Comments on the ICO draft Age Appropriate Design Code of Practice - May 2019

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

These comments address the ICO's draft Age Appropriate Design Code ("the Code"). They build on our September 2018 submissions. Our recommendations to the ICO are in **bold**.

General comments

We welcome the opportunity the Code presents to address the relationship a child has with online services. We support the Code's ambitions to (1) create stronger default privacy settings, and (2) work towards better provision of information to children about terms and conditions and privacy notices, preparing children gradually for adulthood as effective participants online with agency and confidence in their rights.

We further support the Code's intention to uphold children's rights and would welcome greater explicit emphasis on fundamental rights, particularly the right to freedom of expression and access to information, throughout all provisions.

Aims and objectives

We believe it would assist implementation and enforcement for the Code to set out more precisely what it can achieve. The Code states that its focus is to "set a benchmark for the appropriate protection of children's personal data." It also states that service providers should "consider the declared age of your user to help ensure you don't feed them inappropriate content for their age range." This creates confusion for industry and a serious risk that content or products will simply be removed or withdrawn from children, and potentially adults, by service providers with limited economic means to comply and/or nervous of liability.

- **The Code should explicitly clarify that it addresses the relationship between an individual data subject (a child) and a data controller (an online service), the processing that takes place of the data subject's personal data, the basis for that processing, and the responsibility a controller has to that data subject and their rights.**

- **The Code should explicitly state that it does not in intention or effect propose to limit access to online content.**

An interpretation of the Code that leads to content reduction would be an interference with children's rights under Article 19 ICCPR and other international human rights law provisions.

Scope - services and territory

We have concerns about the broad scope of the Code. Information Society Services (ISS) "likely to be accessed by children" effectively reduces to "all online services". Children do, can or may use ISS in a wide range of everyday, social and educational scenarios; consequently, there is a high risk that heavy-handed implementation of the Code could significantly restrict children's ability to engage fully in online life, including limiting personal discovery and academic research. There also seems to be little genuine space for ISS to argue that they are out of scope, with a high evidential barrier required.

- **The ICO should review the "likely to be accessed" requirement and either narrow it through further definitional explication or replace it with an alternative standard. This will ensure that the Code fulfils legal requirements to be necessary and proportionate in application, and facilitate consistent understanding and application by industry - which will in turn aid enforcement.**

The territorial scope of the Code is also unclear as the following paragraphs (page 14) appear to be contradictory:

"The DPA 2018 may also apply to some other services based outside the UK even if they don't have an establishment in the UK. If the relevant establishment is outside the European Economic Area (EEA), the DPA 2018 still applies if you offer your service to users in the UK, or monitor the behaviour of users in the UK. The code applies if that service is likely to be accessed by children.

"Under the GDPR one-stop-shop arrangements, if you have a lead supervisory authority other than the ICO and you do not have a UK establishment, this code will not apply."

These suggest that if a service with no UK link is established in a jurisdiction subject to the GDPR the Code will not apply - even if it is available to UK children; however, if an identical and identically-available service is established in a jurisdiction beyond the GDPR's reach, the Code will apply. This seems a perverse outcome.

- **The ICO should further clarify and narrow the territorial reach of the Code so that services can know with certainty whether or not they are subject to its provisions. We propose limiting territorial reach to service providers with an establishment in the UK. Such a limit would be in line with offline jurisdictional boundaries and ensure that implementation of the Code could be practically enforced - a wide territorial scope that leads to unrealistic enforcement expectations would undermine the Code's legitimacy.**

Additional points

- **We have some reservation over calls for ISS to be able to interpret the "intent" of the Code. Interpreting intent is an exercise fraught with difficulty, and can lead to divergent and inconsistent outcomes. In our view, it would not assist clarity, consistency or fair enforcement for intent to be introduced as a compliance standard.**

- **The section on data minimisation must be further explicated to clarify that the minimisation principle extends to all aspects of data processing, not merely collection.**

- **The principles of purpose limitation and storage limitation require further explication to set out more clearly the GDPR expectations.**

- **With regard to enforcement, we would welcome a renewed call from the ICO to the Secretary of State to review the UK's provisions for the representation of data subjects under Article 80 DPA, including the merits of exercising the power under Article 80(2), with a particular emphasis on the needs of children in this respect and on giving organisations representing the interests of children a formal role in representing children's above data protection rights.**

Beyond these points, we have two specific concerns to raise about the Code in its current draft form: (1) The Code's requirements as a whole will most likely in practical application lead to widespread age verification processes, which could have detrimental privacy impacts on both children and adults; (2) The Code's text does not consider with sufficient sensitivity the effect a disproportionate regulatory regime may have on a child's right to seek, receive and impart information.

<u>Protecting children's privacy</u>

ORG supports higher default privacy settings for children, and welcome provisions in the Code that increase privacy protections. We note that these can have a positive impact also on adult online experience and engagement.

Age verification impacts

Section 2 states that ISS providers must "apply the standards in this code to all users, unless [they] have robust age-verification mechanisms to distinguish children from adults."

We are severely concerned that in practice the Code will result in widespread age verification across websites, apps and other online services. The ICO contends that age verification is not a 'silver bullet' for compliance with the Code, but it is difficult to conceive how online service providers could realistically fulfil the requirement to be age-appropriate without implementing some form of onboarding age verification process.

The practical impact of the Code as it stands is that either all users will have to access online services via a 'sorting' age-gate or adult users will have to access the lowest common denominator version of services with an option to 'age-gate up'. This circumstances creates a de facto compulsory requirement for age-verification.

Requiring all adults to verify they are over 18 in order to access everyday online services is a disproportionate response to the aim of protecting children online and violates fundamental rights. It carries significant risks of tracking, data breach and fraud. It creates digital exclusion for individuals unable to meet requirements to show formal identification documents. Where age-gating also applies to under-18s, this violation and exclusion is magnified. It will put an onerous burden on small-to-medium enterprises, which will ultimately entrench the market dominance of large tech companies and lessen choice and agency for both children and adults – this outcome would be the antithesis of encouraging diversity and innovation.

In its response to the June 2018 'Call for Views', the ICO recognised that there are complexities surrounding age verification, yet the draft Code fails to engage with any of these.

- **We strongly urge the ICO to drop the idea of age-gating and remove all references to this as a solution within the Code.**

Please note: the following comments on age verification are made on the basis that the ICO has opted not to heed the above advice.

ISSUES WITH AGE-VERIFYING CHILDREN

The Code refers to giving service providers "scope to tailor services to children of different ages." This assumes that age verification can apply to children as well as adults.

The ICO must tread lightly when it comes to requesting verification of a child's age. There is a significant risk that an interpretation of the Code will rapidly increase the spread of age verification solutions aimed at identifying children's age, either within a range or precisely. This could increase data collection and profiling of children or lead to inadvertently restricting access to services for children that don't have identity documents or sufficient parental support. Neither of these outcomes would fulfil the Code's goals for children online.

For age verification to be "robust" it needs to go beyond ticking a box or typing in a date of birth. Self-declaration is too fallible a system. In other contexts, robust age verification has been held to require electronic checking of a legal identification document. This creates an obvious difficulty for children, who do not generally hold any ID other than their birth certificate and possibly a passport, to which they may not have access.

It would introduce a disproportionate burden if the Code inadvertently created an expectation that ID has be provided before accessing an online service. In the case of

passports which are costly, this may also lead to digital exclusion based on family income. Use of credit cards, another form of over-18 age verification, contains high privacy risks and potential for fraud and economic harm.

We note that the right to social development in Article 27 UNCRC includes the right to access and experience the Internet. The Code should operate to give children the tools to enjoy social development and be in control of their personal data. The Code should also seek to help children develop their skills online by seeking learning and capacity building opportunities to improve their understanding of their rights.

The right to social development applies to all children equally. Any age verification measure that would require identity attributes so granular or specific that a child is unable to meet those by lack of resources (for instance requiring a passport or identity verification) would be a negative outcome for Article 27 and should be avoided.

- **The Code should exclude ID-based age verification for under-18s.**

PRIVACY IMPACTS FOR ADULTS OF AGE VERIFICATION

Even if only applied to adults, age verification carries significant privacy risks and should not be promoted by the ICO as an acceptable solution.

The Code proposes that online services could carry out their own age verification processes. However, it is concerning that the Code states that, "If you can show that your processing is particularly low-impact and does not carry any significant risk to children, you may be able to show that self- verification mechanisms are reasonable (eg analytics cookies)" without providing any guidance on when an impact is no longer low and what would constitute a "significant risk". It also states that services "must not use data collected for age-verification purposes for any other purpose" without providing any further detail on how compliance with this will be monitored.

- **The Code should give more detail on what the ICO considers to be a robust, low-impact method of age verification, specify stronger restrictions to minimise data collection and limit processing, and set out how compliance with these standards will be monitored and enforced.**

To ORG, arguments that third-party age verification solutions are not necessary as online services can largely discern the age of their users from behavioural indicators are also troubling. It would be a poor outcome for privacy if the Code in effect endorsed individual behavioural profiling.

- **The Code should explicitly exclude using behavioural indicators to discern and verify age.**

As an alternative, the Code suggests using a "trusted" third-party age verification provider. However, as the Code itself recognises, age verification is a developing area with lots of uncertainty. There is currently no mandatory scheme that certifies that or which third-party providers can be trusted to protect privacy: although in other

contexts the BBFC has published a scheme which will assess whether systems comply with GDPR data protection requirements, this is voluntary and untested so cannot be relied upon. This also begs the question of how online service providers will be able to carry out the Code's due diligence requirement.

There are significant concerns that funnelling online services towards using third-party age verification technologies will lead to fakes and scams, putting people's personal data at risk of exposure and criminal activity. Large age verification providers will also seek to offer single-sign-in across a wide variety of services, which could lead to intrusive commercial tracking and devastating personal impacts in the event of data breach.

It would be a poor outcome for data protection rights as a whole, and a poor message to children about the intrinsic value of data protection, if children's privacy protection was to come at the expense of equal protection for adults, including adults in vulnerable positions for whom such protections have particular importance.

Granular age verification (requiring users to verify exact ages or ages within small ranges) would also require data controllers to collect and process specific data, leading to more invasive profiling of under-18s and the potential for tracking children across online services. This carries significant data protection and privacy risks.

Widespread use of age verification technologies would perhaps also give more insight for targeted behavioural advertising, unless it is explicitly restricted (see below). That too would be an ironic twist to a code of practice that seeks to improve privacy standards.

- **The Code should require that the government legislate to provide a mandatory and robust certification scheme for third-party age verification providers, in order to ensure that privacy and personal data is adequately protected.**

REGULATORY BURDEN

If the burden to age verify is too great for online services, they may decide to remove or restrict access to their service when previously they offered it. This has been seen with the General Data Protection Regulation in other areas. While these services may be acting in error, the effect is the same: a restriction of access to information.

Creating, whether by design or inadvertently, an environment where online services do not offer their services would be a negative outcome and fail to achieve all of the Code's goals for children's digital access and engagement.

- **In explaining what proportionality requires, the Code should note that the proportionality of rules in this sector can have extreme responses.**

We emphasise again, age verification will not achieve the outcomes the Code desires and will create further problems. We strongly urge the ICO to drop this as an idea.

Profiling / Behavioral advertising

Behavioral advertising is known to be particularly persuasive to children.[1] At the core of targeted advertising is an increased processing of personal data in order to profile users with accuracy. In its section on profiling, the Code could more strongly restrict the opportunity for data controllers to perform behavioral advertising on children's personal data.

The United States Federal Trade Commission has taken the approach to require affirmative parental consent before behavioural advertising using children's data can be conducted.[2] The Code should go further. Working Party 29 suggested in a 2013 opinion that data controllers should not process children's data for behavioral advertising purposes.[3] The Code should make that recommendation a standard. Profiling children for behavioural advertising is unnecessary and takes no regard of their best interests.

- **The Code should prevent online services from profiling children for the purpose of serving behaviourally targeted adverts.**

<u>Informing children</u>

We welcome the opportunity the Code provides to empower an online system that does not create a completely unrealistic digital life for under-18s which is quickly stripped away and replaced with the online experience of an adult. We encourage digital and rights-based capacity-building for under-18s so that children can become effective participants online and can increasingly understand and exercise their rights as they move into adulthood.

Child Data Impact Assessments

ORG welcomes the requirement for data protection impact assessments. The code could set out further guidance on what these should address.

- **The DPIA assessment could include the clarity of the consent framework the service operates and the ability of the child to understand and activate their rights**.

- **DPIAs should also address the additional vulnerabilities and needs of children with SEN/disabilities and mental health that lack capacity to consent.**

[1] Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment, pg. 16, https://5rightsframework.com/static/Digital_Childhood_report_-_EMBARGOED.pdf.
[2] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[3] Article 29 Data Protection Working Party, Opinion 02/2013 on apps and smart devices WP 202', 27 February 2013, https://www.pdpjournals.com/docs/88097.pdf.

Parental Consent and Counter-signing

Parental consent for under-13s assumes that parents (1) have a good grasp of privacy notices, (2) are sensitive to their children's development needs online and (3) have a realistic assessment of risk for their child in using these services. Arguably, parents fail on all three of these areas continuously. Research has shown that parents do not understand how children use online services,[4] can overreact to misunderstood context [5] and are at risk of 'consent fatigue'[6] leading to clicking without thinking.

Consequently, parental consent, while important, might well result in agreement by a parent for processing that a child may object to. The appreciation of privacy may be drastically different between parent and child. Research shows that children have an instinct towards their privacy, with younger children seeking a greater privacy than older.[7] This could be reflected in their own consent for processing.

Parental consent also does not build children's confidence in asserting their rights. Straight parental consent may miss the learning opportunity that is presented.

We encourage the ICO to support counter-signing, joint consent or parallel consent - these achieve both aims of addressing the relationship between a data subject and a data controller and improving the agency of younger Internet users.

- **The Code should contain a requirement for joint consent between the parent and the child. If the parent consents to data processing, a notice should be sent to the child, in language that the child can understand, that allows them to also consent, giving them the opportunity to co-consent and exercise their right to express their views. If the child does not consent, another notice should be sent to the parent to notify them of this refusal.**

<u>Age-appropriate technology design</u>

Connected toys and devices

ORG welcomes the explicit inclusion of connected toys and devices in the Code. Below we suggest additional wording and provisions which would strengthen this section.

BE CLEAR ABOUT WHO IS PROCESSING THE PERSONAL DATA AND WHAT THEIR RESPONSIBILITIES ARE

- **The Code in this section should add: "Providers of connected toys and devices should make it clear what personal data their devices collect and for what purposes. Providers should also make clear to consumers what the likely consequences of that data collection and processing would be."**

[4] Boyd and Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies, pg. 8 – 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.
[5] *Ibid*.
[6] Consent for processing children's personal data in the EU: following in US footsteps?', pg 171, https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096.
[7] The I in Online: Children and Online Privacy Survey, 2011, pg. 13. The I in Online is provided attached to this response as it is unavailable online.

PROVIDE CLEAR INFORMATION ABOUT YOUR USE OF PERSONAL DATA AT POINT OF PURCHASE AND ON SET-UP

In order to guide best practice in the delivery of information;

- **It would be useful to for the Code to set standard ways of indicating how the packaging of connected toys and devices and their included booklets can clearly indicate that the product is 'connected' and processes users' personal data.**

This would help consumers recognise common labels and reduce packaging design costs for manufacturers. The Department for Digital, Culture, Media and Sport is currently consulting on similar proposals around labelling the security standards of Internet of Things products.[8] There would be some benefit in carrying out a similar process for data protection standards.

- **The Code should make clear that allowing potential purchasers to view and assess privacy information, terms and conditions of use and other relevant information online before making a purchase should extend to making sure that links to these documents are clearly available on the product descriptions on online stores such as marketplaces (e.g. Amazon) and department stores (e.g. John Lewis), as well as on the manufacturer's own online store.**

Our research has found that the privacy policies provided on manufacturers' own online stores often cover the use of the online store rather than the devices sold on that store. Unless this information is made clear on the site where consumers purchase these products, most consumers will not find out how their personal data will be collected and used.

AVOID PASSIVE COLLECTION OF PERSONAL DATA

We support the measures in the Code to avoid the passive collection of personal data. It should be made clear when personal data is being collected.

- **The Code should additionally provide that, whenever possible, physical switches should be included in connected toys and devices to make microphones, cameras and other components which collect particularly sensitive personal data completely inoperable until the switch is re-enabled.**

Friction in Design

[8] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security

Friction in technology can drive people to very different outcomes. Deployed correctly with good usability, it can make people think about what a controller is doing with their data, which is a positive outcome. Deployed incorrectly, it can result in people circumventing controls or disabling controls altogether, leading to negative outcomes.

For example, Apple's parental controls block all https:// websites. The reason for this is that https:// websites are encrypted, content filters are unable to examine the content of encrypted pages and so the system provides that all encrypted websites must be explicitly allowed by parents. Considering the prevalence of https:// and the privacy and security benefits of encryption, the friction created by the parental controls here are counterproductive.

It is against best practice to create a constant need for parents to unblock normal websites. Further, it could easily lead to parents disabling parental controls to save themselves, and their children, the unnecessary hassle. This is bad design.

- **The Code should note the importance of good design being holistic and taking into consideration these kinds of potential negative outcomes.**

Beyond standards for data controllers

While the Code's proposals for better information provision and consultation with children on the wording of terms and conditions and privacy notices would be useful in building up children's agency, it will mean very little unless proper investment in children's ability to be competent, confident online actors is achieved.

This is achieved by doing more than setting standards for data controllers. It requires education at a proper level, from an early age and continuing throughout school years. Beyond the Code, there should be a call for curriculum development that would achieve this.

Research shows that the problems for children begin not at opaque wording in privacy policies but at the existence of privacy policies. Younger people appear unaware of what privacy policies are or where to find them. With a challenge such as this, it does not matter how much work is put into a privacy policy that is clear for multiple reading ages if a child does not know where to find a privacy policy, or to even know they should expect to see one on a service they visit.

The wish for greater education is evidenced also by children themselves. Consultations have shown an interest from children to learn more about how the Internet and companies on the Internet work. These wishes should not be set aside.

- **The Code should call for digital curriculum development to equip children to understand and exercise their rights in relation to the Internet and online services.**

Placing greater burdens on data controllers to operate with regard to children to one thing is a laudable outcome. Investing in educating children to gain a better

understanding than their parents about the Internet, the Internet economy, and their rights online, has the potential to change society.

Conclusion: More reflection required

While we support the aims of the Code, and consider that many of its provisions are clear and sound, the points we have made above highlight fundamental flaws that if not properly addressed will derail the Code's implementation and enforcement and cause significant harm to children's privacy and free expression online.

We strongly urge the ICO to take the time needed to consider all feedback received during this consultation process and not rush to implement the Code to meet any arbitrary deadline or official expectation.

- **We encourage the ICO to open a further consultation period after amendments have been made to the Code at this stage in the process, in order to give all relevant parties time and opportunity to respond to outstanding issues.**