Grant Thornton
An instinct for growth™

21 May 2019

ICO Age appropriate design code.

Thank you for the opportunity to comment on the ICO's draft code.

Firstly, some general points then some more specific ones.

General points:

The draft code probably goes beyond the Data Protection Act 2018's requirement for the ICO to "prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children". The code is more of a comprehensive data protection compliance code and could perhaps focus more on designing services in an age-appropriate way, in terms of the readability of privacy notices, for example. If I was a company designing an online service likely to be accessed by children, I do not think I would find this code as useful as it could be in terms of providing practical design advice as to what a child-friendly online interface should look like or what its functionality should be. There are various parts of the code that add little if anything to existing ICO guidance – e.g. the section on data governance. Perhaps it would be best to remove duplicated content as far as possible and to just include links to this. As it stands, the code is far too long and is unlikely to be used as a reference document by busy practitioners. A simpler good practice Vs things to avoid checklist would be more effective.

The code stretches very considerably the 'likely to be accessed by' wording of s.123 of the DPA 2018. There must surely be a connection between a site being likely to be accessed by children and its content being aimed at children. I accept that children will seek to access sites that are clearly not aimed at them. (I read a piece of research that said that 94% of children had accessed adult sexual material online.) However, surely this cannot mean that adult websites hosting such content, for example, are 'likely to be accessed by children' and that therefore their operators have to comply with this code. This problem is exacerbated by the ICO's contention that even if only a small proportion of a website's visitors are children, this means that the website is likely to be accessed by children. There is a danger that all websites will, in theory, be subject to this code even if they contain content that is clearly not intended to be accessed by children. The code needs to be much more precise - and limited - in terms of the sort of online services it applies to.

The code takes the approach of trying to make data protection law intelligible to children – e.g. through child-friendly privacy notices. Data protection law is largely unintelligible to adults, so this is a big ask. The code seems to have no minimum age cut-off point so presumably service providers are expected to explain the law in terms intelligible to a 3yo, for example. I think this approach is extremely unrealistic, although I accept that there is no 'get out' under the GDPR in terms of providing full GDPR-compliant privacy notices to children. In fact, Art.12 of the GDPR makes it clear that full privacy notice information has to be intelligible etc. 'in particular for any information addressed specifically to a child'. This touches on a basic contradiction in the way the GDPR treats the processing of children's personal data. On the one hand the GDPR treats children as data subjects like any other, on the other it states that children (in the UK, individuals under 13) cannot themselves consent to the use of information society services. Surely if privacy notices can be provided in terms that a child understands, then so can choices over the use of information society services? However, unhelpfully, the law does not take this approach.

Although deviating from a literal reading of the law, it might be much clearer for the ICO to take the approach of assuming that not only are individuals under the age of 13 incapable of giving consent for the use of information society services, but are also incapable of understanding GDPR-style privacy notices, the exercise of their rights under the GDPR and so forth. It would be clearer to say that if a service is genuinely likely to be accessed by someone under 13 years of age then parental consent should normally be sought for the processing of his or her personal information. Similarly, privacy notices should normally be aimed at the child's parent (or guardian et al) and not the child him or herself. (The code tries to distinguish between different ages of children and to explain information rights etc. in ways appropriate to a particular age-group. However, this approach really won't work in practice given the significant difference in mental competence between children within the same age-group and given that service operators will usually have no reliable means of determining the age of the individuals using their services. At various points the code seems to assume a more reliable system of age verification then is actually in place – and that content

can be tailored accordingly. A better default position might be to assume that service providers normally do not know the age of the individuals accessing their services.)

Generally, the code does not acknowledge the role of parents, guardians et al. sufficiently. A good example concerns the issue of whether a child can be monitored without his or her knowledge. This is surely a matter for a parent or guardian rather than a regulator to decide. There may be good reasons for monitoring without a child's knowledge and it is up to the child's parent or guardian to decide the degree of transparency that is appropriate. The underplaying of the authority of parents and guardians is connected to a lack of recognition in the code that the law does not apply to processing carried out by a natural person in the course of a purely personal or household activity. (I accept that this limitation does not apply to organisations providing services, even if those services are accessed in a purely personal or household context.) However, there is a strong argument that many issues covered in the code involve data processing activity that is being carried out for purely personal or household purposes and that should fall outside the scope of data protection law and therefore of this code.

The code often uses language that is difficult to translate into actual practice. For example, it says this, in the context of privacy settings: "The exception to this is if you can demonstrate that you have a compelling reason to do otherwise taking into account the best interests of the child." I think that an 'average' service provider would find this very hard to translate into practical measures, which is what a code of practice should help an organisation to do. What is a 'compelling reason', what are the 'best interests of a child'? Wording like this opens up more questions than it answers and should be avoided wherever possible.

The code gets into general issues concerning the development and well-being of children. This is all hung on the 'fairness' requirement of data protection law, which is maybe being stretched too much. Trying to import the UNCRC's very wide interpretation of the best interests of child into data protection law is problematic. Does the ICO have the necessary expertise to assess to effect of data processing on a child's physical, psychological or emotional development, for example? There is a danger of the ICO taking on a general child protection role that it probably lacks the expertise to deliver.

Summary of code standards.

This section would benefit from a clear initial statement as to the sorts of services and service providers that it is aimed at. As it stands, there is a danger of the code being applied to services that are clearly not intended to be accessed by children.

Under the Data Protection Act 2018 the ICO is tasked with preparing a code of practice about appropriate standards of age-appropriate design of relevant information society services which are likely to be accessed by children. This presents two problems of scope.

Firstly, the term 'Information Society Services' (ISS) is not easy to define. Some online services that collect and use a child's personal information will constitute an ISS whilst others will not. The code generally refers to 'online services' which, technically speaking, broadens its scope beyond the definition of an ISS. However, as far as children using online services is concerned, the distinction between an ISS and a non-ISS service is largely academic. However, the code should be clear about its scope – if it is not just addressing ISS, but rather online services more generally, then it should say so. I think it would be best to address the code to online services likely to be accessed by children, including ISS.

Secondly, what does 'likely to be accessed by children' mean? This is unfortunate terminology. How do website operators know whether their websites are likely to be accessed by children and therefore whether this code is relevant to them? Unfortunately, 'likely to be accessed' is not the same as 'aimed at' – children access all sorts of services that are not aimed at them – see this 2016 report for example: https://www.bbc.co.uk/news/education-36527681 The 'likely to be accessed' test is difficult for service providers to address in practice. However, I think it would be a mistake to suggest that services that are clearly aimed at adults, but that are nonetheless accessed by children, need to adhere to the code's recommendations. Otherwise we will end up in the strange situation of pornography websites, for example, being required to have child-friendly privacy notices etc. because some children access pornography websites. That cannot be the right outcome. 'Likely to be accessed by' needs to be construed more like 'aimed at' – i.e. the code should be for services that host the sort of content that children are likely to

access, because it is aimed at them, rather than services that host content that is not aimed at children but which nonetheless is likely to be accessed by them. This is an important issue for the code in terms of its purpose and scope.

Age-appropriate application.

As written, this suggests that any service that is clearly aimed at adults, but where an age-verification system is not in place, has to be presented as if it were aimed at children. This is unrealistic and over-the-top. The line taken in the code is that even if a small proportion of service users are children, the service has to be deemed to be 'likely to be accessed by children. Presumably this means that a service run by a political party, for example, which clearly some child activists might want to access, but which does not have an age-verification system in place, would have to present content in a form suitable for children. This is clearly a highly unrealistic scenario. Again, if we construed 'likely to be accessed by' more like 'aimed at' then this problem would be avoided. (This also begs the question – which is relevant to many other issues addressed in the consultation document – of what we mean by a child – generally there would be a considerable difference between a three-year old's and a twelve-year old's level of maturity and understanding, although both are children in GDPR terms and for the purposes of the code. Confusingly, the code also uses the UN's 18yo definition at certain points – the code needs a clear statement that for its purposes a child is anyone under 13yo.

Transparency.

It would be useful to explain how GDPR-compliant privacy notices can be delivered to children – e.g. the content about legal bases for processing or overseas transfers of personal information. Of course, this cannot be explained to (the vast majority) of children. This begs the question of how operators of services aimed at children can adhere to the ICO's recommendations whilst satisfying their legal obligations under the GDPR. This perhaps reflects a deeper problem with the approach taken in the consultation document. There is a strong argument that the 'transparency information' set out on a website aimed at children should not be aimed at child website users themselves, but rather at their parents, guardians or others with responsibility for them. Parents et al can then decide whether the child is allowed to use a particular website. It is unrealistic to expect a child – even a teenager – to read GDPR-type privacy notice and to make an informed decision, based on his or her understanding of it, as to whether to provide their personal information to a particular service, no matter how 'readable' or simply-written the transparency information may be. (I realise this problem stems from the GDPR's contradictory and unrealistic approach to the processing of children's personal information.)

If a child wants to use website – for example to play an online game with other children (and quite possibly adults too) – without the supervision or permission of his or her parent, guardian etc., then I find it highly unlikely that they will read a privacy notice posted on the website. They will just go ahead and play the game. Most adults don't read privacy notices, and it seems likely that take-up amongst children will be even lower. (Is there any research on this?) That is why the basic approach suggested here, of providing simple transparency information on websites aimed at children, is unlikely to deliver any meaningful protection to them. The role of parents, guardians and others with responsibility for the protection of children – online and offline - needs much greater prominence here and throughout the document.

Parental controls.

It should be for the parent (guardian et al.) to decide whether a child is told that he or she is being monitored. It should be the parent's prerogative to make this decision. This is an example of data protection law overstepping the mark and straying into areas of private family life. This approach also fails to recognise that where a child lacks maturity, it is for the parent to decide on the child's behalf whether he or she should be aware that monitoring is taking place. It is wrong to use data protection law to diminish parental choice and control in contexts such as this.

Online tools.

Again, this should reference parents as they are probably more likely than children themselves to report concerns about online data protection issues. I suspect that the ICO receives very few complaints from children – if any at all - about data protection issues in the context of online services.

It would be useful for this code to reference the law's provisions concerning processing done for purely personal or household purposes – see GDPR Recital 18 in particular. Although this only applies to processing done by natural persons, and not to an organisation operating a service aimed at children the legal and policy intent of the limitation of the GDPR's scope here must be to allow a 'safe space' for parents, children and others to make decisions about data processing activity without the intercession of data protection law. This goes to the point made above about the problem of the law saying that the default position is transparency – e.g. when monitoring a child – even if a parent with responsibility for the child might not want that. Surely in circumstances such as this, the wishes of the parent must normally prevail.

About this code – At a glance.

It is too bold to state that following the code will "enable you to design services that comply, and demonstrate you comply, with the GDPR and PECR". Firstly, it is not services that have to comply, it is the controller that has to be compliant. Secondly, even if an organisation follows the code to the letter, it might still not be compliant. Ultimately, only a court can rule on whether there is compliance or not. Better wording would be along the lines of "following the recommendations in the code should facilitate your compliance with the relevant law".

Who is this code for?

The DPA 2018 requires the ICO to "prepare a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children". However, I wonder whether the intention here was to just address ISS or online services more widely. It might be better to frame this code in terms of the latter but clarifying in the introduction that the code fulfills the ICO's brief in terms of addressing children's use of relevant ISS services. ISS are referenced at various points in the GDPR, but the only significant references are in connection with a child's consent and the right to erasure. Clearly the code addresses more than those two issues. All the other GDPR requirements binding on service providers – compliance with the principles for example – do not reference ISS but data processing more widely. It might be better therefore to say that this code is aimed at everyone who offers services likely to be accessed by children, including ISS. (The definition of ISS is by not straightforward, given the 'remuneration issue' and the fact that some online services used by children are not ISS. For example, as I understand it, a child's personal use of electronic mail does not constitute the use of an ISS but does constitute the use of an online service.

On territorial scope, the code should be aimed at any organisation that whose services are likely to be accessed by children and that processes personal data in the context of the activities of an establishment in the UK. It is irrelevant whether those services are likely to be accessed by children in the UK or by ones elsewhere. It would be more legally precise to just say "likely to be accessed by children".

It is very confusing to state that the code is "not only for services aimed at children" (note my point above about 'likely to be accessed by' Vs 'aimed at'). If it is aimed at services aimed at anyone – then the code needs to be renamed and substantially re-drafted to reflect that. I accept that a child could access virtually any online service, whether it is aimed at children or not. However, if we are moving the scope of the code from 'likely to be accessed by' children to something more like 'accessible to' children, then that constitutes a very significant widening of scope and runs the danger – as mentioned in my comments above - of all online services being expected to meet child-relevant standards just because a child might be able to access them. The code must be much clearer in terms of its scope and what constitutes a service that is likely to be accessed by children. However, there are approaches in the TV advertising industry, film classification and elsewhere that presumably the ICO could draw on.

What is the legal status of the code?'

The reference to 'DPA 2019' needs correcting.

What happens if we don't comply with the code?

(The 'we's' and 'you's' wording needs checking throughout.)

It would be useful to state the level of potential fine in approximate sterling equivalent rather than the Euro as this implies that the ICO will issue fines in Euros, which of course it won't.

What do you mean by an 'information society service'?

I note that this part of the code includes online messaging services as constituting an ISS – this is an over simplification. This section needs to cite the reference in the legislation that states that the use of electronic mail by natural persons acting outside their trade, business or profession is not an ISS. This suggests that a child's use of an online mail or messaging service for his or her personal use is outside the scope of this code.

The exchange of online mail and messages is a major source of bullying and harassment and is a means of communicating inappropriate content. The code either needs to make it clear that it does not apply to electronic mail services or needs to move away from the technical definition of ISS and address online services that collect and use children's personal information more generally. In my view the latter approach would make the code clearer in scope and more effective in terms of protecting children from negative online experiences, regardless of the definition of ISS and the brief set out in the DPA 2018.

I think the ICO is stretching the definition of 'remuneration' even more than it has already been stretched by the legislators. I find it difficult to accept that any form of online advertising – targeted or not – means that there is necessarily remuneration taking place. In its ordinary meaning; 'remuneration' means 'payment'. There is a (weak) argument that the monitoring of online behaviour and the subsequent delivery of targeted advertising involves the monetisation of personal behaviour and therefore constitutes 'remuneration'. However, it would be very difficult to argue that there is remuneration if an individual's browser settings and the use of other tools means that the service provider receives no information at all about the individual's online behaviour, preferences etc. – or where the website only uses 'broadcast' type advertising – i.e. every user sees the same ad. In cases like that, how does the remuneration take place? It would be useful for the code to clarify whether the receipt of any advertising, targeted or not, necessarily involves 'remuneration'. (I find it hard to accept that there is 'remuneration' where I watch a free-to-air commercial TV channel that carries advertising. Am I really remunerating the TV channel when I watch it? Some online services operate in much the same way.) The code should explain the 'remuneration' issue more clearly.

What types of online services are not covered by the code?

This should reference the 'messaging' issue mentioned above.

It would be helpful to explain why the code does not apply to websites or apps specifically offering online counselling or other preventive services. Is this because they fall outside the definition of ISS or for some other reason?

When are services 'likely to be accessed by children'?

If the ICO is going to cite the UN definition of a child being someone under 18, then we need to explain the interplay with the Data Protection Act 2018's age limit of 13 years. Despite what the law says, it would be better to avoid specific age limits – which are largely useless in a practical sense unless underpinned by a reliable age-verification system. It would be better to rely more on the traditional UK tests of maturity and mental competence. (Although I recognise that the UK also uses specific age limits, for example in respect of the purchase of age-restricted goods.) In any event, the ICO needs to be clear about whether it is relying on the 18yo UN age-limit or the UK 13yo one. (The ICO should rely on the latter as the former has no statutory force in the UK or indeed anywhere else. It is confusing to cite both.)

This statement is not particularly helpful: "This means that when you design your service you need to think about whether it (or any element of it) is likely to appeal to, and therefore be accessed by, children, even if this is not your intent. If it is likely to be accessed by children, then it will be covered by the code." This goes to my point above, about children being likely to access services that they are clearly not intended for them – e.g. adult content websites which may well 'appeal to' them. In my view, website operators will find the 'likely to appeal to' test to be impossible to apply in practice. A more realistic approach would be to set out the sort of features / content / links a website or other online service must have in order to make it likely to be accessed by children. Similarly, "you must be able to point to specific documented evidence to demonstrate that children are not likely to access the service in practice" will be impossible to comply with in practice and places an unreasonable burden on service providers. The code states: "if evidence later emerges that a significant number of children are in fact accessing your service even if this is only a small proportion of your overall user base - you need to comply with the code." – what sort of evidence might this be

and does this mean that if a website about, say, investing in the stock exchange has 1 million users and a few dozen of them are children (assuming you could ever know that), then you have to comply with a code about services likely to be accessed by children? This section of the code is confusing, unrealistic and unhelpful.

Does it apply to services based outside the UK?

This section does not tally to the earlier (problematic) reference to the code applying to services are likely to be accessed by children in the UK.

Best interests of the child.

I know this isn't the ICO's doing, but section 18.1 of the UNCRC strikes me as odd and suggests somewhat anachronistically and in a rather culturally exclusive way that children should normally have two parents.

Generally, it might be best to cite this document sparingly and just to focus on the content that falls within the ICO's statutory remit – e.g. personal information, privacy and issues to do with access to information.

Generally, the UN content about the best interests and rights of the child is very admirable. However, it is too abstract and at too high a level for any 'regular' online service provider to convert this into practical design steps. It would be better to stick more closely to the DP Principles – transparency, necessity, fairness etc. – as those concepts have more real-world relevance and are easier deal with in a practical sense.

Age-appropriate application.

The general approach suggested here will be of little value unless the code provides some practical advice as to how providers can verify the age of people using their service. Ideally, the ICO should develop tools to allow them to do this, assuming this is possible (which it probably isn't). As this part of the code says, "Understanding the age range of children likely to access the service – and the different needs of children at different ages and stages of development – is fundamental to the whole concept of "age-appropriate design". That is true, but unless service provides know how to verify the age range of children likely to access their services, then this well-meaning advice will achieve little in practice and will just cause more uncertainty as to the practical standards organisations are required to meet.

Apply the standards in this code to all children.

Again, it is fine to say that "Asking users to self-declare their age or age range does not in itself amount to a robust age-verification mechanism under this code". I'd agree with that – but if you expect service providers to inform the way they design and operate a service to a child's age then you need to tell them how to do this in practice. Otherwise you will be making unreasonable demands that providers will be unable to comply with. (Much of this code assumes that age verification is available to service providers, when in most cases it is not. What are the "robust age-verification mechanisms" that can confirm the age of each user? This is something of an elephant in the room for this code – and how could a 12yo child ever prove that he or she is 12yo, for example?) As I state earlier, the default assumption should be that service providers do not know, and cannot find out, the ages of the users of their services.)

The code says this: "We recommend that you give your users a choice over the use of age verification wherever possible. In other words, we recommend that you provide a child-appropriate service to all users by default, with the option of age-verification mechanisms to allow adults to opt out of the protections in this code and activate more privacy-intrusive options if they wish." This begs a number of questions. Leaving aside the practicalities of carrying out age verification in the first place, what does 'child appropriate' mean here? What age of child? This seems to suggest a 'lowest common denominator' approach where the default position should be that services are appropriate a very young child, with older children being able to verify their age to access more privacy-intrusive options and presumably to access additional age-sensitive content. According to the approach set out in the code, this would mean that the provider of a service ostensibly aimed at adults – about financial investments for example - but where a small proportion of its users are children (assuming the service provider could know this) – would have to provide its 'default' website in language – and provide content - suitable for, say, a 4 year-old. That would clearly be a bizarre and unworkable outcome. I find it hard to understand your conclusion that your approach "limits age barriers and incentives for children to lie about their age, limits the collection of hard identifiers, helps demonstrate privacy by design and default for all users…"

This part of the code goes on to say that: “If you believe only adults are likely to access your service so that this code does not apply, you need to be able to demonstrate that this is in fact the case.” The language here has changed from likelihood of access by children to access only adults – the two tests are different. I question whether someone who provides a service that is clearly aimed at adults and whose content is innocuous should be required to demonstrate that only adults are accessing the service. The standard should be that if a service that is not aimed at children then this code should not apply to it, even if some children do access the service. It is primarily for parents and others with responsibility for children to stop them doing so if access would be inappropriate.

Transparency.

I do not accept – despite the assumptions of the GDPR’s legislators – that a GDPR-style privacy notice could ever be relevant or intelligible to a young child, or indeed to most children. I do not accept that it is possible to translate information about legal bases or overseas transfers, for example, into language / concepts intelligible to a child. The code should state clearly that children cannot be expected to read and understand GDPR-style privacy notices and that their parents / guardians et al. should do this on their behalf. It would be interesting to see what a GDPR-compliant privacy notice aimed at, say, a 6yo would look like. A cartoon or video illustrating the need to identify a legal basis for processing a child’s personal data would be an interesting watch. The same reservations apply to terms, policies and community standards. It is highly unlikely a child will read or understand these – adults generally don’t, so why should children be expected to?)

Detrimental use of data.

Rather than just citing governmental and other guidance, it would be useful to provide some examples of content that is generally considered to be detrimental to a child. I fear that by getting into the broad issues of detriment and child well-being, the ICO may be going beyond its area of statutory competence and professional knowledge. The argument seems to be that the display of content that is detrimental to a child is unfair and therefore in contravention of the data protection principles. However, I wonder whether the ICO would ever be in a position to enforce over this – it seems to me that other bodies are maybe better placed to safeguard the well-being of children in general terms. The accessibility of, say, pornography or content encouraging self-harming or drug-taking may well be detrimental and may well involve the processing of the child’s personal data, but is this rally a matter for the ICO?

It is a big ask to expect the ‘average’ service provider “not process children’s personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children”. This is very academic and theoretical in tone. Again, some practical examples would be of more value, rather than expecting service providers to research this themselves.

Provide ‘high privacy’ default settings.

This section says: “This will mean that children’s personal data is only visible or accessible to other users of the service to the extent that the child amends their settings to allow this.” It would be useful to qualify this in respect of services that necessarily involve the exchange of personal information – e.g. online game-playing or messaging.

Reset defaults to high privacy for existing users.

This section says: “You should reset existing user settings as soon as is practicable, and in any case within [x] months of this code coming into force.” I question whether choices an individual has made previously should be overridden just because a code of practice has been issued. This also seems inconsistent with the statement a couple of points above that says that existing privacy choices should be maintained where there is a software update. If you mean reset the settings in cases where the user has not set their preferences already, then the code should make this clear.

Identify what personal data you need to provide each individual element of your service.

The general approach here – i.e. breaking down a service into its component parts and assessing ‘necessity’ in respect of each one separately, over-complicates matters and raises the question of how granular you have to be in terms of breaking a service down into its various components. It might be better to approach this from the perspective of only collecting personal information in so far as this is necessary – overall - to provide a particular service.

This section states: “The GDPR requires you to be clear about the purposes for which you collect personal data, to only collect the minimum amount of personal data you need for those purposes and to only store that data for the minimum amount of time you need it for. This means that you need to differentiate between each individual element of your service and consider what personal data you need, and for how long, to deliver each one.” The logic here does not work if the need to differentiate between each element is triggered by difference of purpose. A service may have various elements, but it in most cases the delivery of each of these elements will involve personal information being processed for the same over-arching purpose. The idea that a service involves personal information being processed for a range of different purposes and that each of those purposes has a different ‘necessity’ requirement is unrealistic and over-complicated.

Give children choice over which elements of your service they wish to use.

This section argues that where a service consists of different elements, these have to be ‘unbundled’ and a child allowed to pick x but not y and z. It is perfectly acceptable for the various elements of a service to be ‘bundled’ together provided there is transparency around this and clarity of choice. This section also seems to be going beyond the requirements of data protection law, which says nothing about giving individuals the ability to choose different elements of a particular service. Similarly, it should be acceptable to offer additional purposes or service improvements / enhancements provided there is transparency around this. I would also contest whether the additional processing personal information done to provide an enhancement to a music download service, for example, involves processing personal information for a different purpose. Surely the overall purpose is the same even though the data processing may be additional or different?

Parental controls.

See my comments about this above. At least the code is clear in that the default position is that if a child’s location is being monitored then the child has to be made aware of this. The code is not clear as to whether a child, once told that monitoring is taking place, should be able to turn it off (even if his or her parent wants it to be kept on). However, there are various problems with this position. If a child is very young or otherwise lacking mental competence, will he or she understand what the notification means and the implications of being geo-located? I doubt it - in which case this would make the notification exercise pointless. However, this also touches on the point I have already raised about the degree of control parents (et al.) should be able to exercise over the monitoring of their children and the degree to which children should be made aware of this. It could be perfectly legitimate for a parent (et al) to want to monitor a child without his or her knowledge, for example where there is a suspicion that a child is being bullied and his or her knowledge that monitoring is taking pace could lead to the monitoring being turned off and therefore the scene of the bullying and its perpetrator not being revealed. The role of parents is in general not given enough prominence in this code.

This part of the code says: “Children who are subject to persistent parental monitoring may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the child matures and their expectation of privacy increases.” This runs the risk of telling parents how to carry out parenting and persistent monitors could be seen as being protective and a rational response to, what is for many children, a dangerous world. Parenting has always been about parents trying to find out where their children are and what they are doing. The idea that parents should not be able to find out where their children are because of data protection law seems to be subverting an age-old convention which has generally worked well. The code here says that a child’s expectation of privacy increases as they mature. Is there any evidence for this? If anything, children’s expectation of privacy should decrease as they are expected to provide more of their personal information increasing numbers of third parties and are subject to greater monitoring (school, employment), for example. It’s a nice idea that people expect more privacy as they get older, but I don’t think it’s true.

In general, this part of the code is seeking to extend data protection too far into the essentially private area of the child-parent relationship. The idea that service providers should “provide parents with information about the child’s right to privacy under the UNCRC and resources to support age appropriate discussion between parent and child” is very unrealistic and goes way beyond a service provider’s legal duties under data protection law.

The idea that children ages 0-5yo should be provided with audio or video materials to explain that their parent is being told what they do online to help keep them safe is also very unrealistic.

What do we need to do to meet this standard? Differentiate between different types of profiling for different purposes.

It would be helpful to clarify which age of child this advice is relevant to. I suggest that most children, and indeed many adults, would not understand what 'use my browsing history to provide me with age appropriate advertising material' means.

Use pro-privacy nudges where appropriate.

I accept that 'nudging' can be essentially unfair (in DP terms and more generally) because it distorts the choices that children are given. However, the problem here is the 'nudge' technique itself, not necessarily its consequences. Therefore, I think it is unfair to 'nudge' children in order to encourage them to make pro-privacy choices. Any such choices should be based on fairness and transparency, so a child has clarity of choice. The child should not be 'nudged' in either a 'good' or a 'bad' direction in terms of choices about privacy, or anything else.

When do we need to do a DPIA?

This section says that: "In practice, this means that if you offer an online service likely to be accessed by children, you must do a DPIA." This is very over the top, especially given the interpretation of 'likely to be accessed by' set out earlier in the code. If taken literally, this could mean that in effect every online service has to be subject to a DPIA, given that – according to the rather unconvincing logic of the code – even if only a small proportion of a service's users are children this means it is 'likely to be accessed by children'. Part of the problem here emanates from the ICO's own schedule of situations that require a DPIA. The relevant text explains – in the context of 'high risk' – that "Risk in this context is about the potential for any significant physical, material or non-material harm to individuals". It then goes on to list "Targeting of children or other vulnerable individuals: the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children" as being situations in which a DPIA must be carried out. However, the ICO's document fails to explain why offering online services directly to children necessarily has the potential for any significant physical, material or non-material harm to be caused to children. Surely the risk depends on the nature of the service, the child and other relevant factors. However, both the ICO's 'When do we need to do a DPIA' document and this part of the code go far beyond the intention of the GDPR itself, where the carrying out of a DPIA is triggered by the likelihood of a high risk to rights and freedoms of individuals. It is very difficult to justify the position of any service being offered directly to children being likely to present a high risk to their rights and freedoms.