Response to the Information Commissioner’s Office consultation on its Age Appropriate Design Code

Human Centred Computing Research Group
Department of Computer Science
University of Oxford
31 May 2019

This document provides the response of Oxford University’s Human Centered Computing Research Group to the Information Commissioner’s Office (ICO) consultation on its draft code of age appropriate design for children. This response is based upon our direct research experiences with children as well as our technical knowledge about the algorithms and design techniques that underpin the online services used by children that may influence their online behaviours.

This response is split into three sections. First, we briefly describe our research background. We then make general comments on the overall code, including why it is necessary and where we believe can be strengthened, followed by specific comments to areas of the code that are related to our research experience.

Section 1: Background of our research

The Human Centred Computing research group in the Department of Computer Science at Oxford University is led by Prof. Sir Nigel Shadbolt. One of our research focuses is on empowering users with better control and transparency during their interaction with digital technologies. For this, we take a human centric approach by working closely with human participants throughout our research process. Recently, led by Dr Jun Zhao, we have expanded our research, looking into the impact of algorithmic systems upon children --- what challenges and risks perceived by children when using digital technologies and how we may better support them. Grounded in extensive empirical data that we collected by working closely with children, we have identified critical knowledge gaps in children’s understanding of how algorithms may impact the information they consume and explored new design solutions that might facilitate their knowledge development and risk coping skills[1].

Our response to the Code is primarily based upon our recent research upon data tracking of mobile devices[2], and how this may impact upon adult users’ perception and need for better transparency and control[3], as well as that of young children[4].

[1] The KOALA Project: https://sites.google.com/view/koala-project-ox

[2] Binns, Reuben, et al. "Third party tracking in the mobile ecosystem." Proceedings of the 10th ACM Conference on Web Science. ACM, 2018.

[3] Van Kleek, Max, et al. "Better the devil you know: Exposing the data sharing practices of smartphone apps." Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, 2017.

[4] Zhao, Jun, et al. "I make up a silly name': Understanding Children's Perception of Privacy Risks Online." In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK . ACM, New York, NY, USA

Section 2: Overall feedback to the code

We congratulate the Information Commissioner's Office on the effort that led to this important piece of work. Overall, we believe the code is comprehensive and well-grounded upon research and evidence. We welcome the focus on children's best interests, which sets a clear target for assessing the design process and enables services to make nuanced decisions about their design choices.

We particularly support the areas of code relating to transparency, data minimisation and data profiling, which directly address the under-regulated data tracking behaviours that are widely applied to online services, but not always designed with users' best interest in mind. Children have less ability to comprehend the implications of this opaque collection of their personal data, and we have little evidence of the long term impact of data profiling on children's future digital habits and well-being. The code sets a leading example amongst existing data regulation frameworks for addressing this pressing issue.

An urgent need for the code in the UK

We believe this code meets a most urgent need for addressing the lack of control over the type of information or services children are currently exposed to.

Children are increasingly growing up in a smart society, surrounded by smartphones, smart toys, as well as smart home devices. In the UK, the age of children being exposed to digital technologies is increasingly young[5]. The latest Ofcom report shows that in the UK over fifty percent of the children aged between three and four are spending over nine hours per week online, and they are spending more time in front of their tablet computers than TVs. Although the risks of cyberbullying and cybersecurity have been widely discussed, how the algorithmic systems impact our children is much less understood. At the moment, **algorithms are carelessly implemented,** without considering the potential of children being exposed to inappropriate content online, games that are designed to promote their additions, or social media platforms that are inappropriate to their age.

Existing research has already demonstrated the possibility that algorithms can be used to infer children's personal interest and developmental stages[6], and designs of technologies can be applied to increasing addictive behaviours[7]. Our recent research has identified that children's data and their online behaviour information are often tracked by the mobile apps used by them and sent over to third-party online marketing or advertising companies without children or their guardian's explicit consent or knowledge [2]. Although research has not yet established how children's data may be used to influence the information they see online or the game promotions they experience every day, our interactions with children have shown that online or

[5] 'Children and Parents: Media Use and Attitudes Report', Ofcom, 29 November 2018

[6] Newman, Joe, and Joseph Jerome. "Press Start to Track Privacy and the New Questions Posed by Modern Video Game Technology." AIPLA QJ 42 (2014): 527.

[7] Kidron, Beeban, et al. "Disrupted childhood: the cost of persuasive design." (June 2018). 5Rights.

in-app promotions are becoming a major means for young children to identify new online content or games, which are not always designed with their best interest in mind.

Parents who have been involved in our research were surprised by the extent of tracking that occurs, and expressed a strong desire for better control and more transparency. They indicated that this is where regulatory frameworks should step in, and the code is an important part of that.

This code is therefore of great importance to the safeguarding of children operating in online environments and interacting with online services. There are nonetheless some considerations missing from the code that it ought to address.

Target audience challenge
The code describes its target audience as “relevant information society services which are likely to be accessed by children”. It also provides some exemplar services later. We found the detailed information about “When are services ‘likely to be accessed by children’?” very useful.

However, it is unclear whether all service providers should expect to provide the market research that is required in the code, to demonstrate the likelihood that the service is to be accessed by the children. This clarification could be very useful both for code validation and for SMEs and service providers with less resources, to prioritise their implementation process.

Interconnection of the code
The sixteen provisions of the code are very interconnected and inter-reliant, which can be challenging for online service providers to interpret and comply with the code. It would be helpful if the interconnection of the code is drawn out more clearly at a glance.

Consideration of families and children from disadvantaged background
We welcome the code’s emphasis on parental control and parents’ role in safeguarding their children. However, we would like to suggest that the code consider families who may not in a position to provide strong parental support for the children. If a parent or carer with very limited digital literacy skills themselves, we should also ensure children to be sufficiently supported and safeguarded even with a lack of parental support.

Section 3:
Here we made specific comments to the following codes that are related to our area of expertise:

1. Transparency

We welcome the encouragement for more transparency in relation to the use of data, and at the point that use is activated. We also welcome the implementation guidelines suggested for children of different age groups or developmental stages. However, we are concerned of
1/ the complexity of the task involved, for service providers to carry out testing for different age groups and document the testing results in the DPIA.

2/ the diversity of the actual implementation in practice, due to a lack of standardised practices, which may lead to more challenges for children and their families to comprehend, and
3/ the implication for service providers to have an age estimation component in place, in order to implement age-appropriate transparency notice.

Existing research has explored various ways of making data collection notice in a more transparent and just-in-time manner for adult users [8,9] . However, the results have shown a diverse level of effectiveness. Further, other than showing interest to know what data is being collected, users also cared (if not more) about the purpose for which information is being collected.

We suggest the code:
1/ make a clearer statement about what transparency is for
2/ make it clearer that transparency should not be an excuse for collection of data for unelicited purposes, and finally
3/ consider the need of children with special education needs regarding their ability to comprehend transparency notices and need for additional support

2. Data minimisation
   This provision of the code is highly related to the above code of transparency. We acknowledge that the collection of some personal information can be essential for the provision of some of the services, such as navigation services or ensuring our children's safety. However, our and others' research has also shown that a large amount of personal information is being collected for unknown or unnecessary purposes.

   Data should only be collected if they are required for specific purposes, and how this data will be stored, retained or access after the purpose has been served should also be made clearer to the users. If children were given a choice to permit data collection for a specific purpose, this data collection should be stopped either automatically or clearly communicated to children. The "actively and knowingly engaged" in the code is related to this scenario, however, it could be clearer.

3. Parental control

[8] Emami-Naeini, Pardis, et al. "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior." *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019.

[9] Almuhimedi, Hazim, et al. "Your location has been shared 5,398 times!: A field study on mobile app privacy nudging." *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, 2015.

Recent literature has shown that parents and children do not always believe that a parental control mechanism[10][11], which enables parents to monitor or restrict children's online behaviours, is the most effective mechanism. Parents and children prefer technologies that would promote their communications and interactions in relation to the use of technologies.

Although the current provision achieves a good balance between parental control and children's rights, by emphasising the transparency of parental control, which includes clear signposts for children regarding the control, we would recommend the code puts a stronger emphasis on the purpose of any parental control in place.

Instead of collecting extensive sensitive information and data on children, parental control should collect the minimal amount of information that is required for safeguarding children. The code should also make clearer that parental control should not be used by the service providers for any purposes.

4. Profiling

We agree that profiling should be default off wherever it is possible and appropriate to provide children with a choice, but the Code should also be clear that the profiling of children must be ***limited in general***.

This provision is closed related to Data Minimisation and Purpose Limitation, and should cross reference those sections.

Further, we recommend the current code to make clearer that children must not be profiled, unless
a) There is a strong reason that profiling is essential to the service or feature the child is using
b) Appropriate measures are in place to protect the child from any harmful effects, and
c) It is in a child's best interests.

Service providers should be urged to carefully consider the need for profiling children, and the benefits from a personalised experience and the potential harm to children.

We agree that profiling should be off by default. We would also like to see a strong emphasis from the Code that any profiling on children should be made visible in the services, and children and their parents/carers should always be provided an option to opt out.

[10] Wisniewski et al. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. ACM, 51–69.

[11] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 523.

Profiling should never be used to target children with advertising or marketing. If profiling is used to recommend children to additional online content, service providers should carefully consider children’s best interest, and avoid recommendations of content that are inappropriate to their age or likely to promote harm to their online digital wellbeing (such as addictions or being exposed to violent content).

5. Connected toys and devices

We welcome the provision for considering this rapid emerging form of technologies, which would expose children to digital technologies in a much more ubiquitous and ambient manner. Impact of the use of such technologies from a young age is little known, although risks to children’s personal data privacy have been repeatedly identified[12][13].

The Code should include a definition of connected devices, and a rationale for why certain devices are in scope and others not. Without a definition, some providers may be unsure if the Code applies to them.

We support the Code’s effort to restrict the passive collection of data by connected devices, but ‘processing’ as well as ‘collection’ must be limited. A device that needs to collect data to function in listening or stand-by mode, must be subject to data minimisation, purpose limitation, and storage limitation principles.

[12] McReynolds, Emily, et al. "Toys that listen: A study of parents, children, and internet-connected toys." Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM, 2017.

[13] Seymour, William. "Privacy Therapy with Aretha: What If Your Firewall Could Talk?." *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019.