Bates Wells

Response to ICO's Consultation on the Age Appropriate Design Code

Bates Wells hosted a roundtable discussion on 13th May 2019 to discuss the draft Code. Representatives from the Children's Society, the Guide Association (Girlguiding), Field Fisher LLP, Peat Fire Studios, the Internet Advertising Bureau UK, the Royal Foundation and the National Deaf Children's Society were present. This response draws on the discussions from the roundtable.

Section 1. Your Views

Q. 1. Is the 'About this Code' section of the code clearly communicated?

No. We do not consider that the status of the Code in practice is sufficiently clear. This section sets out both that the Code is a key measure of compliance with data privacy law (such that not following the Code may invite regulatory action from the ICO or be used as evidence in court proceedings), but also states that the Code amounts to practical guidance. We consider that there is a need for greater clarity about the purpose of the Code – either an actionable set of rules made under section 123 of the Data Protection Act 2018 ("**DPA**"), or a set of practical guidelines.

Drawing up the Code by reference to the United Nations Convention on the Rights of the Child (UNCRC) leads to potential confusion with specific provisions in the GDPR which relate to handling children's data - the UNCRC defines a child as any person under 18, while the GDPR allows Member States to legislate that children of 13 years of age or over can provide valid consent to their own personal data being processed in certain circumstances. The Code should be clear about its relationship with other key data privacy and child focussed regulatory requirements.

Q. 2. Is the 'Services covered by this Code' section of the code clearly communicated?

No. We do not consider that the Code defines in sufficient detail which websites will be affected and which will not. Given that, by the Code's own admission, an ISS means, in effect, most online services; how "likely" does it need to be that a child may access an online service? Does the concept of "likelihood" require a probability of access by a child, or any possibility; no matter how remote? In theory, the number of websites (and the amount of services available via each website) which could be materially affected by the Code is enormous, entailing a significant amount of work for service providers.

The scope of the applicability of the Code is not wholly clear. Does "likely to be accessed by children" mean that there is a reasonable probability of access; that it is more likely than not on balance that a child will access the services; or that there is any possibility of access by a child, no matter how remote? In practice, it is also difficult to ascertain whether a service is "likely" to be accessed by children because of variable factors such as age, levels of technical sophistication and levels of interest in IT and online activities compared to other pursuits. It may be that only a few children from a wider group are interested in a particular niche online service - does this mean that the website is

likely to be accessed by children? For instance, a child may search online for information about an activity he or she is interested in – say, a children's outdoor activity club – and land on the main website of that organisation which is designed to be read by adult donors and adult volunteers etc. and not primarily designed to be read by children. Does that website, because part of its main mission is to provide activities for children, need to anticipate that a child could perform a general online search and therefore be likely to access its main website? It would be helpful if the ICO could provide concrete examples of when an ISS is not likely to be accessed by children.

In practice, how can an organisation demonstrate that its website is only likely to be accessed by adults? There is only a limited amount of content which is clearly understood to be intended for an adult audience, and, in reality, children often access website content which is stated online to be restricted for adult consumption. The Code touches on a wider debate concerning how individuals validly prove their identity in the online world. The Code intimates that organisations will be required to verify identity (and therefore an individual's age) but does not take sufficiently into account the significant impact on the user experience.

The Code puts the onus on online service providers to ascertain whether the service offered is likely to be accessed by children – we consider that the Code should provide more practical guidance on ways in which online service providers can judge likelihood of access by child users. For example, are they expected to carry out targeted market research? Are online service providers entitled to carry out user surveys on their websites soliciting information as to users' ages, and are they entitled to rely on that information (for example, may precocious users who wish to access content which may be inappropriate for their age have an incentive to misrepresent their personal information?). Our consultation with industry representatives indicates that most online service providers do not know how old their users are, and the amount of work involved/ the process by which users' ages could be reliably identified would not be straightforward. What are the expectations, for example, on more generic or generalised websites, which are not aimed at specific age groups? Are they expected to take a more conservative approach that children might access the relevant service, no matter how remote the possibility?

We suggest that the ICO considers a "de minimis" personal data threshold, under which the Code does not apply, or an exemption for inadvertent/ incidental processing of children's personal data. We also suggest that the Code sets out practical examples of how an online service can satisfactorily demonstrate that it is only intended for use by adults (unless it is obvious from the nature of the content).

In addition, we suggest that the Code clarifies the extent of the definition of "service". For example, whether it applies to "information-only" websites which, at most, only collect more "passive"/ less sensitive personal data such as IP addresses, or whether its focus is on profit-making enterprises. For example, arguably charities collecting donations from children and young people are not really providing a "service" in the strictest sense. What about examples of service provision which are clearly intended to benefit children, such as online textbooks or assessment services used by schools? In general, it would be helpful to have more clarity on whether any transactions or arrangements are excluded from the scope of the Code.

Q. 3. Have we communicated our expectations for this standard clearly?

(1) Best interests of the child

No. Section 123 DPA provides that "*in preparing a code or amendments under this section, the Commissioner must have regard to the United Kingdom's obligations under the* [UNCRC]". We consider that the Code could be guided by the standards of the UNCRC more consistently, setting out a number of rights that children have regardless of any harm that may result from use of online services. The Code indicates that the 'best interests of the child are whatever is best for that individual child'. This implies that the service provider needs to understand the circumstances of a particular child in order to act in their best interests, which introduces a very high bar.

As a more general point, we consider that the ICO might usefully provide more guidance as to what is considered/ what online service providers are entitled to assume is in the best interests of children (if they can be treated as a group rather than individually). It is a subjective concept (both in the eyes of child users and online service providers) and there are different levels of interpretation – some online service providers may prefer to adopt a "bare minimum" approach in order to reduce disruption whereas others will take a more conservative approach. For example, ensuring good safeguarding practice or minimising the risk of any instances of abuse are generally agreed to be in the best interests of children. Further practical examples in the Code would assist.

(3) Transparency

No. We note that the Code highlights the application of Articles 13 and 14 GDPR to online services, but recommend that the Code also directs readers to the provisions set out in Recitals 60 and 61 GDPR, in particular:

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

If an online service for children above the age of 13 is provided, it would be useful if the Code clarified whether the service provider must provide two privacy notices for the two different age range groups.

We also recommend that the Code includes targeted provisions to children with specific needs in relation to transparency; for example those who are visually impaired or those with relevant educational needs.

(6) Default settings

No. The Code uses the term "*compelling reason*" in relation to the provisions on default settings.

While we understand the ICO's approach in requiring online service providers to justify their proposed use of children's personal data, we consider that it would be useful if the Code defined, or provided examples of, what amounts to a "compelling reason" and particularly how this is assessed when taking account of the best interests of a child. .

(8) Data sharing

No. The Code repeatedly uses the term "compelling reason" in relation to the provisions on data sharing. While we understand the ICO's approach in requiring online service providers to justify their proposed use of children's personal data, we consider that it would be useful if the Code defined, or provided further examples of, what amounts to a "compelling reason".

We also consider the Code does not make it sufficiently clear that it is only permissible to share a child's personal data with third parties to the extent that it is necessary to do so in order to provide the service that the child wants to use.

In addition, the ICO may usefully consider the situation of online services which need to share personal data as part of their primary function. Would this constitute a sufficiently compelling reason to share children's personal data?

While it is implied, it would be helpful if the Code is clear that this standard does not prevent data sharing with third party processors. Additionally it would be useful if data sharing was considered acceptable to third parties who are law enforcement agencies or in circumstances where a controller needs to defend itself.

(9) Geolocation

No. The Code repeatedly uses the term "*compelling reason*" in relation to the provisions on geolocation. While we understand the ICO's approach in requiring online service providers to justify their proposed use of children's personal data, we consider that it would be useful if the Code defined, or provided examples of, what amounts to a "compelling reason".

In addition, while the Code recognises that children's geolocation data is particularly sensitive and requires more protection, as currently drafted it does not address the full range of ways that online services collect geolocation data; for example mobile phones which store locations of photographs taken and uploaded to, or online comments/ posts made on, social media. Bearing in mind the sensitivity of the data, we consider that the Code should set out that if a child has not given an online service permission to process their geolocation data, the Code should prohibit that service from collecting the relevant child's geolocation data from other sources (as opposed to collecting the geolocation data from the child him or herself).

(11) Profiling

No. The Code repeatedly uses the term "compelling reason" in relation to the provisions on profiling. While we understand the ICO's approach in requiring online service providers to justify their proposed

use of children's personal data, we consider that it would be useful if the Code defined, or provided further examples of, what amounts to a "compelling reason".

Taking a more general approach, we consider that there is a risk that the Code will be interpreted to provide that any profiling of a child may not be in his or her best interests, even if it is actually beneficial, convenient or desired by the relevant child.

(13) Connected toys and devices

No. We recommend that the Code includes a more specific definition of a connected device and examples, including reasons why certain devices may come within the scope of the Code and why others may not.

(15) Data protection impact assessments

No. It is not entirely clear whether a child data-specific DPIA needs to be carried out as well as a wider DPIA for online services that are relevant to individuals of all ages and require a DPIA, or whether DPIAs should have a specific section to cater for the risk or likelihood of processing children's personal data.

As a general comment, as currently drafted the Code seems to suggest that, in effect, if an organisation offers an online service which is likely to be accessed by children, then it must carry out a DPIA. Given the potential breadth of the term "likely to be accessed by children" (as discussed elsewhere in this response), there is a risk that organisations consider themselves required to carry out a DPIA whenever they provide an online service which may be accessed by children (no matter how remote that possibility of access). We consider that this is an onerous requirement, especially bearing in mind the narrower scope of Article 35 GDPR and the ICO Guidance on DPIAs.

Q. 5. Do you think this standard gives rise to any unwarranted or unintended consequences?

(1) Best interests of the child

Yes. We consider that the Code does not give enough consideration to how online services should take into account, safeguard and meet additional vulnerabilities and needs that children with special educational needs or disabilities, children in care or children with mental health issues face when using online services.

As a general comment, we consider that the Code effectively sets out that processing children's personal data automatically constitutes a high-risk processing activity.

(6) Default settings

Yes. Requiring online service providers to implement "high privacy" settings by default, unless they are able to demonstrate a compelling reason for a different default setting, is a significant and

potentially onerous requirement which, while well-intentioned, can end up disrupting the user experience. In addition, a requirement on a service provider to return to default high privacy settings at the end of a session or for each different section of a website/ related service may result in a less appealing user experience, which may undermine legitimate commercial or other operations.

We recommend that the ICO considers in more detail that children at the more advanced age ranges may be sufficiently technically sophisticated to change their default settings and understand the significance of doing so. The Code should find a balance between protecting children with privacy settings, recognising children's right to choose their own privacy settings (where appropriate to do so) and online service providers' right to inform children that they can amend their settings to access different or enhanced content (without unduly incentivising that option).

(7) Data minimisation

Yes. We consider that the Code places too much emphasis on data minimisation as compared to the purpose limitation and storage limitation principles. What online service providers do to understand the limits on how they can use children's personal data, and how they implement that understanding, is equally as important in relation to purpose and storage limitation as in relation to data minimisation.

(8) Data sharing

Yes. We consider that the relevant provisions in this section are at variance with the summary provision itself. The Code states that "*you should not share personal data if you can reasonably foresee that doing so will result in third parties using children's personal data in ways that have been shown to be detrimental to their wellbeing*". By comparison, the summary prohibits the sharing of personal data unless there is a demonstrable "compelling reason" to do so.

We also consider that "compelling" reasons is a high threshold. Taken at its literal interpretation, there is a risk that having to meet this standard – i.e. to only share children's personal data where there is a compelling reason to do so – may unintentionally exclude ordinary, reasonable and/or legitimate commercial or other operations. Arguably, there is a conflict in required standards when comparing the Code with the GDPR, which allows controllers to process personal data (sharing being a type of processing under the broad definition in Article 4(2) GDPR) where it is in their "legitimate interests" to do so. A requirement to have a "compelling reason" to share personal data appears to be a higher standard than a requirement to have a "legitimate interest". This comment also applies to other aspects of the Code where "compelling reasons" is the applicable threshold.

(15) Data protection impact assessments

As the standard is drafted currently, there is potentially a requirement for all online service providers that cannot provide evidence that their online service is not likely to be accessed by children, to be required to carry out a DPIA.

Q. 6. Do you envisage any feasibility challenges to online services delivering this standard?

(1) Best interests of the child

Yes. While online service providers may be able to source, and then provide, evidence of what is in the best interests of their, for example, customers, beneficiaries or constituents, requiring them to define, and then apply, an approach in the best interests of the child may require them to take more into consideration than is relevant to the service they provide.

(2) Age-appropriate application

Yes. We consider that the Code needs to be more realistic and flexible in recognising that, while it is possible to establish online servicer users' ages in a privacy-friendly manner which does not have to disproportionately impact the user experience, widespread age verification and assessment is not yet the norm. The Code should give examples of available mechanisms, along with practical explanation, and set out which such mechanisms may be of particular use in particular situations.

(3) Transparency

Yes. It will not be straightforward in practice to provide the information required in a way that such a wide range of ages can understand (on the basis that any person under the age of 18 is considered a child for the purposes of the Code). As currently drafted, the Code sets out five different age ranges of children – does this mean that, on top of an online service provider's privacy notice intended for adults, it needs to produce up to 5 separate additional privacy notices depending on an analysis of how old its users may be?

(8) Data sharing

Yes. The way in which some online service providers share personal data is opaque – sometimes this opacity is deliberate to try and circumvent obligations under applicable law which service providers consider may undermine profitability. While we consider that the ICO is entirely correct to focus on the privacy risks of sharing children's personal data, we consider that the Code faces a tall order in tackling the lack of transparency in sharing, or to implement practical barriers to prevent data sharing where it is unfair to do so.

(10) Parental controls

Yes. Industry representatives we have consulted raised concerns about whether it is appropriate for them to decide what content should be subject to parental control – different parents will take different approaches to what types of content their children should be able to access, depending on the approach they personally take to parenting. Some parents may have a more liberal approach than others. Seeking to make judgments in this area may alienate user bases including both children and parents. The ICO may usefully consider clarifying the issue with examples of a range of different options.

(12) Nudge techniques

Yes. Nudge techniques are ubiquitous online and differ between those that are benign or useful to children and those that deliberately encourage children to make decisions which are not necessarily in their best interests. We consider that it would therefore be useful if the Code set out examples of nudge techniques that are prohibited by the Code, in express comparison to those which may be useful to a child, or at least harmless. As presently drafted, the Code does not appear to recognise that there is value and benefit in personalised content and advertising.

We also consider that there may be an unintended conflict with the GDPR and applicable e-privacy law here. Organisations are required to seek users' prior opt-in consent (to the standards required under Article 4(11) GDPR) to send them electronic direct marketing. Given that direct marketing has such a broad definition under section 122(5) DPA, there is a risk that implementing unduly onerous terms in relation to nudge techniques may invalidate consent previously obtained to send electronic direct marketing – content such as newsletters or charitable requests for funds, when unsolicited, may be considered as nudge techniques bearing in mind their purpose. We consider that the ICO may usefully consider clarifying this point by providing that, for the avoidance of doubt, the provisions of the Code on nudging techniques do not require updating previously obtained consents under the GDPR.

Q. 7. Do you think this standard requires a transition period of any longer than 3 months after the Code comes into force?

We have approached this question on a more general basis instead of identifying particular implementation periods in relation to the 16 separate standards. Section 123 DPA allows for a transition period of up to 12 months, but the Code as currently drafted implies a shorter transition period. We, and industry representatives we have consulted, consider that anything shorter than 12 months is optimistic. As set out throughout this response, as currently drafted, the Code will apply to the vast majority of online services and websites, and will require operators to undertake significant research followed by significant additional compliance action.

Some industry representatives we consulted asked whether the ICO would contemplate allowing a "sandbox" implementation strategy, where it analyses test cases of organisations applying the requirements of the Code and trying to mitigate the risks associated with processing children's personal data, and seeing how the process works on a practical level.

Q. 9. Is the "Enforcement" section of this Code clearly communicated?

No. We consider that it would be useful if the ICO agreed to consider intent when assessing compliance with the Code. The Code (as currently drafted) is very broad, applying to many different types of website, online services and potentially new technologies.

Depending on whether the ICO intends the Code to be an actionable set of rules or less strict guidelines, we consider that it would be useful that the Code states that providers of online services should have regard to the intent of the Code, as opposed to the strict provisions of the Code. We consider that this would represent a more realistic approach to promoting compliance and good

practice.

In addition, the ICO makes clear in its draft Regulatory Action Policy[1] that it will take a fair, targeted, reasonable and proportionate approach to enforcement. In general, we recommend that online service providers are expected only to expend reasonable and proportionate effort (judged by their individual circumstances such as financial/ personnel resources and risk of harm bearing in mind the nature of personal data processed and context/ purpose of the processing activity) in complying with the Code. We consider that this would be a more realistic approach to promote compliance and good practice – if it transpires that stricter standards need to be imposed, these can always be imposed in the future.

In particular, we recommend that the ICO sets out in the Code that it will consider relevant factors such as (i) vulnerability of individuals affected, (ii) the nature of technology available, (iii) whether an organisation's contravention is intentional, wilful or negligent and (iv) an organisation's history of compliance with data privacy law.

We also consider that, when implemented, the Code needs to ensure space for legitimate commercial activity.

As a general comment, we (and industry representatives) are concerned that the Code seeks to apply more onerous obligations than under the GDPR. This may have unintended and wide-ranging consequences, for example invalidating (or rendering out of date) reasonable and proportionate efforts taken by online service providers in good faith to comply with their obligations under the GDPR. Is it the case that, where there is a conflict between the Code and the GDPR, the provisions of the Code take precedence? Industry representatives we have consulted suggest that there is a risk that they are required to "go back to the drawing board" and consider implementing *another* layer of data privacy law compliance which may conflict with current rules with which they are already trying to comply.

Q. 11. Are there any key terms missing from the "Glossary" section?

Yes. While this does not necessarily need to be a specified term, the Code should make clear that data inferred or derived from a child's personal data is also considered personal data, and therefore subject to the provisions of the Code.

Q. 17. Do you think any issues raised by the Code would benefit from further (post-publication) work, research or innovation?

Yes. The Code (correctly) refers to non-screen-based online services and connected devices. In the future, there will undoubtedly be more examples of online services which are not screen-based (in particular with the increased daily prevalence of the internet of things). We consider that the Code should also apply to such services, to the extent that they involve processing children's personal data, but that research and further consideration may be required to work out how the Code can apply to such technologies on a practical level.

To the extent it has not done so already, the ICO also may usefully undertake research into how

[1] Currently subject to Parliamentary consultation and approval

online relationships between service providers and children function on a practical level. The current draft of the Code arguably assumes some sort of account-based relationship between service providers and child users, including established privacy settings or interfaces like a dashboard, in a way in which service providers can attribute an identity to most users. Our consultations with industry representatives suggest that this is not true of most websites, and websites frequently have relationships with users that are not account or profile related.

Section 2. About you

From the ICO's list in its Code consultation document, the most applicable category is 'other'. Bates Wells is a professional services firm, combining a top UK 100 legal practice with consultancy services in impact measurement, outcomes-based planning and strategy, and financial services regulatory compliance. We work with a wide range of clients across a variety of sectors, but we have a particular focus on charities, social enterprises, public bodies, innovative start-ups and high-profile individuals.

Bates Wells

31 May 2019