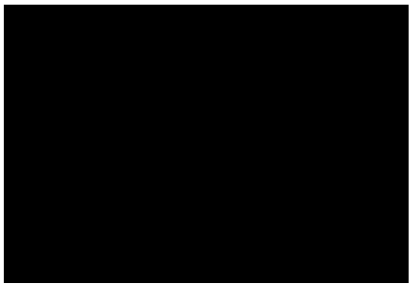
Information Commissioner's Office

Call for evidence:

Age Appropriate Design Code

Evidence from Human Centred Computing Group
Department of Computer Science, University of Oxford

18 September 2018



ico.
Information Commissioner's Office

Introduction

The Information Commissioner (the Commissioner) is calling for evidence and views on the Age Appropriate Design Code (the Code).

The Code is a requirement of the Data Protection Act 2018 (the Act). The Act supports and supplements the implementation of the EU General Data Protection Regulation (the GDPR).

The Code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet. Once it has been published, the Commissioner will be required to take account of any provisions of the Code she considers to be relevant when exercising her regulatory functions. The courts and tribunals will also be required to take account of any provisions they consider to be relevant in proceedings brought before them. The Code may be submitted as evidence in court proceedings.

Further guidance on how the GDPR applies to children's personal data can be found in our guidance Children and the GDPR. It will be useful to read this before responding to the call for evidence, to understand what is already required by the GDPR and what the ICO currently recommends as best practice. In drafting the Code the ICO may consider suggestions that reinforce the specific requirements of the GDPR, or its overarching requirement that children merit special protection, but will disregard any suggestions that fall below this standard.

The Commissioner will be responsible for drafting the Code. The Act provides that the Commissioner must consult with relevant stakeholders when preparing the Code, and submit it to the Secretary of State for Parliamentary approval within 18 months of 25 May 2018. She will publish the Code once it has been approved by Parliament.

This call for evidence is the first stage of the consultation process. The Commissioner seeks evidence and views on the development stages of childhood and age-appropriate design standards for ISS. The Commissioner is particularly interested in evidence based submissions provided by: bodies representing the views of children or parents; child development experts; providers of online services likely to be accessed by children, and trade associations representing such providers. She appreciates that different stakeholders will have different and particular areas of expertise. The Commissioner welcomes responses that are limited to specific areas of interest or expertise and only address questions within these areas, as well as those that address every question asked. She is not seeking submissions from individual children or parents in this call for evidence as she intends to engage with these stakeholder groups via other dedicated and specifically tailored means.

The Commissioner will use the evidence gathered to inform further work in developing the content of the Code.

The scope of the Code

The Act affords the Commissioner discretion to set such standards of age appropriate design as she considers to be desirable, having

regard to the best interests of children, and to provide such guidance as she considers appropriate.

In exercising this discretion the Act requires the Commissioner to have regard to the fact that children have different needs at different ages, and to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

During Parliamentary debate the Government committed to supporting the Commissioner in her development of the Code by providing her with a list of 'minimum standards to be taken into account when designing it.' The Commissioner will have regard to this list both in this call for evidence, and when exercising her discretion to develop such standards as she considers to be desirable.

In developing the Code the Commissioner will also take into account that the scope and purpose of the Act, and her role in this respect, is limited to making provision for the processing of personal data.

Responses to this call for evidence must be submitted by 19 September 2018. You can submit your response in one of the following ways:

Online:
Download this document and email to:
childrenandtheGDPR@ICO.org.uk

Print off this document and post to:
Age Appropriate Design Code call for evidence
Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the call for evidence please telephone 0303 123 1113 and ask to speak to the Engagement Department about the Age Appropriate Design Code or email childrenandtheGDPR@ICO.org.uk

Privacy statement

For this call for evidence we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our privacy notice.

Section 1: Your views and evidence

Please provide us with your views and evidence in the following areas:

Development needs of children at different ages
The Act requires the Commissioner to take account of the development needs of children at different ages when drafting the Code.

The Commissioner proposes to use the age ranges set out in the report Digital Childhood – addressing childhood development milestones in the Digital Environment as a starting point in this respect. This report draws upon a number of sources including findings of the United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group in its literature review of Children's online activities risks and safety.

The proposed age ranges are as follows:

3-5
6-9
10-12
13-15
16-17

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be (delete as appropriate):

~~Not at all appropriate~~
~~Not really appropriate~~
Quite appropriate
~~Very appropriate~~

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services),

These age brackets are *quite* appropriate as they seem to take into account transitionary points in learning and childhood development. We can see from our own work with children that such a multi-segmented approach is required as children develop. The perspectives of young people can vary significantly between age ranges: for example, a young person aged 13 is likely to engage with materials differently from a young person aged 16, even though there are only three years between them.

Even though we support this age segmentation, we suggest that further work and investigation should be done to determine the precise sub-boundaries of age.

Our work on the project UnBias,[1] where we engaged extensively with young people (>13) through workshops and youth juries, shows that even within age groups, other demographic variables, such as the background of a child, the school they go to, etc., can also play a part in determining how well they are able to grasp and understand different issues related to their privacy and safety online. This means that these age segmentations may not be sufficient when deciding how to demarcate young people and setting design standards accordingly (this comment also has implications for question 2, and for our other comments which discuss differences between age ranges).

Q2. Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age brackets.
The precise age brackets to be used will need to be refined from empirical evidence. Presently, we do not have enough evidence to differentiate more specifically, so it is better to start by building on the age ranges suggested; it is important to take children's development stages into account.

It is also important to account for the fast pace of technological change. The experiences of, for example, ten-year-old children today differ from those of ten-year olds five years ago.

There also does not seem to be any mention of children below the age of 3, yet we know that very young children are also exposed to ISS and there may even be services targeted at them.

Our views expressed below are mainly thanks to [redacted] of the ORBIT Project (which we discuss later in our evidence to Q5E).[2]

3-5: At this age children are becoming more socialised and gaining the confidence to reach out and explore their world more, make independent

---

[1] UnBias: Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy
September 2016 – November 2018
Funded by Engineering and Physical Sciences Research Council (EPSRC) under the Trust, Identity, Privacy and Security (TIPS) call, Project Reference EP/N02785X/1
https://unbias.wp.horizon.ac.uk/
Note that our colleagues on the UnBias project from the Horizon Digital Economy Research Institute will be making a separate submission of evidence. This does not, of course, reflect any disagreement.

[2] https://www.orbit-rri.org/about-rri/ (accessed 18/09/2018)

friendships and develop social and empathic intelligence. However, this is also the age at which social disparities start to be seen - for example, children who come from literate households often begin to attend nursery school with larger vocabularies than those who come from families that may be time- and resource-poor, with knock-on effects in terms of interaction and attention. It is possible that ISS for this latter group and for other disadvantaged groups may be able to offer resources that could narrow the gap. Children at this age cannot keep themselves safe online.

6-9: During key stages 1 and 2, children are expanding their networks of friends and starting to experience themselves as individuals in the world. There is enormous growth in understanding during this period. They are moving from a 'believe everything' stage, to a stage where they begin to question what they are told. This is the ideal point at which to introduce concepts like information literacy, law and ethics. ISS at this point - as well as supporting basic learning blocks like maths - could provide a broader range of options than is available in the classroom. Children at this age are unlikely to be able to keep themselves safe online.

Below this age/stage children do not have a grasp of how the Internet differs from television and should not be deemed able to accept terms and conditions about gathering of data/use of personal information.

The United Nations Convention on the Rights of the Child
The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.

Q3. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services)

By requiring the Commissioner to take account of the UN CRC, it is clear that, from Article 3 of the Convention, "the best interests of the child shall be a primary consideration".

Aspects of design

The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code.

These are as follows:

- **default privacy settings,**
- **data minimisation standards,**
- **the presentation and language of terms and conditions and privacy notices,**

- **uses of geolocation technology,**
- **automated and semi-automated profiling,**
- transparency of paid-for activity such as product placement and marketing,
- **the sharing and resale of data,**
- **the strategies used to encourage extended user engagement,**
- **user reporting and resolution processes and systems,**
- **the ability to understand and activate a child's right to erasure, rectification and restriction,**
- the ability to access advice from independent, specialist advocates on all data rights, and
- any other aspect of design that the commissioner considers relevant.

(We have bolded the areas to which we have made contributions in this response).

Q4. Please provide any views or evidence you think the Commissioner should take into account when explaining the meaning and coverage of these terms in the code.

Overall, applying to all areas of the code

The code should emphasise that responsibility lies primarily with developers and regulators. Children (or their parents[3]) should not be expected to take all the responsibility for keeping safe by changing privacy settings, turning off geolocation, or in other ways. This is why we argue for the highest protection levels by default. It should not be up to children to assess whether a platform they are using is or is not adequate in terms of data protection and other privacy and online safety dimensions. This is the responsibility of the regulator, and of developers following regulation design practices.

It is important to emphasise that the Code applies to all ISS "likely to be accessed by children", not only those aimed directly at children. The NSPCC's NetAware guide has identified ISS most used by children. Many of these services (Facebook, Instagram, Reddit …) are not child-specific and, in fact, mostly do not allow children below the age of 13 to join - although this is widely circumvented – as evidence from our project UnBias demonstrates.

A further cross-cutting consideration is that different design standards will be appropriate for children at different development stages. This might seem obvious, but a cut-off age of 13, for example, below which nothing is allowed and above which nothing is prevented, may not allow for children to grow up safely in the digital environment (see also our responses to Q2 above).

---

[3] In using the term "parents" we also include guardians, carers and others "*in loco parentis*"

Equally, our comments focus on children (<18). There are clearly other vulnerable groups in relation to ISS, but we feel it is important for this Design Code to focus on children and young adults.

Children should be seen as active users of the online space whose rights can be as affected as much as any other group; there should be mechanisms to give them a voice.

Multi-stakeholder evidence from the UnBias project shows that there is a challenge arising from the proprietary nature of some aspects of what providers of ISS develop, and the maintenance of their competitive edge. It is important to ensure that ISS providers adhere to regulation in the spirit of the best achievable standards, rather than superficially. There is a danger here that service providers may appear to be adhering to regulation while shortcomings may "slip under the radar". Mechanisms to uphold regulation effectively will be required, and also to take into account potentially conflicting areas such as competition law.

The Code must be backed by a firm commitment from government. ISS providers must be incentivised by robust and effective enforcement of the Code, supported by sufficient expertise and resources made available to the ICO.

Default privacy settings
Privacy settings refer not only to the ways in which a child's personal data can be accessed by the ISS provider, but also to the ways in which it can be collected, stored, passed on to other companies, and processed.

Every ISS has a set of default privacy settings which applies from the moment that the user signs up, unless they take action to change them (if they are allowed to change them by the service).

Personal data is very extensive, including not only basic attributes such as name, address, age, but also hobbies, preferences, habits, fitness level and many more, building up to a detailed profile, so that an ISS might "know" a child better (although in different ways) than their own family and friends.

Data Minimisation
The data protection principles in GDPR Article 5 require that collection of personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" and must not be further processed in a manner inconsistent with those processes.

Presentation and language of terms and conditions and privacy notices
Data protection policies are often contained in terms and conditions (T&Cs), and therefore it is important to make these clear, short, explicit, and easy to understand (as we discuss below in our response to Q5A).

Use of geolocation
The capability for geolocation – the collection and storage of location data either by the ISS or an online intermediary, or locally on the device - using accurate GPS is almost universally built into mobile phones and often for tablets. In addition, location can be found using techniques such as triangulation with nearby cell antennae. Even for laptops and non-mobile computers, location information can be inferred from Internet Protocol (IP) address or WiFi positioning.

Geolocation has privacy implications when location data is collected and/or stored by service providers (as it often is).

Geolocation is necessary for some ISS, such as navigation (but not always simply to display a map), delivery tracking, transport information, and some games. However, geolocation is widely used in situations where it is not directly necessary for the *child's needs*, such as for profiling or location-related advertising.

Automated and semi-automated profiling
Automated profiling is related to data minimisation, because the collection of voluminous and heterogeneous data enables detailed profiling of children at ages when they may be particularly vulnerable to outside influences.

However, even when personal data collection is *"limited to what is necessary in relation to the purposes for which they are processed"*, the large amount of data combined with advances in machine learning allows a child's personality and interests to be determined and potentially manipulated.

The sharing and resale of data
It is important to note the many kinds of data and of data sharing. Data may be shared as specific data items or as part of a large single or agglomerated dataset. Data can be shared within a company, shared by a large group of companies, or sold to other parties.

Strategies used to encourage extended user engagement
"Free" services are often based on a business model of commoditising personal data or selling views to advertisers. Such services often deliberately include design features which are called "sticky", "reward loops", "captology" and "enrapture" to encourage extended use. Sounds,

notifications, auto-suggested content, counts of "Likes" and retweets, etc., are designed to keep the user engaged.

The ability to understand and activate a child's right to erasure, rectification and restriction
All data subjects, adults and children, are entitled to bring complaints or legal proceedings against a data controller or processor if they suspect non-compliance. Everyone has basic rights to retract, rectify and erase personal information (or social media posting etc.). However, it is important for these rights to be supported by systems which actually allow users to benefit from them.

Q5. Please provide any views or evidence you have on the following:

Q5A. about the **opportunities and challenges** you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas.

Default privacy settings
A challenge in setting design standards for privacy is that concepts of privacy are inconsistent, with different ages for protection of identity, different ages at which children are allowed to join various platforms (typically 13, according to the ISS providers' own rules), and inconsistently applied.

Children's understanding of privacy may not be as developed as adults and may also be influenced by culture. However, many people of all ages fail to understand that the apparently private spaces of online worlds are routinely collecting and sharing large amounts of data. Personal data is kept for a very long time, so that posts made by a person at a young age can come to light and negatively impact their future many years later.

Our project Digital Wildfire[4] demonstrated the importance of teaching children about the long-term implications that the posting of content on social media can have. In this project, teachers informed us that children often do not take a long-term view and do not see themselves as vulnerable to harm. A possible exception may be children who have had negative online experiences directly or applying to someone that they know.

The UnBias project also found that in many instances, as well as lack of awareness, it was difficult to get many young people to take a pro-active

[4] Digital Wildfire: (Mis)information flows, propagation and responsible governance
November 2014 - November 2016
Funded by Economic and Social Research Council as part of Research Councils UK "Global Uncertainties" programme, Project Reference ES/L013398/1
http://www.digitalwildfire.org/

interest in the consequences of data collection. This is particularly as the data collection and further processing of their data may seem abstract and, therefore, inconsequential to them on a personal level.

A challenge, which underscores the importance of the Code, will be to help young people understand their rights, and to engage seriously with the problematic issues that are related to data collection. An opportunity regarding the development of the code will be to raise awareness amongst young people and do more work to close this *abstraction gap*.

The Digital Wildfire project also showed us that children are able to reproduce the online safety messages they are taught, but also have a very personal interpretation and understanding of their online experience. This means that they can sometimes appear to breach online safety rules even though they are aware of them. To young people this does not necessarily seem a breach because they have their own understanding of their choices and behaviours, and in that context feel that they are being reasonable.

To address this, there is a need to gather evidence directly from children to understand their perceptions rather than attempting to make interpretations on their behalf.

A general point about "privacy" is that it is a very contested term and therefore can easily lose its meaning; for example, ISS providers routinely claiming to "take privacy seriously" as a shibboleth. Terms such as data management and protection are more concrete - whilst also being constitutive elements of privacy - and can be easier to act and reach agreement on. The Code should use specific, concrete language rather than general terms, to avoid ambiguity.

Data Minimisation

A challenge in ensuring minimisation of data is that the scale of data collection is often not apparent to children (or their parents). As well as data which is, to a greater or lesser extent, shared explicitly – sign-ups, customer service interactions, purchases/transactions, chatting, commenting or liking, searching, sharing, questionnaires, ..., there are less obvious forms of data sharing which include browsing history, loyalty cards, some email services, and GPS. Children are particularly vulnerable to the collection of new forms of data, such as from cameras (on mobile phones/webcams), microphones, and, especially, the Internet of Things, as we have already noted.

A further challenge is that children inadvertently generate more personal data than adults; for example, children are more likely to access ISS from mobile devices which reveal their geolocation (see our comments on this below). Data on this scale inevitably contains inaccuracies, with

potentially serious life-changing implications. Even in the absence of errors, this highly personal data may lead to inferences which reinforce unfair assumptions and stereotypes – for example, relating to children's mental health or disabilities.

Evidence from the UnBias project shows that generally there was a large disparity between young people's awareness and the actual extent of data collection from the various ISS that they used. Often, young people displayed surprise and shock at the extent of data collected - especially as they were unable to understand why certain data, seemingly unrelated to the function of the ISS, was collected – and, importantly, how it was used.

Re-enforcing our point about differences in background, culture and education even within age ranges, evidence from both the Digital Wildfire and UnBias projects shows that young people can vary a great deal in their knowledge of the above. Whilst some are very knowledgeable, others know very little. Knowledge is often voiced in terms of esafety and protection from harm. Some young people can display understanding of algorithmic processes and rules even if they do not articulate them in technical terms.

This variance is likely due to levels of individual interest as well as variance in what schools and parents are teaching young people. We have engaged with some schools that are very active and confident to teach about these issues – in particular in connection to esafety lessons – whereas other schools are less so.

A further challenge is that, despite data minimisation under GDPR, many of the ISS are provided by very large groups of companies, who are able to share data among themselves, and may interpret acceptance of agreement to share data with one of their companies as agreement to share data widely around the group, for many different purposes.

A particular challenge relates to helping young people to view data collection and use as a long-term issue. Even if they feel that this does not affect them now, there may be detrimental consequences in the future for them personally and/or on a societal level (see also our comments about default privacy settings above).

Another important challenge, which also provides opportunities, is to help young people to feel they are active users online, with opportunities to shape their own online experiences or even to push for wider scale improvements.

Presentation and language of terms and conditions and privacy notices

There is plenty of evidence that children (and adults) do not read T&Cs when signing on to a new service[5]. Indeed, it is unreasonable to expect them to do so when these run to thousands of words and require university-level reading ability.[6]

T&C are almost always non-negotiable, and children, less likely than adults to accept delayed gratification and with a less developed ability to weigh up long-term consequences, are likely to simply click through the "accept" button. This is a large imbalance of power in favour of the ISS provider against the user.

As we noted above in our general comments, many ISS widely used by children are not specifically aimed at children. A challenge is that service providers may claim that this absolves them of any special duty to protect children from collection and use of their personal data; the Code should make clear that this is not the case, and that ISS providers do have a special responsibility towards children users of their services.

T&Cs must be agreed by affirmative action, and, under the DPA 2018, only children aged 13 or over may consent to terms and conditions. Younger children are developmentally unable to give meaningful consent (parents or guardians may give it, however, which assumes a level of parental control). Even older children may fail to appreciate the long-term consequences of the impact on their privacy.

Use of geolocation

Geolocation presents some particular challenges for children's data privacy.

Geolocation can be difficult to turn off and may be operational, gathering data, even when a service or app is not active. Even if privacy settings have been set to restrict location data, some services may turn them back on during an upgrade or when a user logs-off (see our comments on default privacy and user engagement – restrictions should be tight, by default, and remain tight unless explicitly changed by the user).

Embedded data in a photo or story may reveal a child's location. Thus, a user may not be aware that their location data is being gathered. Even if they are aware, many ISS make acceptance of geolocation a condition of use, even when it has no clear benefit for the user.

---

[5] For example, Phillips (2017): *Reading the fine print when buying your genetic self online: direct-to-consumer genetic testing terms and conditions*, New Genetics and Society 36(3) 273-295 http://dx.doi.org/10.1080/14636778.2017.1352468

[6] Wigley + Company Solicitors. (2015): *To read or not to read . . . Online Ts and Cs. Or Hamlet.* http://wigleylaw.com/assets/Uploads/To-read-or-not-to-read.pdf (accessed 18/09/2018).

Geolocation data can enable a service provider to build an extremely detailed picture of a child's habits, adding to their already extensive profile. There are also services available to parents that enable them to track their children's whereabouts. While this may reassure over-protective parents, excessive control may negatively affect the development of a child, as well as being a serious infringement of the child's right to privacy.

Automated and semi-automated profiling
A challenge in design codes around profiling is that, despite the vast volumes of data, profiling is often inaccurate because the data quality is poor or biased. Discussions in the UnBias project have highlighted these issues.

Profiling often perpetuates existing stereotypes: even if obvious labels are avoided, proxy values (such as place of residence) may have discriminatory impact. It is extremely difficult to trace the source of profiled attributes, and difficult to remedy them. The effect may carry forward into a child's adult life and may have life-changing consequences.

The sharing and resale of data
If data is shared around a company or group of companies, or sold (even in "anonymised" form), this may reduce the expected level of data minimisation.

Even if data is anonymised or "pseudonymised", we know from research in information security that it is often possible to identify individuals by combining multiple datasets.[7] Governments are particularly keen storing and sharing of data in the absence of clear goals, "in case" it is useful for some future purpose.[8] This is a particular risk for children, whose data is collected in large amounts, for example by schools and health services.[9]

Strategies used to encourage extended user engagement
"Captology" (persuasive technologies, especially where the aim is to encourage the user to stay online) and related design features are a challenge for age-appropriate design.

---

[7] Ohm, P (2009): *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review 57, pp1701-1777. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/uclalr57&id=1713 (accessed 18/09/2018)
[8] Anderson, R., Brown, I., Dowty, T., Inglesant, P., Heath, W., & Sasse, A. (2009). *Database state*. York: Joseph Rowntree Reform Trust. http://www.jrrt.org.uk/publications/database-state-full-report (accessed 18/09/2018)
[9] A recent example is the Metropolitan Police Gangs Matrix database, in which data is routinely shared between the police and other government agencies. Amnesty International (2018), *Secrecy, stigma, and bias in the Met's Gangs Database*. https://www.amnesty.org.uk/files/reports/Inside%20the%20matrix.pdf (accessed 18/09/2018)

Users of any age can find that they have spent much longer using a service than they wished, but young people are particularly vulnerable because they are less able to self-regulate, while habits which may be hard to break are formed before the age of 9. Children are less able to make informed choices, and may be unaware of the cues that are being used to keep them engaged with a service. ISS are able to play on a child's desire for social acceptance.

Addressing captology is challenging because it is a feature of almost all the ISS which are widely used by children. Because attracting and maintaining an audience is at the core of their business models, ISS providers are likely to resist any restrictions. However, there is also an opportunity, because companies are subject to pressure from shareholders, users and the public.

The ability to understand and activate a child's right to erasure, rectification and restriction

Data protection and the right to retract, erase or rectify data are already legally granted rights, but just because someone has a right to something does not guarantee that they have the power to enact it. Data protection rules are complex. Lacking the resources to investigate and understand their rights, but disproportionately impacted by privacy breaches, children need greater support in accessing their rights.

In the case or retraction or erasure, there is an additional technical challenge that data may be widely shared or propagated, or remain available in an archive such as the WayBack Machine.[10]

As with other privacy implications, children may be affected more than adults because, for example, ill-advised comments made by a young person may be regretted later.

Q5B. about how the ICO, working with relevant stakeholders, might use the **opportunities presented and positively address** any challenges

Presentation and language of terms and conditions and privacy notices

The Code offers opportunities to address some of the challenges we have identified in T&C and privacy notices.

The ICO guidelines already address some of these challenges, but, if included in the Code, these would have a statutory basis.

[10] https://archive.org/web/

In particular, routine failure by an ISS provider to keep to its own published rules on joining age, T&Cs and privacy notices should be considered a breach of the Code.

ISS providers should take reasonable steps to ensure that anyone who provides consent is actually over 13.

The "take-it-or-leave-it", binary choice of most T&Cs should be avoided. Instead, data minimisation (see our other comments) and good standards should allow for meaningful choice.

Q5C. about what **design standards** might be appropriate (ie where the bar should be set) in each or any of the above areas and for each or any of the proposed age brackets.

Default Privacy Settings

Overall, data privacy should be as high as possible by default, without unnecessarily blocking children from access to services.

Design standards offer a number of opportunities to address the challenges of default privacy settings.

"Data Protection by design and by default", or "Privacy by Design", is now well-established as a principle and is included in GDPR Article 25 and the UK Data Protection Act 2018 Paragraph 57 – it was not explicitly required under the Data Protection Directive 95/46/EC or the UK Data Protection Act 1998. The checklist and established methods could be particularly helpful to SMEs and start-ups with limited resources. In drawing up the Code, consider carefully how each of the foundational principles[11] and legal requirements of GDPR and the DPA 2018 apply particularly to children.

Children should have to ability to open up some restrictions, subject to what is appropriate to their development stage, but, importantly, any changes should revert to the default, high setting when the child logs off or stops using a service (unless the child has amended the settings to be higher than the default, eg., defining in more detail who can see a social media post). The implications of any changes must be clear to the child. These considerations also apply to other settings such as geolocation which may be enabled for specific uses, but must revert to a restrictive default at other times.

Data Minimisation

---

[11] Cavoukian, A (2011): *"The 7 Foundational Principles Implementation and Mapping of Fair Information Practices"*, Information and Privacy Commissioner of Ontario, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf (accessed 18/09/2018)

The purposes for which data are processed should be limited to the strict requirements of the ISS. "Catch-all" phrases such as "improvement of services" should not be allowed to justify data processing that goes beyond the needs *of the child* in using an ISS. Equally, a child should not be required to consent to widespread data processing in order to access an ISS.

Data should only be collected during actual use of a service by a child.

Presentation and language of terms and conditions and privacy notices

Privacy notices should be clear, concise, and written in age-appropriate language, with a maximum reading age of 13.

In addition to privacy agreed in T&Cs, an important general point from the UnBias project is that at points where it is relevant, there should be means by which young people (>13) are presented with clear information on which rights are affected by particular services and on what is happening to their data (our suggested standard labelling will go some way towards this; see also our comments on the times at which this information should be presented to users).

Our engagement with young people shows that currently many do not have a clear understanding, and at times are completely unaware of any privacy/security issues.

A clear labelling scheme, such as "traffic lights" or icons, based on universally agreed standards, similar to what is done for energy ratings and nutritional value of products, could make it easier for children to make informed choices.

It is important that these signals are standardised, so that children become familiar with them as they move from one ISS to another. Use of persuasive technologies should also be a factor in such a labelling scheme.

Importantly, the level of understanding varies not only by age but also according to other demographic variables (see our comments about age ranges). The needs of more vulnerable communities (such as those whose parents may have additional difficulties in understanding rights) should be considered and protected.

Consider offering translation of the code for communities whose first language is not English, and other formats for those with other accessibility needs (such as, for example, dyslexia).

Use of geolocation

We have already stated that geolocation should be off by default. Where it is absolutely necessary to the service, for example for navigation, as much as possible should be done within the device and as little information as possible relayed remotely.

Any location data should be destroyed once the child has finished using the services, and, as with other settings, enablement of location data should return to the default off setting on log-off or leaving the service.

Where a child's location is being tracked, this must be made clear to the child.

There is almost never good justification for geolocation for children under 9, as below this age children are rarely unaccompanied.

Automated and semi-automated profiling
Automated or semi-automated profiling should be avoided unless there is a clear benefit to the child.

Where profiling is in the best interests of the child, the user (that is, the child and their parents) must be able to understand the basis of the profiling, indicated by a clear, recognised icon or in a similar way, as part of our suggested labelling scheme.

They must be able to understand how they have been profiled, express their point of view, and, if necessary, to correct it.

Data which has the potential for life-changing, legal, health, or welfare consequences (now or in the child's later life), unless volunteered by the child, must be pro-actively checked for accuracy by humans.

There must normally be an expiry date on gathered data and profiles.

The sharing and resale of data
All agencies and companies which share data, internally or with third parties, need to be aware of the difficulties of anonymisation (as we discussed in Q5A). Data should only be stored or shared for clear and legal purposes.

In general, it should be assumed that there is a high probability that data can be re-identified and linked to an individual or small group, even if it is anonymised.

User reporting and resolution processes and systems
There should be a clear indication of how children (and parents, teachers etc.) can relay their concerns if standards are not met. Findings from the

UnBias project show that children often feel powerless to deal with problematic issues as they do not know how.

We also believe that there must be mechanisms for children to access their rights in which they do not have to be a named complainant.

The ability to understand and activate a child's right to erasure, rectification and restriction

In the instances that children do wish to take action, there needs to be a clear indication of what exactly young people can do if their rights are being violated.

This is important and should be a clear, simple process. At present children often feel powerless or do not know how to take any action as it is too complex. However, if we are to see them as active users of the online space whose rights can be as affected as much as any other group, then there should be mechanisms to give them a voice.

We suggest simple, standardised tools to report abuse or retract/erase/rectify, that children can learn to recognise and use.

Q5D. examples of ISS design you consider to be **good practice**.

Nothing particular at this point

Q5E. about **any additional areas**, not included in the list above that you think should be the subject of a design standard.

Future-proofing

Technology is continuing to develop at an increasing rate. To ensure that the Code is as future-proof as possible, it should lay out principles and standards rather than requirements specific to today's services.

New services should be subject to Childhood Impact Assessments *before* they are made widely available. The Responsible Innovation approach supported by the Engineering and Physical Sciences Research Council[12] provides a framework for understanding the ethical and social implications of technology and could form the basis for such assessments.

Engagement and dialogue are key dimensions of this approach, and, in particular, children's voices should not be neglected as stakeholders in the design and development of new technologies.[13] Children may experience

---

[12] https://epsrc.ukri.org/research/framework/area/ (accessed 18/09/2018)

[13] Parsons, S. and Cobb, S. (2013): *Who chooses what I need? Child voice and user-involvement in the development of learning technologies for children with autism*. EPSRC Observatory for Responsible Innovation in ICT, https://www.orbit-rri.org/case-studies/who-chooses-what-i-need-child-voice-and-user-involvement-in-the-development-of-learning-technologies-for-children-with-autism/ (accessed 18/09/2018)

technologies in different ways than adults, but are also the adult users of the future, who may be impacted by the downstream consequences some years in the future.

Our work in the Framework for Responsible Research and Innovation in ICT (FRRIICT) project[14] sought to develop a grounded understanding of ethical issues in ICT research and development. This work is being carried forward by the ORBIT project,[15] which provides an online set of resources, leadership in the promotion and application of responsible research and innovation practices, and a peer-reviewed, open-access journal.

The Commissioner should pro-actively look forward and "horizon scan" for issues relating to children which may be raised by emerging technologies. As with the enforcement of the Code as a whole, this will require a firm commitment from government, backed up by adequate resources.

Q6. If you would be interested in contributing to future solutions focussed work in developing the content of the code please provide the following information. The Commissioner is particularly interested in hearing from bodies representing the views of children or parents, child development experts and trade associations representing providers of online services likely to be accessed by children, in this respect.

Name: [redacted]

Email: [redacted]@cs.ox.ac.uk

Brief summary of what you think you could offer
[redacted] a research group in Human Centred Computing in the Department of Computer Science at the University of Oxford.

The group's research focusses on understanding the challenges and opportunities presented as computational systems are increasingly integrated into the fabric of people's lives.

The group investigates ways to ensure fair, non-discriminatory, transparent, and accountable data-driven algorithmic systems and to empower individuals to take better control of their data, including exerting control over their privacy in future, sensor-rich information environments.

We would be interested in contributing to further development of the Code, as it embeds and evolves in practice. Our expertise is particularly relevant in on-going monitoring of the Code to ensure that it remains

[14] Framework for Responsible Research and Innovation in ICT
September 2011 – August 2014
EPSRC funded, Project reference EP/J000019/1
[15] https://www.orbit-rri.org/about-rri/ (accessed 18/09/2018)

relevant as technology continues to emerge. It is certain that future ISS will differ greatly from those we currently experience, raising new challenges which we cannot predict but can try to prepare for through anticipatory exercises.

Further views and evidence

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

Our evidence is informed in particular through our participation in two research projects:
1. Digital Wildfire: (Mis)information flows, propagation and responsible governance
November 2014 - November 2016
Funded by Economic and Social Research Council as part of Research Councils UK "Global Uncertainties" programme, Project Reference ES/L013398/1
http://www.digitalwildfire.org/
[redacted]

2. UnBias: Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy
September 2016 – November 2018
Funded by Engineering and Physical Sciences Research Council under the Trust, Identity, Privacy and Security (TIPS) call, Project Reference EP/N02785X/1
https://unbias.wp.horizon.ac.uk/

Section 2: About you

Are you:

A body representing the views or interests of children? **Please specify:** In academic research we have specifically worked to elicit the views of children and their requirements for design of technologies	☒
A body representing the views or interests of parents? Please specify:	☐

A child development expert? Please specify:	☐
A provider of ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An ICO employee?	☐
Other? **Please specify:** A University research group in human centred computing, and Responsible Innovation with experience in projects involving (1) use of social media by children and young people and (2) Children and young people's perceptions of fairness in algorithms Colleagues in the Human Centred Computing theme at Oxford will also be making a separate contribution based on evidence from other research.	☒

Thank you for responding to this call for evidence.
We value your input.