children's charities' coalition on internet safety

Comments on the ICO Code of Practice on Age Appropriate Design for Online Services

Foreword

We are aware that different parts of the internet industry are at present lobbying the Government and the ICO with a view to securing a significant delay to the implementation of the Code of Practice on Age Appropriate Design. There is a widespread fear that the request for such delay is principally about giving commercial interests an opportunity to renegotiate, dilute or abandon key concepts contained in the Code. We urge the Government and the ICO to resist these blandishments.

Childhood is short but the impact of negative experiences in childhood can last a lifetime. In the many years of their existence some of the firms urging delay had ample opportunities to address the matters raised by the ICO Code. They chose not to act or at any rate failed to and it therefore seems doubly unfair and highly unreasonable that they should now be seeking to kick the can further down the road, particularly if the undeclared agenda is really the abandonment or substantial modification of key principles contained in the ICO document. There was a substantial period of consultation before the ICO published its current proposals.

It is accepted there will always be a need or scope for clarification of a text but anything beyond that should be stoutly resisted. A short timetable for completing any outstanding discussions necessary to clarify or illuminate the code should therefore be established as soon as possible. Only matters of detail and implementation should be on the table. Once the Code is finalised a reasonable commencement period can be agreed to give companies time to adjust their internal systems and settings.

In the end it will be a business decision for each of company to decide whether or not to bring themselves into compliance with the Code. We are confident that a sufficient number of businesses will choose to comply and that a healthier and rich online environment for children will be the result.

Introduction

The internet began its life as a small "adults-only" environment populated exclusively by scientists and technologists. There was a high level of trust and mutuality of interest among the early pioneers. In a famous Ted Talk, given in 2013, Danny Hillis brandishes a booklet published in 1982. It is a slender volume containing the names, addresses and telephone numbers of everybody in the world (literally) who had an email account. There were two other Dannys listed. Hillis knew them both.

At some point in the early to mid-1990s, following the release of the first web browsers, the internet began its long march towards the mass market. Yet in some influential circles much contemporary discussion about the devices and services which connect to or use the internet remains rooted in the idea that all users are fully competent, literate, numerate adults who could have been one of the three Dannys. If they aren't, they *ought* to be and it is somebody else's, everybody else's, responsibility to deal with the consequences of that unfortunate fact.

Any attempt to accommodate the presence of a "non-Danny" is regarded as introducing an imperfection, an irritating, resented departure from the purity of the original idea.

However, in 2015 for the first time it was documented that children make up 1 in 3 of all human users of the internet. It hovers around 1 in 5 in the richer countries such as the UK but soars to approximately 1 in 2 in many lower income nations. Children are now an important, substantial and ever-present constituency in cyberspace.

The modern internet is much more like the High Street than it is the adults only space of yesteryear. Yes, you can wander off the High Street into adult places such as pubs, clubs and betting shops but on the main thoroughfares certain rules and conventions are well established and, though disliked by a small minority, are accepted by the vast majority of people. That is where we now need to be in respect of the internet. The arc of public policy is moving in that direction worldwide. Not before time.

It is important to establish a new narrative, one that proceeds from a recognition that, among several other important things, the internet now functions as a consumer product or service which is intimately and unavoidably enmeshed in family life and therefore in the lives of children.

Being in consumer markets brings with it a set of expectations that are far from being met at the moment. To the extent adults have different or additional rights or needs in relation to the internet as compared to children then, of course, they should be provided for. What is important, though, is to get away from the practice which to a large degree has existed hitherto where the position of children as users of a device or service is only thought about following a calamity of some kind.

Every technology company needs to adjust the way it thinks before *"putting it out there"*. Back in the 1990s Professor Ross Anderson of Cambridge University's

Computer Laboratory said (page 2) a typical attitude was *"ship it Tuesday, fix it by version 3"*. Whatever view one took of that then it surely has no place in a world where children are known to be present at scale. Yet it persists, finding a modern echo in the famous dictum of Mark Zuckerberg *"move fast and break things"*, or his updated version*, "the fast shall inherit the earth"*. These are metaphors which give businesses permission to be careless and, in respect of children, they rest on the assumption that the burden for policing their products is shared equally or to a substantial degree with parents and teachers. The legal or economic incentives to be careful have been absent up to now. On the contrary, the legal protections provided by platform immunity and the economic incentives provided by capitalising on "network effects" point in exactly the opposite direction

The ICO's draft Code of Practice on Age Appropriate Design, taken together with the contemporaneous consultation on Online Harms seem to point the way towards a better kind of internet where children are never an afterthought. That is how it should be.

Response to individual questions:

1. Best interests of the child

It is important to begin by making an important conceptual distinction.

Historically, the *"best interests of the child"* were typically discussed in the context of emphasising the importance of avoiding a risk of harm to a child or as the basis of an expectation that provision will be made to guarantee, for example, a child's health, education or other benefit.

However, the GDPR and the Digital Economy Act, 2017 make clear children have a right to privacy which is not contingent upon other considerations. Failure to honour or observe a child's right to privacy within the bounds of the law is unlawful in and of itself without more.

Where a failure to honour a child's right to privacy in fact leads to harm then the consequences for the business or other organization responsible for the breach will be commensurately more serious but that is a different point.

The obligation to consider the best interests of the child, including their right to privacy, exists in respect of every developer or online business wherever they are in the value chain. Every developer or online business must or ought to know that the internet is a mixed environment in which children are present in large numbers. Unless they take active steps to prevent children from accessing their service, they must assume they will, in which case they must also consider the child's right to privacy and more generally how to act in their best interests so as to avoid the risk of harm.

Owners of online services are entitled to expect that a child's parents or carers will be engaged in protecting their children from potential harms and in protecting their right to privacy, but they are not entitled to delegate that responsibility entirely to them. There is no reasonable basis on which the developer can assume a parent or carer will have as much or more knowledge of the service than they as the producer of it did. Within the technical environment these businesses have constructed they should do everything they reasonably can at the design level to minimise the risk of foreseeable harms and to safeguard a child's right to privacy.

Mutatis mutandis similar considerations should be applied to manufacturers of a great many devices which can connect to the internet. Perhaps that is implied in everything in the Code – because devices generally provide online services of some sort, if only to allow them to be used – but it is worth making that explicit.

2. Age appropriate application

The general drift of policy is pointing towards online businesses having a greater obligation to know who their customers are.

Would it be too harsh to say that if internet businesses had already been sufficiently incentivised, they would have found a way to determine a person's

age and they would have done it in a heartbeat? We don't think so. Could the law create such an incentive? Yes it could. This Code could.

Please do not misunderstand what is being said here: there is no general case to be made to say every internet user should be age verified, either in relation to risks of harms or in relation to privacy issues. In relation to children everything hinges on the risk assessment and that is true both under the GDPR and under the Digital Economy Act 2017. Nevertheless, as age verification tools improve, responsible businesses should find it easier to satisfy themselves that they are making appropriate arrangements to meet the safety and privacy needs of their users.

Beyond that we endorse the views set out in the ICO Code.

However, we think there is an urgent need for the ICO to issue authoritative guidance on whether or to what extent, in what circumstances, it is permissible to use "legitimate interests" as the basis of processing data where under 18s and under 13s are concerned.

3. Transparency

The Code gives insufficient attention to or provides insufficient guidance in respect of children with special needs or vulnerabilities, including children from linguistic minorities in a given territory.

Beyond that, without being overly prescriptive, while it should always be possible for any actual or potential customer to see the full range of a site's terms and conditions, and be able to find a full explanation of the way in which the site or service works (in particular with respect to its data sharing practices and information about how the data it collects are used) each site or service should be obliged to ensure it presents information in a way that is likely to be understood by the full range of its users. Even if a parent signs up a child for a service, the company should ensure, as far as is reasonably possible, the child is able to understand the environment. With apps designed for the pre-literate young that may be difficult or in some cases impossible but that does not detract from the general principle.

4. Detrimental use of data

If the guiding principle is the best interests of the child, there should never be any detrimental use of children's data. If the developer has permission to pass on data to a third party, they must make that fully clear to their users, accepting full and joint responsibility for its subsequent use by the third party.

5. Policies and community standards

Companies in the online space should be under an obligation to stay up to date with technical developments which would contribute to making children's experience of the site or service safer or more respectful of their privacy rights.

Elsewhere we refer to the importance of companies not unfairly exploiting children's naivety about the commercial background against or within which they are operating.

More widely, it is important that a company can show that it is making every effort to enforce its own state terms and conditions of service. Absent that this reduces terms and conditions to mere marketing material. Parents and children are entitled to look at service's terms and conditions and rely on them as an indicator of the kind of environment they will find if they use the service.

6. Default settings

Every app or service should be set to the highest level of security, safety and privacy by default. Parents, carers or children themselves should not have to jump through hoops to make something as privacy respecting or as safe as it is possible for it to be. There should be scope to liberalise, weaken, perhaps in certain circumstances even to abandon altogether, protective measures that are pre-installed, but it should be that way around.

We know from research that the default settings of any device or app are hugely important not least because inertia, ignorance or a lack of confidence or literacy mean that a great many users will never change the defaults.

We also know from research e.g. from the Norwegian Consumer Council that difficult to understand or find settings can "nudge" or trap people in ways which encourage greater disclosure of data. These techniques are designed to enhance the profitability of the business. They are not designed with the best interests of the child in mind or with the privacy rights of the child in mind. They are therefore unacceptable.

In addition, at the initial sign up or default stage it should be fully transparent to the parent and the child what the full cost implications are of engaging with the app or service. This is to avoid drawing a child or a family into a service which only becomes truly usable or enjoyable, or which can only be completed, if significant additional sums of money are expended.

7. Data minimisation

There is something that doesn't feel quite right about companies that have made their fortunes by sucking in as much data as possible, often against a background lacking in transparency, now pleading fidelity to the principles of data minimisation as a reason for refusing to maximise their efforts to enhance the rights and safety of children. This arises particularly acutely where the issue of age verification is under discussion.

Granted the new rules on data privacy are in part a product of, and are meant to be a corrective for, the previous lack of clear regulations, but we trust we are not alone in remarking on the irony of children being victims of the earlier age of excess now continuing to be disadvantaged by a new era of parsimony.

8. Data sharing

It is vital it is made clear that "inferred data" is nonetheless personal data and that there is full transparency surrounding the purpose of processing and any sharing that might take place.

See also our comments on "Detrimental use of data."

9. Geolocation

The Code gives insufficient attention to the full range of ways in which geolocation data can be collected e.g. from EXIF data, "check-ins" and WiFi connections. It is exceptionally hard for many adults to understand how some of these types of services or parts of Apps work, so it is doubly challenging to ensure children do and to ensure children's rights to privacy are not compromised through their operation.

We welcome the suggestion that when a child navigates away from or logs off from a service that uses geolocation data that the collection of geolocation data from the service is terminated but this may be nugatory if other mechanisms continue to collect and transmit geolocation data.

Whenever geolocation is in use there should be a visible and easily comprehensible reminder of that fact. It should not be possible easily to disable, hide or switch off such a reminder on any device or app that is used by a child and if there are circumstances where it is in the best interests of the child for the reminder to be disabled these should be carefully explained and justified otherwise it will raise a presumption that whoever was responsible for the concealment was acting against the best interests of the child.

The circumstances in which a child's whereabouts, either current or historic, are disclosed to any third parties need to be fully explained and justified. As ever, the best interests of the child should be the prevailing and dominant consideration.

Otherwise we broadly endorse the recommendations in the Code.

10. Parental controls

We endorse the recommendations in the Code. In particular it is important to emphasise the provision of parental controls will likely always be undertaken as a voluntary measure by access or service providers. In general, it will be possible to modify or abandon key settings. This means the service provider needs to think carefully about their own independent obligations to the child. They should not imagine that merely making parental controls available to parents, providing them with an option to deploy or not deploy them, in any way absolves them of their own obligations to children. In relation to the default settings, as previously stated, a device or service should be as safe and privacy respecting as it can be at the point of first use and it should not be

trivially easy to relax or liberalise the settings that establish the default environment.

11. Profiling

Profiling is generally associated with data collection and processing practices designed to allow advertisers to target ads at persons most likely to be interested in acting on the information the ad provides, typically by making a purchase or doing something else that favours the advertiser.

The GDPR and the Code do not say that all profiling is bad or should be banned. We endorse that position. Some profiling might lead a child to a web site or service containing information about local sports activities or other matters likely to be beneficial to the child or take them to an appropriate form of entertainment or engagement.

The guiding principle, once again, has to be the best interests of the child. It would be extremely useful if the ICO could publish detailed examples of the kind of profiling activities which would be considered beneficial and those which would be unlikely to be considered beneficial. Behaviourally based advertising to children is limited under the Advertising Standards Authority's and the IAB's guidelines but it would be useful for these limitations to be made explicit within the Code.

12. Nudge techniques

Sees comments above on "Detrimental use of data" and "Default settings"

13. Connected toys

We note that there is a consultation currently taking place on the evolution of policy in respect of the "Internet of Things". The ICO doubtless will be closely engaged in those discussions. The new "Centre for Data Ethics and Innovation" now exists. However, we note, with regret, that in the Centre's work programme for 2019/20 none of the following words appear: child, children, young. That does not mean the Centre does not intend to engage with this dimension, but it would be useful if, at an early opportunity, it could be made clear how and when it might. The ICO may wish to raise this with them.

It hardly needs saying that in respect of toys and other artefacts likely to be used by or be regularly in proximity to children the greatest clarity and stringency is required. See also our earlier reference to "inferred data".

In particular account will need to be taken of how the absence of a screen or some other child friendly user interface, could inhibit or restrict aspects of children's rights e.g. by making it difficult or impossible to update, change or control the settings themselves.

14. Online tools

We endorse the sentiments expressed in the Code.

15. **Data protection impact assessments**

In some ways this is the single most important part of the whole Code. It will be important for businesses to understand that when they think about data processing this is not a narrow construct which can be viewed simply or solely as a matter of how one, mechanically, collects, processes and stores data. Those matters are critical, but the uses to which the data are put and the consequences of that use in terms of its impact on the quality of children's lives is what lies at the heart of the Code.

Some clarification on how individual trades associations are to engage with drafting best practice codes and impact assessments tools which take account of the position of children would be extremely useful.

16. Governance and accountability

"Nothing about us without us" is a familiar idea designed to ensure that policies which impact on particular groups are framed following discussions with and research about them. The right for children to be consulted is one enshrined in the UNCRC and even though the context is slightly different the idea itself is very powerful and apposite.

It will be impossible for any business to discharge its obligations to children without having reliable information about how they interact with or are likely to interact with the services they provide or intend to provide.

A business that cannot show it has taken the time and the trouble to do its homework properly, for example by talking to children, will or ought to have a much harder time convincing the ICO or a court that it has properly discharged its obligations.

There should be scope for "super-complaints" to be brought by appropriate agencies acting on behalf of children.

---ooo---

31st May 2019.

John Carr OBE
Secretary
Children's Charities' Coalition on Internet Safety
10, Great Queen Street
London WC2B 5DD

www.chis.org.uk