Information Commissioner's Office

Call for evidence:

Age Appropriate Design Code

Start date:27 June 2018
End date: 19 September 2018

V1.0 20180626

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 their 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: *Yes but see below.*
Very appropriate –

The Children's Online Privacy Protection Act, 1998, (COPPA), is a US Federal law which applies to websites and online services operated for commercial purposes and directed towards children. Inter alia, the Act requires businesses to obtain verifiable parental consent before collecting personally identifiable information from a child below the age of 13. Broadly speaking persons above the age of 13 are assumed to be fully competent to give informed consent to any and all forms of personal data being processed by a commercial concern without the need for the young person or the business needing to engage with a parent or anyone else. Some sites and services will advise a young person over the age of 13 to talk to a parent or carer before initiating certain types of data transactions but not all sites and services do and US law does not requires it.

Despite the title COPPA was created principally to control the extent to which commercial companies could send advertising to children. It was never envisaged as or intended to form the basis of a comprehensive or wide-ranging law on children's privacy rights. COPPA most certainly did not anticipate the way the internet would develop. Nor could it have.

*Because of the dominance of US businesses on the internet 13 quickly became a **de facto** online standard in most countries, including the UK. In the latter case this was despite the fact it was slightly at odds with the advice then proffered by Britain's data protection authority.*

Much of the research supporting the USA's choice of 13 was carried out in 1996 and 1997 or earlier. This was before Google existed. It would also be several years (2002) before "Friendster" (the first real social media platform) appeared. It was eight years before "My Space" and "Facebook" began their journey. In other words, 13 was set as a standard long before the "modern internet" emerged.

Under the previous EU data privacy regime age was not mentioned at all. There was simply a requirement for all parties to process data "fairly". In that connection if someone was a child that was a relevant consideration. However, as the 21st century progressed, as children took to the internet in ever increasing numbers it was recognised that the old formulation was too vague and that more specific guidance was needed.

In 2012 the European Commission published its proposals to establish a new data privacy regime for the EU by way of the GDPR.

In line with the UNCRC the GDPR defines a child as anyone under the age of 18 and sets out a number of limitations in respect of persons below that age. However, while recognising 18 as a critical cut off point, a separate question arose about the age at which a child who had not yet reached 18 could nonetheless still be considered capable of consenting to their personal data being processed by a commercial entity without the business concerned having to obtain verifiable parental consent.

The great pity about the way the EU institutions and the Article 29 Working Party approached this question is that at no point prior to the final adoption of the GDPR did any of the principals commission or consider new research which might have provided insights into children's competencies, vulnerabilities or levels of understanding in relation to the ways in which the internet now operated. Yet there had been enormous and dramatic changes since the USA adopted 13.

*In the draft GDPR the European Commission simply suggested making the **de facto** standard of 13 the **de jure** standard for the whole of the EU with no possibility of variation. Moreover, this was put forward solely on*

the grounds that 13 was already being widely used. This rather thin argument was eventually and brusquely swept aside in a rushed, ill-considered, politically driven last-minute scramble conducted without the benefit of any consultation with experts. An idea based on zero evidence was then changed on the basis of zero evidence.

In the end, and as a result of that scramble, by virtue of Article 8 of the GDPR, each Member State was given the option to choose its own minimum age, providing it was between 13 and 16, with 16 as the default. The UK went for 13.

The implementation date for the GDPR was set for May 2018. Before then a number of countries did consult internally about what their Article 8 age should be but, as previously stated, nowhere, including the UK, was any serious effort made to reach an evidence based informed view about optimal outcomes.

Altogether 10 EU Member States have opted for 13, 11 have chosen 16, 4 have adopted 15 and three 14. The ramifications of this spread of ages remain unclear as do consequential but vital questions about applicable law. This is a highly unsatisfactory state of affairs.

The UK's ICO is therefore to be congratulated on being the first, perhaps still the only data protection authority in the EU to have asked for research to be done in this field. It is being conducted by Professor Sonia Livingstone, and we look forward to seeing the results before reaching a final view on the ICO's proposed age ranges.

In an ideal world it would be possible to tailor every site or service to the specific capacities, vulnerabilities and levels of understanding of each child. Were that to be the case deciding on the appropriateness of age ranges would be redundant. This "ideal" approach would also be more closely aligned with the UNCRC, with its emphasis on the evolving capacities of the individual young person. However, for the foreseeable future that is an unrealisable counsel of perfection.

While a great many online businesses pride themselves on being able to absorb and analyze large numbers of datapoints in order to "personalize" the service they deliver to each of their customers, the nature of any additional information that would be required about children might be particularly sensitive.

Even if the collection and processing of such additional data was carried out by independent third parties, rather than the service provider itself (as is likely to be the case, for example, when the age verification provisions of the Digital Economy Act, 2017 come into force), its collection would be likely to require even more intrusive enquiries to be

made of the child or their parents or carers, or both. That would look odd in a context where data minimization is held to be of such importance (although see comments below).

For the time being, therefore, while age banding is impersonal and runs counter to the idea of delivering services which meet the needs of each child, it seems to be the only practical way forward and, subject to the need to revisit the matter when Livingstone's research is concluded, as previously stated, the age bands suggested in the ICO consultation paper seem reasonable.

Notwithstanding these remarks, where broad age bands are applied, if a business acquires actual knowledge of a particular child's situation, it should be required to adjust the settings that are otherwise standard for the relevant age group in order to protect the individual concerned from a reasonable apprehension of the risk of harm.

We would also like to emphasise the importance we attach to all businesses observing the requirements of Article 35 of the GDPR and its UK legislative equivalent. This requires companies to carry out a data impact assessment (DIA). These should cover every discrete aspect of the site or service. The assessments must include an evaluation of the potential impact of allowing third parties to gain access to children's data.

The DIAs must show that the business has evaluated the impact of their decisions or actions on children's privacy across all relevant age groups accessing or using the site or service. It should not be assumed that one size fits all. A child of 13 is not the same as a child of 17. The Code should prohibit the use of general consents or consents which permit varying levels of privacy within the same service.

We understand businesses will not be required to file their DIAs with you. That is a shame. Nevertheless, we hope your code will say that you may require child focused DIAs to be produced to you on request and in short order, together with supporting evidence that the business had carried out a thorough analysis of each aspect of the service they offer. Substantial penalties should attach (a) to failing to produce a child focused DIA in a timely manner and (b) to producing a DIA which fails properly to take account of children as users.

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),

At the lower end of the age spectrum one would expect stringent protective requirements to be in place, linked to higher penalties for failure to observe them.

As children get older a tension arises. On the one hand their capacities evolve and, for many, their level of understanding of the internet also improves. This implies both a need and a right for older children to be allowed greater latitude to explore and make decisions for themselves.

And yet, based on the experience of CHIS members, it is among these same, older age ranges that the vast majority of concerns arise in relation to, for example, online grooming, bullying, anxieties about emerging sexuality, peer pressure, and engagement with age inappropriate content of different kinds, including sites or services which promote self-harm.

This suggests significant numbers of children have and sustain some kind of disconnect between their apparent understanding of the online world and the ways in which they actually behave. *This disconnect is a fairly common aspect of adolescent development that is increasingly being understood in terms of what we know about brain development in adolescence. Cognitive reasoning and skills develop, but are not necessarily linked to skills in planning, problem-solving, emotional regulation and consequential thinking. In short, adolescents are typically smart but impulsive and particularly subject to peer influence.*

Policy needs to find a way to balance these tensions. The precautionary principle suggests we should always err on the side of caution.

We were very pleased the UK Parliament removed any doubt surrounding the status or significance of Recital 38 of the GDPR. It is extremely important for there to be no let or hindrance to children being able to access good quality sex and relationship information and counselling. Any suggestion that parental consent was needed before a child could engage with a site or service providing it would be extremely unhelpful. Neither should such sites or services be put behind age gates or other types of filtering or blocking mechanisms.

On a related point which follows on from our earlier comments about the lack of research in this area, it is important to note, for example, that 13 has no legal standing in any of the four countries that make up the UK. Neither does it have any particular significance in terms of child development milestones. Moreover, it does not obviously square with the Government's recent decision to allow someone aged 15 or above, for example, to opt out/in of Relationship and Sex Education, and its newer component of Health Education (which has a strong online safety aspect).

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 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)

The UNCRC is essentially a pre-internet document although its core idea – which focuses on the evolving capacities of the child – must remain at the heart of all childcare policies, including policies which touch on children's privacy rights.

There are now a number of other relevant international instruments or standards to which the UK is party e.g. EU Directives and the Lanzarote and Budapest Conventions. The Council of Europe's recently adopted (July, 2018) "Recommendations to Ministers" are also important in describing contemporary best practice and aspirations.

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

Hitherto too much reliance and responsibility has been placed on the importance of children and their parents and carers getting to know the privacy settings for an individual App or service. There is, of course, a great deal to be said in favour of this but the protection of children's privacy should not be a prize to be claimed only by those children who

can either do it for themselves or are lucky enough to have parents who are capable of solving the puzzle and able to engage with the App or service long enough. Some of the neediest children may have parents who lack the necessary capacities.

Thus, at the point of first use, a site or service which is targeted at a child or is likely to be accessed by a child, every privacy choice or option should be set at a point which yields the minimum amount of information about the user consistent with being able to run the service at its entry level and that minimum must, in turn, be consistent with best practice in terms of children's privacy rights and their contingent well-being. Such is, in any event, a requirement of the GDPR but it is of particular importance that this is observed where children's privacy interests are concerned.

The company should have the prime responsibility for guaranteeing the privacy rights of its users. That cannot be delegated or assigned by them to unknown parties with unknown competencies.

Within an individual site or service some activities may be inherently riskier than others and this should be reflected in how the privacy dimension of each activity is explained and offered.

If choices are to be made about liberalising or relaxing any settings these must be hedged around by context sensitive and age appropriate language, support and guidance.

Thus, the Code should unambiguously state that companies have an obligation to be certain the defaults are set at the optimal level of privacy and any and all changes which are subsequently made must be fully and properly explained in accessible language.

Greater consideration also needs to be given to ways, after the initial sign up is completed, of ensuring children do not go on to publish material which is likely to compromise their privacy or damage their longer terms interests. Clearly here education has a vital role to play but so too do technical measures e.g. measures which detect images that are likely to be inappropriate or text which discloses personal data such as phone numbers, the address of one's school and similar.

Many companies already use tools which do this. It would be useful, however, if the Code could refer to them and give them some legal backing. Our view is, wherever privacy protective technical tools are available, and it would be reasonable and proportionate to deploy them to safeguard children, then the site or service should be under an obligation so to do with heavy penalties attaching to a breach.

- data minimisation standards

This is an important principle. However, it should not be taken to extremes i.e. to a point where a child's privacy rights or right to a safe internet experience are sacrificed in its name. Data minimisation should be seen as an enabler of children's privacy not as a road block which in fact results in children being placed at greater risk. Some guidance on balancing potentially competing policy objectives in this area would be most welcome.

One question which remains unclear is whether or to what extent ensuring children's privacy entails expanding the scope of age verification.

"Knowing Your Customer" is vitally important. However, without going so far as to say that every App or service has to age verify every user in order to be sure it is properly identifying children (or indeed adults) to ensure they are not gaining access to sites or services which are not meant for them, where it is reasonable and proportionate, there should nevertheless be an obligation on sites to use algorithmic and other technical tools to determine whether or not an individual's postings or other activities are aligned with their declared age. This is consistent with a range of actions sites and services take in the interests of a variety of security concerns e.g. to combat spam, malware and illegal content. The safety, security and privacy rights of a child should have equal standing.

- the presentation and language of terms and conditions and privacy notices

If 13 is the legal entry point for a site or service there is a strong argument for saying any and all information about the site or service should be presented in ways which 13 year olds can understand.

While acknowledging the difficulty that may attach to achieving this, there should nevertheless be an overriding obligation on all companies to promote and draw attention to all of the choices which impact on privacy and to do so in the most user friendly and age appropriate way. Where there are any specific concerns in relation to children these should be given extra emphasis. It should not be too difficult for a business to do this because they are, in any event, meant to have carried out a risk assessment in respect of every aspect of their service so this would be a logical extension of that exercise.

We hope the code will encourage the deployment of simplified systems, such as one finds increasingly with food labelling, to describe levels of risk and corresponding levels of privacy on offer in respect of each discrete aspect of a site or service.

Any mismatch between the stated terms and conditions on which a site or service is offered and the actual performance of the site or service should be heavily censured and penalised. It is unacceptable for a site baldly to state, for example, that certain types of images are not allowed if it then takes no active steps to enforce that rule. A parent or child may rely on such statements so making no effort to deliver on the implied promise amounts to a misrepresentation or deceptive marketing

- uses of geolocation technology

There are two parts to this.

- *1. Until someone reaches the age of 18 geolocation data should be regarded as sensitive data. In effect, via the Code, the UK should create a new class of data to be added to the list in Article 9 (1).*

- *This means ordinarily it would be prohibited to collect children's geolocation data unless certain conditions are met. Our suggestion, therefore, is that the ICO should also add one or more new clauses into Article 9 (2), to describe the conditions under which children's geolocation data may be collected and the purposes for which they may be further processed.*

- *Such conditions would make it clear that children of all ages, without limitation, should be able to use sites and services which allow them to interrogate maps, for example to obtain directions or acquire other forms of geographical information. However, where a site or service collects data on someone's current or previous physical geolocations, special measures have to be put in place to ensure such data pertaining to children of any age cannot be broadcast or published to any third party without extra precautions, warnings, permissions or contextually appropriate limits. If a site or service allows third parties access to location data they should ensure similar restrictions apply.*

- 2. *Where a site or service collects or otherwise processes geolocation data, or it allows third parties to do so it is engaging in or facilitating a form of profiling. While Recital 71 says that profiling should not "concern a child", and this is further amplified in Recital 75, because these are only Recitals and the language is not reflected in any Articles, there is no clear-cut legal requirement to refrain from this type of activity and the language used is in any event insufficiently explicit or unambiguous.*

- *That said, it may be acceptable for certain types of commercial or other activity to be linked to an older child's geolocation data but*

until there is much greater clarity about the circumstances and context in which utilising geolocation data would be acceptable in respect of a child, companies will need to be very careful to develop fully justified use-cases. Alternatively, companies may be better advised to await the development of authoritative guidance.

- automated and semi-automated profiling

- *It is important to have greater clarity about the types of automated and semi-automated profiling activities that might be considered to be acceptable in respect of children. An extensive list of examples would be very welcome. These could also act as authoritative guides for self-regulatory codes which might be developed and adopted by trade associations or other relevant bodies.*

- transparency of paid-for activity such as product placement and marketing

- *There should never be any ambiguity or doubt about matters of this kind. We commend the practices recommended or specified by the Advertising Standards Authority.*

- the sharing and resale of data

- *The GDPR requires that there should never be any ambiguity or doubt about matters of this kind and it is of obvious and special importance where children's data are concerned. The principle must be that if you, as a business, allow third party access, either via sharing or resale, you assume full knowledge, and therefore full liability and responsibility for what happens next.*

- the strategies used to encourage extended user engagement

It is difficult to come up with a comprehensive answer to this question. Much will depend on the nature of the extended user engagement. However, we greatly approve of recent advances whereby leading services close down altogether after a user has been on for a certain length of time. This entails a cessation of collecting any data. Sending prompts or reminders to ask the user to consider stopping may also be a useful strategy.

The use of the law of diminishing returns could be deployed more aggressively and extensively e.g. in relation to games, the longer you play or stay the harder it should be to amass points or win.

There is also a strong case for limiting the ability of social media platforms to construct or offer services which are likely to disrupt a child's sleep or distract them during school hours with pings and other forms of real time notifications. Auto play and read receipts can act in a similar way and therefore, again, should be limited at certain times of the day where it is known the user is a child.

- user reporting and resolution processes and systems

  It is of paramount importance that such matters are fully explained in an age appropriate way

  The Code should encourage a greater degree of uniformity of practice and consistency of look and feel between sites and services. As one moves from site to site or service to service it should not be necessary for a child or his or her parents or carers to learn a whole new set of terms, icons, or approaches to reporting.

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

  It is of paramount importance that such matters are fully explained in an age appropriate way. The code should clarify and give unambiguous legal backing to a child's right to erasure.

  In particular, in principle, there should be no greater formality or difficulty attaching to securing the erasure of an item that has been posted on a social media site or service, than there was to it being posted there in the first place.

  Thus, if a site or service does not check a child's age before allowing them to post, say, an image, why should the child have to prove their age to have it removed? For example, it is unacceptable to force a child to jump through hoops to prove they are under 18 before they can secure the removal of an image they find embarrassing. It is likely to discourage too many children from going through the process.

  Every day, perhaps many times in a day, the IWF and companies have to determine if, for example, a particular sexual image involves a person below the age of 18. They do not ask for proof before they decide. They make a visual assessment, a judgement, and they act on it. The same should be the case here.

Companies should follow the same practice and always err on the side of believing the child. Typically, there is an asymmetry of power and ability in the relationship between a company and a child which favours the company and disadvantages the child. The code should eliminate or reduce that asymmetry.

The code should mandate services to build simple and effective tools which are accessible even by young people not members of the site or service in question. If an image or piece of text is of them or about them they have a right to request its removal.

Thus, even where an image of themselves has been created or shared by others, a child should be able, speedily and easily, to obtain its removal and, once removed, the site or service should be required to have mechanisms in place to ensure it is not re-uploaded or further distributed or shared on their platform. Should such an image nevertheless reappear it should not be necessary for the site or service to wait for another request from the child in order to have it removed.

Our earlier comments about the uniformity or consistency of design, look and feel are once again relevant. Children and their parents and carers should not have to learn several different ways of exercising their right to request erasure or have to get to grips with different icons or pictorial representations or textual descriptions to claim what is their right in all online environments.

- the ability to access advice from independent, specialist advocates on all data rights, and

  It is of paramount importance that such matters are fully explained in an age appropriate way.

  Children should not have to face obstacles or difficult or confusing challenges to work out what their privacy rights are, or how to categorise them, in order to complain or seek redress in relation to a potential breach.

- any other aspect of design that the commissioner considers relevant.

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.

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.

The Code should put companies on notice that they may be required to explain and justify every aspect of the way they design and present their services in order to ensure they are respectful of and protective towards children's privacy rights.

In research conducted by the University of Nottingham

https://psauthority.org.uk/-/media/Files/PSA/For-Businesses/Resources/Consumer-behaviour-and-ICSS-Exploring-how-consumers-respond-to-ICSS.ashx?la=en&hash=ACE521A3348ADED0F7346DA4459CD6FEBE38D316

we are reminded of the pivotal importance of how and where information is placed on a page, the colours used and so on. This can have a decisive impact on whether the information is found, understood and acted upon even by adults. Businesses should be able to show an awareness of factors of this sort when they design their service and be able to show how their final design choices helped rather than hindered children's privacy rights and did not seek to exploit or profit from a child's commercial naivety.

Similarly in a report recently published by the Norwegian Consumer Council ("Deceived by Design") we see how companies deploy a range of techniques which produce or utilise.. " patterns, techniques and features of interface design meant to manipulate users… to nudge users towards privacy intrusive options. They use privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users."

This may be thought by many to be reprehensible and to be contrary to the spirit or letter of the GDPR even where adults are concerned, but such approaches should be completely forbidden in any site or service which is targeted at children or is likely to be accessed by them. It is simply unfair and unacceptable to make children the object of techniques which are designed to maximise revenues via disguised or manipulative techniques

of this sort. When it is known that adults have difficulty negotiating or understanding such things there can be no justification for using them with children.

Particularly in the present climate businesses should be going out of their way to reassure the public, parents and children alike that they are taking all reasonable and proportionate steps not to take advantage of or exploit children's lack of worldly experience.

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

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.

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

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

The growing use of facial and voice recognition software by online services, including in IoT products, raises key privacy concerns particularly in the context of the continued rapid growth of the "Internet of Things". Many toys, for example, utilise such technologies. Aspects of this may fall to be considered as a dimension of profiling. This simply underlines the importance of our earlier comments about the need for an extensive list of examples where profiling might be allowed in respect of children.

Article 9(4) of GDPR allows Member States to 'introduce further conditions, including limitations, with regard to the processing of…biometric data', and the Code is a good opportunity for the UK to do that, at least insofar as children are concerned.

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: John Carr

Email: john@johncarr.eu

Brief summary of what you think you could offer:

I am Secretary of the Children's Charities' Coalition on Internet Safety. Coalition members connect with a broad range of concerns which impact on children's privacy.

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.

---ooo---