from casual and widespread data sharing. Given how widely, carelessly, and opaquely children's data has been shared, sold, and made available to date, this is a critical change.

Inferred data
Please see comments on this in the general comments section above.

Transparency
The sharing of data by and between online services is notoriously opaque. In 2017, GPEN found that 51% of website fail to mention that they share data at all.[18] Which? found that 'consumers tend to operate with an incomplete picture of data sharing and third parties, which means that most are surprised to learn about the extent of the data sharing ecosystem.'[19] The Horizon Digital Economy Research Institute's work with children also found that many were not aware that their data was collected and shared. Where they were aware, they disagreed with it and felt disempowered.[20]

The Code should tackle the lack of transparency in sharing, either in this section or under the transparency provision. Online services should be required to clearly alert child users and/or their parents or carers when their data is being or has been shared, as well as provide clear and prominent details about who specifically their data has been shared with and for what purpose. In the case of children, it should be the norm not to share their data.

Sharing required to provide a service
We are very concerned that the text in this section creates a contradiction with the summary provision itself. Specifically, the Code states:

> 'You should not share personal data if you can reasonably foresee that doing so will result in third parties using children's personal data in ways that have been shown to be detrimental to their wellbeing.'

The summary provision disallows the sharing of children's data unless there is a 'compelling reason' to do so, which is a higher and more appropriate bar.

The sharing of children's data for purposes that are clear and beneficial should be welcomed, but if the provision is to work, the starting point must be that a child's data should not be shared unless it is in their best interest. Moreover, this principle should apply to the sharing of children's data with each individual third party. Being able to justify the sharing of data with one third party does not entitle a service to share data with all third parties, and services should not be allowed to bundle permissions for sharing with multiple third parties unless they have a good reason for doing so. This is consistent with the provision and offers children a higher bar of protection for their data.

As an additional safeguard, the Code should also stipulate that a child's access to a service or feature that does not rely on the sharing of data must not be contingent on consenting to the sharing of that data. Equally, if a service or feature does rely on the sharing of data, it must only be shared with

those parties with whom it is necessary to share it (under the definitions of the Code – i.e. for the purpose intended by the child and in their best interests). If a service relies on the sharing of data with *one* third party, that does not mean data can be shared with *any* third party.

Whilst this provision poses a challenge to the business model of many online services, the purpose of the Code is to protect children's data, even if that protection conflicts with the commercial interests of the companies whose services they are using. Businesses in all sectors are required to consider the safety and wellbeing of their customers, especially children. As businesses and whole sectors move online, so too must the protections that they offer to children. As noted in our general comments, this has the potential to create a new market of products and services that prioritise children, leading to a more innovative and competitive environment.

We recommend:

- The Code must make clear that it is only permissible to share a child's data with third parties to the extent that it is necessary to do so in order to provide the service the child is actively and knowingly engaged with, and for the purpose that they might reasonably be expected to have intended
- The Code should clarify that making children's data available to third parties is covered by the definition of data sharing under this provision
- Inferred data must be considered as personal data for the purposes of this provision
- The Code should require online services to be more transparent about who specifically it is sharing children's data with and why and allow a child to opt out
- The Code should stress that sharing must be demonstrably in the best interests of the child.

9. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

We applaud the ICO's recognition in this section that the Code is designed to uphold the *rights* of children, rather than to simply keep them safe. It states:

> 'It may potentially fail to respect the child's rights under the UNCRC to privacy, freedom of association, and freedom from economic exploitation, irrespective of threats to their physical safety.'

We also welcome the Code's requirement that settings which make a child's location visible to other users should revert to off when children either navigate away, log off, or are not actively and knowingly engaged with that service or feature.

All geolocation tracking should default to off at the end of a session

The persistent tracking of a child's location fails to respect a child's rights whether their location is shared with other users of a service or it is collected and/or shared by the service itself. It is also likely to run counter to the principles of data minimisation and purpose limitation. The Code should clarify that geolocation tracking, even when not visible to other users, should default to off when a child navigates away or is not actively and knowingly engaged with that service (unless there is a compelling reason to continue tracking, taking account of the best interests of the child).

We recognise that there are many benefits to the processing of children's geolocation data, and many purposes for that processing that clearly serve the best interests of the child. However, geolocation data is also processed for a range of purposes that aren't in the best interests of the

child or are deliberately obscured from them. The Code is an invitation to industry to offer geolocation services to children in a manner that is transparent and truly offers them the benefits of the technology, whilst refraining from using their geolocation data in ways or for purposes that are not in their best interests.

Different ways of collecting geolocation data

The Code is right to recognise that children's geolocation data is particularly sensitive and therefore requires specific protection. We are concerned, however, that, as currently drafted, it does not capture the full range of ways that online services are able to collect geolocation data.

For example, many digital cameras record where a photograph is taken and stores that location in the EXIF metadata of the photograph. When a photograph is uploaded to an online service such as an email provider or social network, that metadata may be stored by the service irrespective of whether a child's settings allow the service to collect geolocation data directly. Many services might 'delete' or 'hide' EXIF metadata from other *users*, but that is not to say that they do not retain it themselves.

This is just one example of many of how a service might collect a child's location data 'indirectly', even if the child's settings do not allow the service to collect it 'directly'. In fact, Facebook's policy states:

> 'When Location Services and Location History are turned off, we may still understand your location using things such as check-ins, events and information about your Internet connection.'[21]

From the perspective of a child, *how* an online service collects their geolocation data makes no difference, and therefore it should not be possible do so without their active and knowing participation.

The Code should state that an online service must not process a child's geolocation data *irrespective of where it has come from*, unless the processing is service critical, and the child is knowingly and actively engaged in a way that makes them aware of the geolocation data collection and has explicitly consented to (and could reasonably be expected to understand the implications of) this processing through that specific service.

Data minimisation/purpose limitation/storage limitation

In addition, no more location data than is necessary should be taken or further processed (e.g. if a general location is adequate then a more precise one must not be collected), the data should not be stored for any longer than is necessary, and inferences must not be drawn from the data unless it is necessary for the functioning of the service (defined earlier in the context of purpose limitation and 'reasonable expectations'). In all cases it must be necessary to demonstrate a compelling reason to process a child's geolocation data, having regard to the best interest of the child.

In sum, the onus should be on the online service, not the child, to ensure that geolocation data is not collected or further processed either when it is unnecessary to do so or when the child is likely to be unaware that it is being collected.

We recommend:

- If a child has not given an online service permission to process their geolocation data, the Code should prevent that online service from collecting that child's geolocation data from elsewhere

- The Code should clarify that the processing of children's geolocation data is subject to the other provisions, and particularly to the principles of data minimisation and purpose/storage limitation
- The Code should clarify that geolocation tracking should default to off once the child navigates away, unless there is a compelling reason to do otherwise, having regard to the best interests of the child
- In fulfilling the *intent* of the Code (see general comments) an online service must ensure that a child's default geolocation settings are in the best interests of that child, and do not nudge them to activate geolocation services beyond the purpose they intend.

10. Parental controls: If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

This provision strikes an excellent balance between the rights of children and the responsibility of parents or carers. The provision makes clear that the purpose of parental monitoring services should be to protect and promote the rights of children, not undermine them. Clearly indicating to children that they are being monitored, having regard to their best interests and the stage of their development, is an extremely welcome development.

We note that many commercial services allow or support parental tracking, and whilst the code rightly limits its provision to making the child aware, it is worth noting that parental tracking can create a false sense of security and/or pose a security risk if the services are not sufficiently secure.

Parental controls are one feature of child online safety but do not replace the broader provisions of the Code, parental engagement in a child's online life, nor broader education and discussion about a child's use of technology and safe/unsafe conduct – all of which sit outside the remit of a data protection code.

Purpose limitation
Parental monitoring and control services often collect extensive and sensitive data on children, which may make children vulnerable to third parties. At a minimum the Code should make clear that data processed for these purposes must not be used by for any other purpose. Online services should also be required to demonstrate that they have sufficient security measures in place to prevent parental controls being hacked, as required by Article 32 of the GDPR.

Wherever possible, parental control services should not collect any personal data and instead allow data to flow only between the device of the child and that of the parent (or at least allow for the data to be encrypted).

Parental controls or permissions are not a substitute for applying the provisions in this Code
The Code should make clear that providing parental controls does not in any way abdicate the responsibilities of an online service to give children specific protection in relation to their data or to uphold their obligations under this Code.

We recommend:
- The Code should make clear that data processed for providing a parental monitoring service or feature must not be used by online services for any other purpose
- The Code should state that providing parental controls must not be used to allow an online service to fail to comply with the provisions of this Code.

11. Profiling: Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

We agree that profiling should be default off wherever it is possible and appropriate to provide children with a choice, but the Code should also be clear that the profiling of children must be limited in general. This provision should be linked to and indivisible from the data minimisation and purpose limitation principles. That is, services must only collect (or infer) the minimum amount of data necessary to build a profile, where 'necessary' relates to the specific purposes for which the profiling is required.

Presumption against profiling children

The Code should prevent online services from profiling children either in more detail than is necessary to provide them with the service or feature they are actively and knowingly engaged with, or for purposes that are not necessary to provide that service.

Given the requirements around data minimisation and purpose limitation, the current concentration on default settings alone is inadequate. The Code should state that a child must not be profiled unless:

a) Profiling is essential to the service or feature the child is using
b) Appropriate measures are in place to protect the child from any harmful effects, and
c) It is in a child's best interests.

If profiling meets these criteria, the Code should then stipulate (as above) that profiling must only be carried out to the extent and for the purposes that it is necessary.

If services wish to give children access to services or features that *do not* rely on profiling, but which may be enhanced or improved by profiling, they must first consider whether they have appropriate measures in place to protect the child from any harmful effects. If they cannot demonstrate this, options to activate such services or features must not be made available to children. If they can demonstrate that appropriate measures are in place, these services and features can be made available to children but must be switched off by default and must still comply with the Code's requirements on bundling permissions, data sharing, and data minimisation/purpose limitation.

None of this is to say children can never be profiled. The Code rightly identifies that profiling can be used for a wide range of purposes, some of which are legitimate. What it must rule out is the practice of profiling children in limitless and unnecessary detail, for limitless and unnecessary purposes, with no regard for their best interests.

Do not profile children to target them with advertising or marketing

The evidence here is unequivocal. Children are less able than adults to identify paid-for content, whether in the form of native advertising, promoted search results, campaign material, or otherwise.[22] Behavioural advertising has a significant impact on children's perceptions and behaviour, exposing their developmental vulnerabilities and threatening both their freedom of thought under Article 14 of the UNCRC and their right to form and preserve their identity under Article 8.[23] Children are more vulnerable and susceptible to 'pressure to purchase', either through prompts to make in-app purchases or games based on 'pay to win' features.[24]

We do not say that children of all ages should never be exposed to all advertising, but if such advertising continues to be 'highly opaque', 'murky', and even 'fraudulent' (as stated in evidence to the House of Lords Communications Committee last year[25]), the presumption must be that children are protected from it. This includes nudges that encourage children to make purchases (common to many online games), as we cover in the section on 'nudge' techniques.

The Advertising Standards Authority (ASA) currently regulates some aspects of online behavioural advertising but it does not cover all aspects, does not always provide child-specific advice, and it does not cover children up to the age of 18.

The Code should make clear that unless there is a compelling reason to do so - having regard to the best interests of the child and their stage of development - online services must not profile children for the purpose of targeting them with advertising or marketing.
In the US, an amendment to the US Child Online Privacy Protection ACT (COPPA) along these lines has been introduced in the Senate. More details can be found here: https://www.congress.gov/bill/116th-congress/senate-bill/748/text#toc-id8c90b4c35e854e93a8614ca6e970fecd. The Code could usefully align with the approach offered here.

We recommend:

- The Code should prevent online services from profiling children unless there is a compelling reason to do so, having regard to the best interests of the child
- Where profiling is deemed to be in the best interest of the child, the Code should make clear that its intention is to prevent online services from profiling children either in more detail than is necessary to provide them with the service or feature they are actively and knowingly engaged with, or for purposes that are not necessary to provide that service or feature.

12. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

This is a ground-breaking provision, and as far as we are aware, the first time anywhere in the world regulation has sought to address the manipulation of online users through nudge techniques and persuasive design. We are pleased that the ICO has recognised, and moved to prohibit, the widespread practice of online services using nudge techniques to 'lead children to lie about their age'.

Examples of nudge techniques
Nudge techniques are ubiquitous. Some are relatively benign and some deliberately encourage children to make decisions that are not in their best interests. Collectively the culture of nudge (and sludge, which makes good decisions inconvenient) makes the digital environment a manipulative one for a child. The Code need not set out an exhaustive list, but it would be useful for the Commissioner to set out her expectations in more detail. Providers of online services must be clear that the 'addictive capabilities' sited by the UK Chief Medical Officers,[26] the persuasive design features identified by industry insiders such as Facebook co-founder Sean Parker,[27] former Google Design Ethicist Tristan Harris,[28] the inventors of the 'like' button and 'pull-to-refresh' mechanism respectively, Justin Rosenstein and Loren Brichter,[29] Virtual Reality pioneer Jarod Lanier,[30] and all the nudge techniques covered in the 5Rights report *Disrupted Childhood*[31] are covered by the Code.

This includes strategies to extend user engagement (such as auto-play features and timed notifications) and nudges that may encourage risky behaviours, both of which should be clearly tied to the section on detrimental use of data. These extended use strategies are fundamentally incompatible with the principles of fairness and data minimisation under Article 5(1) of GDPR, as well as a range of children's rights under the UNCRC.

The Commissioner should future proof the Code and make clear that it covers prompts and nudges from wearable technology, voice-based devices, and other non-screen versions of nudge.

Nudge (and sludge) techniques in online gaming

Online games, just like other online services, collect huge amounts of data on their users – which increasingly includes messages, voice recordings, and video footage as gaming becomes more interactive. The techniques games use to maximise this data capture, and to ensure that children are giving up as much of it as possible, need to be explicitly covered by the Code.

For instance, many popular games, including Fortnite, fail to allow players to save progress or pause, meaning that children feel compelled to stay and finish even if they need or want to stop. 'Loot boxes', which allow players to purchase a randomised and hidden selection of virtual items, drive compulsive use, as well as being financially exploitative. The player (child) spending the money often has no way of determining what the pay-out will be, so 'loot boxes' have been described as gambling for kids. Adam Cox, a clinical hypnotherapist specialising in addiction, says that 'The freemium model where the game is free but then you pay for extras is putting the emphasis on game developers to make them incredibly addictive and meet psychological needs such as significance and connection, to incentivise players to spend money and time on these games.'[32]

Privacy researchers have also found that companies process players' data to determine who is more likely to spend money on a game. According to the study, 'a player's psychographic information can be used to…dynamically adjust a game's difficulty or mechanics to keep players engaged (and spending money).' The researchers also note that 'it is increasingly common for data to be used outside the game world and shared with third parties', something that has 'a high likelihood of surprising players and violating their trust.'[33]

In sum, children are at significant risk of exploitation by the online gaming. The use of their data to drive compulsive use or pressure into making purchases is entirely inappropriate and must be expressly covered by the Code.

Intention and impact of the nudge rather than the nudge itself

It is important to avoid the misconception that the Code seeks to prohibit the use of specific design features by online services. Whilst some design features may be judged inappropriate for children in every circumstance (loot boxes being one possible example), the majority of features that can be deployed negatively can also be deployed positively – or neutrally. For example, a pop-up or push notification reminding a child to take a break would not fall foul of the Code in the way that a pop-up or push notification might if it encouraged a child to make an in-app purchase. Clarifying that it is the intent and impact of the 'nudge technique' that the Commissioner will consider, rather than the nudge technique itself, is crucial.[iv]

We recommend:

- The Code should clarify that it is the intent and impact of the nudge technique that it is important, rather than the nudge technique itself.

[iv] Not least given the headlines that greeted the draft Code's publication, including 'Facebook and Instagram may have to remove "Like" buttons to protect UK children'.

- The Code should provide more concrete examples of what constitutes a nudge technique. Useful examples would include techniques used in online gaming to encourage extended use, payment, or the sharing of more data. Techniques that seek to 'punish' inactivity, such as personalised and timed notifications, should also be included.
- The Code should require online services to set out what nudge and sludge techniques it intends to use, what the intention of those techniques is, and whether they are in the best interests of the child.
- The Code should provide strict limits on online games offering 'loot boxes' and/or other gambling-related or coercive in-game, in app purchases.
- All games played by children must provide them with opportunities to disengage without suffering significant disadvantage in the context of the game.
- All online services should offer children periodic and meaningful opportunities to disengage.
- Auto-play must be off by default, and when switched on, revert to off when a child navigates away.

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this code.

The Code is ground-breaking in its efforts to bring connected devices and the Internet of Things (IoT) under regulation. Rapid growth in the market for these devices will continue, and it is vital that regulation seeks to protect children in all connected environments just as it must protect them when using more traditional, screen-based technologies.

We note that the Government recently announced a consultation on proposals to ensure that connected devices are properly secure, and we welcome the acknowledgement of Digital Minister Margot James that security must be 'built-in from the design stage and not bolted on as an afterthought'.[34] This is also true of privacy, particularly where children are concerned. There may be a need for the Code to evolve in light of both what comes of these proposals and the emergence of new technologies, but the Code will be a useful (and more immediate) driver of good practice in this area and is much anticipated around the world.

Clarity on definition of connected devices
The Code could usefully include a definition of connected devices, and reasons why certain devices may be in scope and others not. Without a definition, some providers may be unsure if the Code applies to them. It would seem sensible to align the definition in the Code with the definition that will be used by the Government in bringing forward its IoT proposals.

Communicating information
We welcome the Code's stipulation that connected devices find ways to communicate 'just in time' information clearly, and believe this requirement should be extended to the communication of all information, 'just in time' or not'. The absence of a screen-based interface should not give rise to a lack of transparency or failure to uphold other provisions in this Code.

Passive collection of data
We support the Code's effort to restrict the passive collection of data by connected devices, but the expectation should be that 'processing' as well as simple 'collection' will be limited here. If a device needs to collect a small amount of data to function, whether in listening or stand-by mode, restrictions on the use and storage of that data must be made clear. The data minimisation, purpose limitation, and storage limitation principles are important to cross reference here.

Security of connected devices

The security of connected devices is vital, given the sensitive and intimate data they often process. Multiple reports in recent years have warned of insufficient security protections of devices and toys used by children. In 2018, for instance, researchers discovered that a location tracking smartwatch, worn by thousands of children, could be hacked 'with ease', allowing anyone to track their movements.[35]

Article 32 of the GDPR requires providers of online services to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' of their data processing. The Code should make reference to this and make clear that, where children are concerned, the risk is high and the security of devices must be similarly so.

We recommend:

- The Code should provide a clear and robust definition of connected devices
- The Code should make clear that a lack of a screen-based interface is no excuse for a lack of transparency for child users, or to fall short of upholding the other provisions in this Code
- The Code should provide greater clarity about its expectation that connected devices do not collect and process children's data 'passively', or when they are not actively and knowingly engaged with the service
- The Code should provide more detail on its requirements vis a vis the security of connected devices, in line with Article 32 of GDPR.

14. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

Additional tools to support the rights of the child
The Code has a good list of the kind of tools that services ought to provide, but there are a few additions we can suggest, including:

- A 'show me who has seen or accessed my data' tool
- A 'show me the data inferred or derived from my personal data' tool
- A 'show me my "profile"' tool
- A 'show me a simpler version of these terms and conditions' tool
- A 'reset all my settings to default' tool
- A 'show me what geolocation data you have collected on me' tool
- An 'opt out of all advertising and marketing' tool
- An 'only store this data for X period of time' tool

15. Data protection impact assessments: Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

This section is comprehensive and helpful. Asking questions that support the autonomy and rights of children in advance and systematically designing them in, is the greatest hope of making a digital world one in which a child can flourish. A comprehensive DPIA is the very best way of implementing data protection by design, and a good way for companies to demonstrate compliance with it. We particularly welcome the proportionate approach set out in 'step 6', which encourages service providers to identify and assess the level of any risks, and to implement protections, including age verification mechanisms, that are commensurate with those risks.

We recommend:

- As recommended elsewhere, the Code should require online services to include in their DPIAs the steps they have taken to cater for children with specific vulnerabilities or needs.

16. Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code.

We support the breadth and intention of this provision, and note that when we or the children we work with talk to developers and engineers, the developers and engineers say - almost without exception - "I never thought about it that way". If the code can institutionalise consideration of children and their needs or vulnerabilities as a norm, it will go a long way towards driving good design and corporate accountability.

Transition period

We acknowledge that different provisions of the Code may require different periods of time to implement. We also note that online services should already be complying with many of the Code's requirements as part of their existing obligations under the GDPR. We recommend that the Information Commissioner to make the transition period(s) as short as is practicable, bearing in mind the urgency of the Code's provisions and the length of time that has already passed since the Data Protection Act 2018.

---

[1] One in Three: Internet Governance and Children's Rights, S. Livingstone, et al, Unicef, January 2016
[2] Regulatory Action Policy, ICO, 2018
[3] Data Ethics: The New Competitive Advantage, Guy Hasselbalch and Pernille Tranberg, 2016
[4] Elizabeth Denham CBE, House of Commons Select Committee on Digital, Culture, Media, and Sport, April 2019
[5] How big data is disrupting the gaming industry, Kevin Rands, CIO, 2018
[6] E.g. see Vulnerable Children in a Digital World, Adrienne Katz and Dr Aiman El Asam (Internet Matters), 2019
[7] The Ofcom Broadcasting Code, Ofcom, January 2019
[8] Conditions of Use, Amazon, October 2018
[9] Privacy Statement, Netflix, April 2019
[10] Safety Net: Cyberbullying's impact on young people's mental health, The Children's Society and Young Minds, 2018
[11] Snapchat's evidence to the Digital, Culture, Media, and Sport Committee's inquiry on Immersive and addictive technologies, March 2019
[12] Private traits and attributes are predictable from digital records of human behaviour, M. Kosinski, et al, PNAS, 2013
[13] Unfair contract terms: CMA37, Competition and Markets Authority, 2015
[14] Online Harms White Paper, UK Government, April 2019
[15] The OFT's Principles for online and app-based games, OFT1519, Office of Fair Trading, 2014
[16] During Mark Zuckerberg's appearance before the Senate's Commerce and Judiciary Committee, it was noted that Facebook allows for high privacy settings, but the user "really has to work at it."
[17] Deceived by Design, Norwegian Consumer Council. 2018
[18] 2017 GPEN Sweep Report, Online Educational Services, Information and Privacy Commissioner of Ontario, October 2017
[19] Control, Alt, Delete, Which? 2018
[20] Horizon Digital Economy Research Institute response to the Information Commissioner, September 2018
[21] Location History, Facebook, 2019
[22] Children and Parents: Media Use and Attitudes Report, Ofcom, November 2017

[23] Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, European Commission, March 2016
[24] Principles for online and app-based games, Office of Fair Trading
[25] Oral and written evidence, UK Advertising in a Digital Age, House of Lords Select Committee on Communications, April 2018
[26] Commentary on 'Screen-based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews', UK Chief Medical Officers, 2019
[27] Sean Parker unloads on Facebook: 'God only knows what it's doing to our children's brains', M Allen, Axios, November 2017
[28] Truth about Tech: A Road Map for Kids' Digital Well-Being, Common Sense Media, Center for Humane Technology, February 2018
[29] 'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia', the Guardian, October 2017
[30] Jarod Lanier on fighting Big Tech's "manipulation engine", Financial Times, July 2018
[31] Disrupted Childhood: the cost of persuasive design, 5Rights, June 2018
[32] NHS to launch first internet addiction clinic, The Guardian, 22 June 2018
[33] Press start to track? Privacy and the new questions posed by modern videogame technology, J. Newman, et al, 2014
[34] Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, DCMS, April 2019
[35] MiSafes' child-tracking smartwatches are 'easy to hack', BBC, November 2018

Appendix 1

FAQs

"Does the Code risk undermining data processing that is positive for children?"

The first provision of the Code states unequivocally that the best interests of the child should be a primary consideration in the design of services and the handling of children's data. Moreover, throughout the Code the Information Commissioner permits services to deviate from the rules where they can demonstrate a compelling reason to do so, if it is in the child's best interests. This prevents an unintended consequence from arising and allows any service to act in a way that is genuinely and demonstrably in the best interests of a child.

"Will the Code hamper innovation?"

Implicit to the Code is the recognition that technology and the internet play a hugely important role in children's lives. Far from wanting to undermine innovation, the Code's ambition is to promote innovation that anticipates the needs and upholds the rights of children.

Additionally, it is disingenuous to suggest that innovation and data protection are mutually exclusive. There is a widely-held view that introducing new standards to which all companies must adhere will allow different business models and design approaches to create a more diverse and competitive sector, with new players entering the market forewarned of its rules. In fact, a company's approach to data ethics has become an important competitive differentiator.[36]

Indeed, Sir Tim Berners-Lee,[37] Tristan Harris,[38] Senator Mark Warner,[39] US Financial Conduct Authority (FCA),[40] Farhad Manjoo,[41] House of Lords Communications Committee,[42] George Soros,[43] Foursquare co-founder, Naveen Selvadurai and former Facebook employee, Josh Lee,[44] believe that innovation is hampered by having only a few dominant players.

In the case that there is *genuine* conflict between innovation and data protection or child safety, there is no question that the best interests of the child must come first. Online services used by children must offer a high bar of data protection for children – it is the price of doing business.

"Will the Code have a negative impact on the rights of adults?"

Different rights must always be balanced with one another, and the rights of one group must often be balanced with the rights of another group. The Code correctly asserts that it is up to online services to ensure that they are age-appropriate for their child users, but it also allows online services to determine how best to do that whilst also promoting the freedoms and user experience of adults.

It is not reasonable, however, to suggest (as some seem to) that the rights of adult users must never be encroached upon – not by an inch – even if the cost is failure to uphold the rights of a child. Children and adults live together in all other environments, and as such many adult behaviours are restricted in respect of children (e.g. smoking in cars, providing ID at a nightclub, even taking children out of school for holidays in term time). The implication that these are intolerable encroachments on the rights of an adult to smoke in a car, enter a nightclub, or go on holiday when

they wish is dismissed by society's broad insistence that we make specific arrangements for children. This should clearly be no different in an online context.

The Code does take care not to adversely affect the online experience of adults, but catering for the specific needs and vulnerabilities of children is non-negotiable.

In relation to privacy specifically we are clear that the status quo represents the more significant threat to privacy. Identify fraud based on publicly available information about children will affect 7.4 million individuals by 2030,[45] Facebook can predict someone's undisclosed sexuality with 88% accuracy,[46] and 70% of employers analyse a young person's social media activity during the hiring process.[47] Many adults would welcome the privacy protections that the Code affords.

"Isn't it the responsibility of parents to keep their children safe online?"

Parents and carers are often the first line of support for any child, but we all have a duty to consider how our actions impact on the rights and safety of children; whether or not they are our own. In the UK, we are signatories to the UNCRC, and we make special arrangements for children in all areas of life; from education, criminal justice, health, media, etc. Online services have consistently failed to fulfil either the implicit or explicit duties they have to children, which has significantly undermined the ability of parents or carers to keep their children safe and promote their wellbeing. The Code therefore supports parents and carers by creating an environment that is designed with children in mind, transferring to the online world the protections that children have long enjoyed in the offline world. The Code does not replace the need for the engagement and wisdom of parents or carers in a child's online life.

"The age-verification provision is technically burdensome."

This is answered in our comments under the age-appropriate application section.

"Won't age verification be easy to circumvent?"

In the offline world children have been known to use 'fake IDs' to gain access to bars or to ask adults to purchase age-restricted products for them in shops. The fact that these 'workarounds' exist does not mean that asking for proof of age is pointless, and does not detract from the duty of online services – or bookmakers, nightclubs, supermarkets and cinemas – to ensure that the age-checks they have in place are as robust as possible nonetheless.

An 'expectation of challenge' is an important social norm and whilst children will always transgress and experiment, the setting of boundaries is crucial to their development and safety. In other words, an age gateway need not be 100% effective 100% of the time for it to have a positive impact. Rather, it must – at a minimum – 'exclude the possibility for someone to simply side-step its requirements',[48] which is something that the self-declaration mechanisms of many online services currently fail to do. This 'expectation of challenge' exists in the real world (bouncers do not simply ask for a person's age and accept uncritically their answer), and it should exist online too.

"What positive impact will the Code have on children?"

The Code will end the practice of online services routinely failing to establish which of their users are children, and therefore routinely failing to provide children and their data with the specific protection they merit.

Taken together, the Code's 16 provisions will address a range of concerns that have been voiced repeatedly by child's rights experts, academics, health professionals, and law enforcement; not to mention parents, carers and children themselves.

For instance, many platforms and services have minimum joining ages of 13 or 16, yet 61% of UK children have a social media profile by age 12.[49] Researchers at Berkeley in the US found nearly 3,000 children's apps in the Apple store that deliberately mislabelled themselves as 'not primarily directed to children' so that they could track users and target them with ads.[50] The UK's Chief Medical Officers have called for a curb on the 'addictive capabilities' of online services,[51] following the formal classification of internet and gaming addiction as a mental disorder by the World Health Organisation.[52] The National Crime Agency[53] and police forces[54] up and down the country have issued warnings that services collecting geolocation data could be used to stalk, bully, abuse or sexually exploit children. The FBI warned last year that interactive dolls, which record footage of children as they play with them, are easily hacked and may then be used to generate child sexual abuse material.[55] After the suicide of Molly Russell, it emerged that a contributing factor to her death was the loops of graphic content promoting self-harm and suicide that she had been viewing on Instagram.[56] Importantly, rather than Molly having to seek this content out herself, it was being continually recommended to her, based-on data drawn from her viewing and browsing history. These are all problems caused or exacerbated by the misuse and rapacious pursuit of children's data.

"Most people are happy to trade their data so they can use services for free"

First and foremost, the Code does not say that online services cannot collect children's data, nor does it say that this data can never be used for commercial purposes. Rather, it demands that the best interests of the child are a primary consideration in decisions regarding their data, in a way that they haven't been to date.

In any case, the idea that people are happy to give up their data is flawed:

- polling consistently demonstrates that people are uncomfortable about sharing their data with private companies (with social media companies ranking the lowest in terms of trust), [57] or don't even appreciate that this is happening. Which? found that "consumers tend to operate with an incomplete picture of data sharing and third parties, which means that most are surprised to learn about the extent of the data sharing ecosystem."[58]
- The terms and conditions, community guidelines and privacy notices that set out the rules of this 'free-for-data' exchange are routinely flouted by the online services. As the Code makes clear, it is difficult to see how the exchange can be considered 'fair' in this context.
- Children are often incapable of appreciating the many ways that they can be impacted by giving consent for their data to be collected and used, and – in any case – the terms and conditions of many online services require a university level education to understand. This puts their consent on shaky ground from the outset, even without the 'nudge techniques' that services use to manipulate children into decisions that favour data capture.
- Even if children were able to provide meaningful consent, the data practices they'd be consenting to might still be inappropriate given their age and stage of development. The evidence is clear that children lack the 'cognitive defences' to identify paid-for or promotional content,[59] and behavioural advertising significantly impacts on children's perceptions/behaviour when they are still developing.[60]
- An individual's right to privacy is now increasingly contingent on the choices of others, who are free to share information about you online with limited constraints. Facebook's 'People You May Know' feature is a good example – as one spokesperson put it: 'suggestions may be

based on contact information we receive from people and their friends. Sometimes this means that a friend or someone you know might upload contact information – like an email address or phone number – that we associate with you.'[61]

---

[36] Data Ethics: The New Competitive Advantage, Guy Hasselbalch and Pernille Tranberg, 2016
[37] World Wide Web Foundation
[38] Tristan Harris Essays
[39] Potential Policy Proposals for Regulation of Social Media and Technology Firms, U.S. Senator Mark Warner, 30 July 2018
[40] The Big Tech Competition Dilemma, Financial Conduct Authority, 1 November 2018
[41] How the Frightful Five Put Start-Ups in a Lose-Lose Situation, New York Times, 18 October 2017
[42] UK Advertising in a Digital Age, House of Lords Select Committee on Communications, 11 April 2018
[43] Remarks Delivered at the World Economic Forum, 25 January 2018
[44] Will Facebook Kill All Future Facebooks? WIRED, 25 October 2017
[45] 'Sharenting' puts young at risk of online fraud, BBC, 2018
[46] Private traits and attributes are predictable from digital records of human behaviour, Kosinki et al, 2013
[47] CareerBuilder, 2018
[48] *Ibid.*
[49] Safety Net: Cyberbullying's impact on young people's mental health, Children's Society and Young Minds, 2018
[50] 'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale, Reyes et al, 2018
[51] UK Chief Medical Officers' commentary on 'Screen-based activities and children and young people's mental health and psychological wellbeing: a systematic map of reviews', 2019
[52] WHO calls gaming disorder and mental health condition, WebMD, 2018
[53] Snapchat's new map feature sparks privacy row and fears it could put children at risk, Evening Standard, 2017
[54] Police issue child safety warning over Snapchat maps update that reveals users' locations, The Telegraph, 2017
[55] Hello Barbie, hello hackers: accessing personal data will be child's play, Australian National University, 2015
[56] Instagram 'helped kill my daughter', BBC, 2019
[57] British consumer attitudes to sharing personal data, Open Data Institute, 2018
[58] Control, Alt, Delete, Which? 2018
[59] Children and Parents: Media Use and Attitudes Report, Ofcom, November 2017
[60] Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, European Commission, March 2016
[61] How Facebook Figures Out Everyone You've Ever Met, Gizmodo, 2017