Information Commissioner's Office

Call for evidence:

Age Appropriate Design Code

Start date:27 June 2018
End date: 19 September 2018

Introduction

The Information Commissioner (the Commissioner) is calling for evidence and views on the Age Appropriate Design Code (the Code).

The Code is a requirement of the Data Protection Act 2018 (the Act). The Act supports and supplements the implementation of the EU General Data Protection Regulation (the GDPR).

The Code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet. Once it has been published, the Commissioner will be required to take account of any provisions of the Code she considers to be relevant when exercising her regulatory functions. The courts and tribunals will also be required to take account of any provisions they consider to be relevant in proceedings brought before them. The Code may be submitted as evidence in court proceedings.

Further guidance on how the GDPR applies to children's personal data can be found in our guidance Children and the GDPR. It will be useful to read this before responding to the call for evidence, to understand what is already required by the GDPR and what the ICO currently recommends as best practice. In drafting the Code the ICO may consider suggestions that reinforce the specific requirements of the GDPR, or its overarching requirement that children merit special protection, but will disregard any suggestions that fall below this standard.

The Commissioner will be responsible for drafting the Code. The Act provides that the Commissioner must consult with relevant stakeholders when preparing the Code, and submit it to the Secretary of State for Parliamentary approval within 18 months of 25 May 2018. She will publish the Code once it has been approved by Parliament.

This call for evidence is the first stage of the consultation process. The Commissioner seeks evidence and views on the development stages of childhood and age-appropriate design standards for ISS. The Commissioner is particularly interested in evidence based submissions provided by: bodies representing the views of children or parents; child development experts; providers of online services likely to be accessed by children, and trade associations representing such providers. She appreciates that different stakeholders will have different and particular areas of expertise. The Commissioner welcomes responses that are limited to specific areas of interest or expertise and only address questions within these areas, as well as those that address every question asked. She is not seeking submissions from individual children or parents in this call for evidence as she intends to engage with these stakeholder groups via other dedicated and specifically tailored means.

The Commissioner will use the evidence gathered to inform further work in developing the content of the Code.

The scope of the Code

The Act affords the Commissioner discretion to set such standards of age appropriate design as she considers to be desirable, having
regard to the best interests of children, and to provide such guidance as she considers appropriate.

In exercising this discretion the Act requires the Commissioner to have regard to the fact that children have different needs at different ages, and to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child.

During Parliamentary debate the Government committed to supporting the Commissioner in her development of the Code by providing her with a list of 'minimum standards to be taken into account when designing it.' The Commissioner will have regard to this list both in this call for evidence, and when exercising her discretion to develop such standards as she considers to be desirable

In developing the Code the Commissioner will also take into account that the scope and purpose of the Act, and her role in this respect, is limited to making provision for the processing of personal data.

Responses to this call for evidence must be submitted by 19 September 2018. You can submit your response in one of the following ways:

Online

Download this document and email to:
childrenandtheGDPR@ICO.org.uk

Print off this document and post to:
Age Appropriate Design Code call for evidence
Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the call for evidence please telephone 0303 123 1113 and ask to speak to the Engagement Department about the Age Appropriate Design Code or email childrenandtheGDPR@ICO.org.uk

Privacy statement

For this call for evidence we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our privacy notice.

Section 1: Your views and evidence

Please provide us with your views and evidence in the following areas:

Development needs of children at different ages

The Act requires the Commissioner to take account of the development needs of children at different ages when drafting the Code.

The Commissioner proposes to use their age ranges set out in the report Digital Childhood – addressing childhood development milestones in the Digital Environment as a starting point in this respect. This report draws upon a number of sources including findings of the United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group in its literature review of Children's online activities risks and safety.

The proposed age ranges are as follows:

3-5
6-9
10-12
13-15
16-17

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be (delete as appropriate):

Not at all appropriate
Not really appropriate
Quite appropriate
Very appropriate

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services),

Our evidence is mainly informed by the KOALA (Kids Online Anonymity and Lifelong Autonomy) project (http://www.cs.ox.ac.uk/projects/KOALA-IAA/), funded by Oxford University's EPSRC Impact Acceleration Account, led by Prof. Sir. Nigel Shadbolt and Dr

Jun Zhao, which is aimed at investigating the impact of data tracking upon the general well-being of young children aged between 6 and 10. Our views are also informed by the findings from a related project, the SOCIAM project (http://sociam.org), funded by the EPSRC and led by Prof. Sir. Nigel Shadbolt.

Between summer 2017 and 2018, the KOALA project has interviewed over 50 children between 6 and 11 years old from Oxfordshire, with an aim to understand children's perception of online privacy risks [1,2] related to their use of mobile devices, such as tablets or smartphones.

Through our studies, we observed the following differences between children older than 8 and those younger:

- First, when analysing how children described situations that made them feel uneasy or worried, children older than eight were able to provide a more elaborate description and recognition of risks than younger children. Older children demonstrated better awareness and could use a broader range of vocabulary to describe things that appeared strange to them, such as "being hacked or tricked", or to describe things in a more precise matter, such as "my personal data".

- Further, children older than 8 demonstrated much broader experience with online platforms and services than younger children. Probably related to this, they reported experience of more privacy-related risks, and they also had had more discussions about these issues with their peers, than younger children.

- Finally, we found that participants who were younger than eight mainly relied on guidance from parents or help from older siblings. Older children appear more aware of techniques to cope with risks, such as obfuscating their identity information, and they felt more confident about trying to see what happens even though understood that they could put themselves at risk.

Although we have to be cautious about generalising our findings given the sample size of the study, we would recommend that app designers consider the following when designing with children in mind:

1. Consider mechanisms that will facilitate **children's learning about privacy knowledge**, instead of mainly focusing on restricting or monitoring what children can access
2. Consider using **simpler language** to signpost or explain risks for children under 8, given their literacy development and their experiences
3. Provide more support for children under eight by **explaining the implications of the risks**, so that they are able to develop from merely following rules to an ability to recognise and understand risks
4. Provide more support for children older than eight regarding **online video or game recommendations**, so that they become more mindful about the content they are consuming and the implications of these recommendations
5. Provide tools to support parents, guardians and educators in discussing privacy risks with their children

Q2. Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age brackets.

We recognise that although children have different needs at different ages, children share a need to protect their personal space online even though they may engage in different types of activities, have different abilities to depict these risks, and have different preferences over the safeguarding mechanisms taken by their parents. Children's rights to data should be respected, but at the same time we should recognise some critical differences in their ability to cope with risks and their preferences of how to be supported.

1. Research of early childhood development has shown that children as young as three years old already demonstrate the ability to develop a complex concept of secrecy and deception [3,4]. Our experience in the KOALA project with children aged as young as six also confirmed that children care about their personal online space and who may have access to their personal data [2]. This `theory of mind' should be taken into consideration by policymakers and designers, regarding children's rights to data.

2. Several reports have looked into the range of online activities engaged in by children, including games (particularly multiplayer games), watching videos, participating in online social media platforms, or search for information [5]. Children go online to have fun or to learn about new things. At the same time, these reports recognise that as children grow older, they are engaged in a broader range of online activities. This can be related to their developmental needs --- more confidence when engaging in more diverse (social) activities or placing more value on friendships and peers' opinions [6-7]. In our studies, older children were observed to have experienced more risky scenarios than younger children.

3. Previous research, as well as our own research in the KOALA project, have shown that younger children (6-10yo) often have more trust in and reliance on their parents' help and advice before reaching adolescence [1,8,9]. Teenagers, by contrast, do not communicate as much with parents about their online risk experiences [10]. This indicates a need to introduce parental mediation regarding privacy risks to children from a young age [1,8], This is largely neglected by both parents and designers when supporting children's online privacy needs.

4. Given that the majority of online privacy safeguarding tools for children focus on a restrictive or monitoring approach, previous research has looked into how parents and their children perceive these tools [11]. Findings show that both parents and teenagers believe that they would appreciate more tools to help parents discuss privacy issues with their children than simply monitoring or restricting them. In this way teenager's personal space is respected, and at the same time, parents can retain an awareness of a child's safety in the online space [11]. Similar research was conducted for children under 11 and found that younger children understand the need for parents to monitor their safety online, even though the design proposed by the children showed a higher preference of restrictions over other approaches, such as monitoring, parental mediation or automated controls [12].

The United Nations Convention on the Rights of the Child

The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.

Q3. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services)

Children care about their personal privacy in both the physical world and in virtual and online spaces. Their rights to data and their best interests should be respected.

Aspects of design

The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code.

These are as follows:

- default privacy settings,
- data minimisation standards,
- the presentation and language of terms and conditions and privacy notices,
- uses of geolocation technology,
- automated and semi-automated profiling,
- transparency of paid-for activity such as product placement and marketing,
- the sharing and resale of data,
- the strategies used to encourage extended user engagement,
- user reporting and resolution processes and systems,
- the ability to understand and activate a child's right to erasure, rectification and restriction,
- the ability to access advice from independent, specialist advocates on all data rights, and
- any other aspect of design that the commissioner considers relevant.

Q4. Please provide any views or evidence you think the Commissioner should take into account when explaining the meaning and coverage of these terms in the code.

Default privacy settings

Previous research has shown that few people make changes to their default privacy settings [13], and this includes children. However, most social media platforms, including those used by children under 13, set their users' profile as public by default. The same applies to privacy settings on mobile platforms. Children not only rarely make changes to their privacy settings, but also struggle to differentiate between public and private profiles [5]. This demands better default privacy setting designs for children.

Data minimisation, profiling and transparency

Our research in the KOALA project shows that children care about their online privacy and what personal information about them might be accessible to whom [2]. However, they had different

abilities to recognise explicit vs implicit personal data collection. When facing explicit personal data collection, like signing-up to new platforms or games, children largely demonstrated their ability to refuse to provide too much sensitive information about themselves. They were capable of making the compromises between what the games required and their information. However, children demonstrated much less awareness about how their data might be tracked by the applications on their mobile devices, which was then used to promote content for their consumption.

Presentation and language of terms and conditions and privacy notices

Extensive research has looked into the ineffectiveness of T&Cs and privacy notices for raising users' awareness of privacy risks [14-15]. Research has proposed alternative ways to present and communicate privacy risks to the users through a visual presentation or summarisation [16-17]. However, the effectiveness of these approaches is highly subject to whether the implementation of such designs was indeed well-thought through, consistent, and coherent. As a result, users often question the reliability of such presentations or misunderstand the meaning of these presentations.

Use of geolocation technology

Location tracking is commonly present on mobile devices applications and can bring both benefits and disbenefits to users. For parents, this can provide essential information for them to track and monitor where their children are and help them be mindful of their safety. For children, this can be an essential function for them to join in some popular applications used by their peers, such as SnapChat.

However, location sharing can always bring additional privacy risks to children when location information is accessed by the wrong people, or used by online marketing companies to generate profiles of children. Children in our study felt particularly anxious about their location information being accessible by people they didn't know [2], and some of them cited how the knowledge of SnapMap made them turn off the location tracking mode on their devices. However, although research on adult users has shown that location data is perceived as one of the most sensitive types of personal information, and how different notification mechanisms could impact on the effectiveness of their control of sharing location data [18], very few studies have focused on collecting such evidence from young children or teenagers.

Q5. Please provide any views or evidence you have on the following:

Q5A. about the opportunities and challenges you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas.

Default privacy settings --- opportunities and challenges

Although children care about their personal online space, they still have knowledge gaps in their understandings about online privacy [8], and more importantly, they struggle to apply risk coping strategies consistently [5], when they consume content from familiar sources or see things that appear to be fun and interesting. Our research in the KOALA project shows that children under 11 particularly struggled to recognise risks related to online game or video promotions, or the idea of data tracking and personalised recommendations.

The code has the opportunity to standardise default privacy setting requirements to app developers and organisations who design applications with children in mind.

Data minimisation --- opportunities and challenges

Recognising implicit data collection is not a challenge unique to children. However, children have less ability to understand how this may impact on their online privacy now, and in the future. Our research and previous research has shown that children may make more of their personal information available to the third-party trackers through the applications they use on the mobile platforms. Our findings in the SOCIAM project has shown that mobile apps from the 'family' genre from the Google PlayStore can have more third-party trackers than games designed for adults [19]. This is also confirmed by another related study [20]. Behind the cute characters, children may be making more of their personal data accessible to data profiling and personalisation than adults. Further, our research in the KOALA project and related reports have shown children's limited resistance to in-app promotions. A large number of children reported that their favourite games were discovered through in-app promotions. Finally, given the widespread practice of shared family devices, exposure of personal data through children's online activities will also have a direct impact on the personal privacy of parents and other family members.

The code has the opportunity to enforce minimal personal data collection from applications designed with children in mind. The app developers should have a legal basis to process children's data, however, the developers should also have a set of ethical considerations in mind when processing children's data, by putting children's best interests first and considering alternative mechanisms. The code should require app developers to consider mechanisms to separate children's personal profile from those of others, such as family profiles from shared mobile devices or smart home devices. The code should also consider mechanisms to encourage the development of an alternative, ethical personal data collection and use, through approaches like rewarding more ethical app developers or promoting an alternative economic model for the sharing and using of personal data online.

Presentation and language of terms and conditions and privacy notices --- opportunities and challenges

Children don't read and mostly can't understand these notices, or understand what they are providing consent to. However, children care about their privacy, and they would value an opportunity to participate and take control. Previous research has shown how young children could have a better understanding of content appropriateness through comic characters put next to the videos [21].

However, the challenge remains how to standardise the representation of risks to children, when we can't even provide effective content ratings for videos on YouTube, and when mobile apps from a genre designed for families can still be associated with the presence of third party data trackers.

The code has the opportunity to look into the primary concerns of children and their families, and promote standardised, simplified notification of privacy risks and implications.

Use of geolocation technology --- opportunities and challenges

Based on existing research on adult users' perception and coping of location tracking, we need more understanding about how children perceive this type of privacy threat and how they would like to manage them.

The code should encourage 'no' location tracking as a default from app developers designing with children in mind, and encourage developers to make location tracking more visible to children during

the use of their applications. Anonymise at source technologies should also be considered so that if data is collected it is verifiably not attributable to identifiable individuals.

Q5B. about how the ICO, working with relevant stakeholders, might use the opportunities presented and positively address any challenges you have identified.

The ICO should work with the following stakeholders to achieve the following:

- App developers, to encourage ethical designs
- App providers, to encourage the development of an ethical market for choice of apps
- Organisations like Common Sense Media (http://commonsensemedia.org) or Good App Guide (http://www.fundamentallychildren.com/good-app-guide/), to promote knowledge about online privacy and choice of technologies for children

Q5C. about what design standards might be appropriate (ie where the bar should be set) in each or any of the above areas and for each or any of the proposed age brackets.

Q5D. examples of ISS design you consider to be good practice.

Q5E. about any additional areas, not included in the list above that you think should be the subject of a design standard.

Any proposed anonymisation technologies.

Q6. If you would be interested in contributing to future solutions focussed work in developing the content of the code please provide the following information. The Commissioner is particularly interested in hearing from bodies representing the views of children or parents, child development experts and trade associations representing providers of online services likely to be accessed by children, in this respect.

Name: [redacted]

Email: [redacted]

Brief summary of what you think you could offer

[redacted] Human Centred Computing in the Department of Computer Science at the University of Oxford.

The group's research focuses on understanding the challenges and opportunities presented as computational systems are increasingly integrated into the fabric of people's lives.

The group investigates ways to ensure fair, transparent, and accountable data-driven algorithmic systems and to empower individuals to take better control of their data, including exerting control over their privacy in future, sensor-rich information environments.

We would be interested in contributing to further development of the Code. Our expertise is particularly relevant in ongoing monitoring of the Code to ensure that it remains relevant as technology continues to emerge and evolve. It is certain that future ISS will differ from those we currently experience, raising new challenges which we cannot predict but can try to prepare for through anticipatory work.

Further views and evidence

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

Our evidence is mainly informed through our participation in two research projects

- KOALA, Kids Online Anonymity and Lifelong Autonomy, funded by Oxford University's EPSRC Impact Acceleration Account (12/17-03/19). PI: Prof. Sir. Nigel Shadbolt. (http://www.cs.ox.ac.uk/projects/KOALA-IAA/)

- SOCIAM, Theory and Practice of Social Machine, funded by the ESPRC (EP/J017728/1;EP/J017728/2 -- 06/12 - 05/18). PI: Prof. Sir. Nigel Shadbolt (http://sociam.org).

[1] Zhao et al. “It’s more than a game”: Understanding Parents’ and Children’s Expectations of Personal Data Privacy on Tablet Computers. KOALA project report. April 2018
[2] Zhao et al. Understanding Children's Description of Online Privacy Risks: Empowering Children to Cope with Risks on Mobile Platforms. KOALA project report. September 2018
[3] Colwell et al. 2016. Secret keepers: children’s theory of mind and their conception of secrecy. Early Child Development and Care 186, 3 (2016), 369–381.
[4] Wimmer and Perner. Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children’s understanding of deception. Cognition 13, 1 (1983), 103–128.
[5] Livingstone et al. 2017.Children’s online activities, risks and safety: a literature review by the UKCCIS evidence group. Technical Report. UKCCIS evidence group
[6] Eccles, J. S. (1999). The development of children ages 6 to 14. The future of children, 30-44.
[7] Damon, W., Lerner, R. M., & Eisenberg, N. (Eds.). (2006). Handbook of child psychology, social, emotional, and personality development (Vol. 3). John Wiley & Sons.
[8] Kumar et al. (2017). 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. Proceedings of the ACM on Human-Computer Interaction, 1(CSCW), 64.
[9] Buhrmester & Prager. (1995). Patterns and functions of self-disclosure during childhood and adolescence. In K.J. Rotenberg, ed., Disclosure Processes in Children and Adolescents. Cambridge University Press, Cambridge, UK, 10–56.
[10] Wisniewski et al. 2017. Parents Just Don’t Understand: Why Teens Don’t Talk to Parents About Their Online Risk Experiences. Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, ACM, 523–540.
[11] Wisniewski et al. 2017. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? In Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW ’17), 51–69.
[12] McNally et al. 2018. Co-designing Mobile Online Safety Applications with Children. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 523).
[13] Spool, J. (2011). Do users change their settings. User Interface Engineering, 2013.
[14] Cranor, L. F. (2003). P3P: Making privacy policies more useful. IEEE Security & Privacy, 99(6), 50-55.
[15] Schaub et al. (2015). A design space for effective privacy notices. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 1-17).
[16] Kelley et al. (2009). A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (p. 4). ACM.
[17] Lin et al. (2014). Modeling users’ mobile app privacy preferences: Restoring usability in a sea of permission settings. In Proceedings of the 4th Symposium on Usable Privacy and Security (p 199).
[18] Almuhimedi et al. (2015). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 787-796). ACM.
[19] Binns et al. (2018). Third Party Tracking in the Mobile Ecosystem. Proceedings of the 10th ACM Conference on Web Science.
[20] How Game Apps That Captivate Kids Have Been Collecting Their

Data.https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html
[21] Hashish et al. (2014). Involving children in content control: a collaborative and education-oriented content filtering approach. In Proceedings of the 32nd annual ACM conference on Human factors in computing systems (pp. 1797-1806). ACM.

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify: In academic research we have specifically worked to elicit the views of children aged between 6 and 10 and their requirements for design of technologies	☐ X
A body representing the views or interests of parents? Please specify:	☐
A child development expert? Please specify:	☐
A provider of ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An ICO employee?	☐

Other? Please specify: A University research group in Human Centred Computing, and ethics and privacy related to the development of Artificial Intelligence technologies, with particular involvement of the use of mobile devices by children aged between 6 and 11, and the use of smart home devices in modern families	☐

Thank you for responding to this call for evidence.
We value your input.