NSPCC

NSPCC Response to the ICO's Call for Evidence regarding the Age-Appropriate Design Code

Introduction

1. The NSPCC welcomes the opportunity to provide evidence regarding a statutory age-appropriate design code ("the code") under the Data Protection Act 2018. In our view, the code has the potential to make a real difference and prevent children from experiencing harm and abuse online.

2. The NSPCC is a child protection charity and our response is focussed on the ways in which the code can prevent children from experiencing sexual and emotional abuse online. From contacts to our Childline service, we know that children also face other online harms, including bullying and exposure to content that is suitable only for adults. An effective age-appropriate design code will play a vital role in preventing children from experiencing all these harms and in supporting children after abuse has occurred.

3. Technology is now central to children's lives. Increased smartphone ownership and use of social media by children in the UK have considerably expanded the range and quantity of data that are shared by, or can be gathered in respect of, children. In 2011, just 35% of children aged 12-15 owned their own smartphone; but by 2017 this had risen to 89% of children this age.[1] Similarly, in 2017, just over half of children aged 12 had at least one social media account. By age 13, that figure rises to nearly three-quarters.[2] Social media is now a ubiquitous part of childhood, but alongside the many opportunities, it opens up an array of potential harms.

4. Children[3] tell us that their lives are lived without distinction between the online and offline environments. They enjoy playing games, chatting with friends and being part of communities online in ways that blend seamlessly with offline friendships and experiences. However, all of this is done in an environment which offers them far less protection than we routinely expect in children's spaces, and evidence suggests that lowered inhibitions can mean that children may act in ways or comply with requests they would not offline.[4] The

[1] Ofcom (2011) UK Children's Media Literacy,; and, Children and Parents: Media use and Attitudes Report (2017).
[2] ibid
[3] Unless otherwise specified, "children" throughout this paper means people under the age of 18.
[4] Hamilton-Giachristsis, C. et al (2017) Everyone deserves to be happy and safe. London: NSPCC.

age-appropriate design code can, and should, mitigate the safety risks that children face on social networks and other platforms.

5. Our interest in data protection is predicated on the understanding that better informed consent regarding the sharing of personal information, and the requirement on online providers to adopt a range of 'safety-by-design' features, should meaningfully help to protect children from the risk of online harm and abuse.

The impact and risks of online sexual abuse

6. There are two principal means by which children can be placed at risk of abuse by the misuse, or inappropriate sharing, of their data.

7. First, children's information may be shared in ways that they do not consent to. Notably, intimate images may be shared without children's consent. Children calling Childline tell us how losing control of intimate images, and other forms of sensitive information, can be hugely upsetting:

> I'm really embarrassed about what I've done but I need some advice on how to stop it. I sent a guy I know topless pictures of me over Snapchat because I didn't think he would save them, but he did. He's now posted them over some other social networking sites and I want them removed but I don't know how? What should I do? (Girl, Age Unknown)[5]

8. Second, personal information (even when shared with consent) can also place children at risk of other forms of technology-facilitated abuse such as grooming. The National Crime Agency has reported that even small clues in a child's social media profile, such as a photo in a child's bedroom with posters or school trophies in the background, can be used by groomers as a way of initiating conversation and to help facilitate the development of a trusting relationship.[6]

9. NSPCC research has shown that the impact of 'online' and 'offline' abuse is the same, despite the common perception that online abuse is less harmful. Children that have experienced online abuse report symptoms such as depression, self-harm, anxiety and self-blame and may have problems at

[5] Childline (2014) Sexual abuse and online safety snapshot. London: NSPCC.
[6] Our understanding has been developed through conversations between the NSPCC, Child Exploitation and Online Protection (CEOP) Command.

school. In some cases they reported more 'online' specific symptoms, including discomfort around cameras or being filmed.[7]

10. As we set out below, an effective age-appropriate design code can be an important mechanism to address these risks.

Design settings

11. This response sets out the elements we recommend the age-appropriate design code must cover, including:

- age-appropriate privacy notices;
- high default privacy settings;
- location sharing and settings;
- the right of erasure; and
- minimising collection of children's data.

The code must also be designed with the flexibility to cover new technologies as they emerge, avoiding any necessity to rewrite outdated and insufficient clauses.

Age-Appropriate Privacy Notices

12. In order for children to exercise their privacy rights online, they need to understand what privacy is, why privacy is important for safety, and how to achieve that privacy through settings and controls.

13. Many popular sites and apps use privacy notices and terms and conditions that are lengthy, legalistic and difficult to comprehend, and there is a clear gap between how terms and conditions are presented and the capacity of child users to readily understand them.[8] Given that most of these services have users younger than 13, this is clearly unacceptable.

14. The code must require online services to explain these three issues to children in an accessible and age-appropriate manner. Since children of different ages will have different levels of development, the online service should provide notices that are accessible to the youngest user, meaning that all users of the service would be able to understand. The code should highlight that online services need not solely rely on written text, and should advise sites to use the

[7] Hamilton-Giachritsis et al., Everyone deserves to be happy and safe": The impact of online and offline child sexual abuse, NSPCC, 2017.
[8] For example, this has been documented by the Office of the Children's Commissioner for England in its project to simplify terms and conditions for social media sites.

most effective methods for engaging children. Indeed, for younger children, it may be most appropriate to use non-written methods like cartoons.

15. Providing simple privacy notices should not be a one-off event. Instead, service providers should provide ongoing advice and prompts about how a child can manage their data, which matches child users' development and the greater autonomy they obtain as they transition into adulthood.

16. Under the GDPR, if online service providers rely on consent to process the personal data of children under the age of 13, they must secure parental consent to do so. Therefore, the code must also ensure that online service providers generate privacy notices that are appropriate and accessible for parents and carers, some of whom will face similar challenges to their children in understanding the implications of how data will be used.[9]

High Default Privacy settings

17. Privacy settings determine the extent to which a child's personal data and identity can be shared with the online service provider and, crucially, with other users.

18. The code should require online service providers to offer default high privacy settings on children's accounts and should require that children's accounts are not publicly searchable. Although NSPCC research finds the majority of children know how to adjust their privacy settings (67 per cent),[10] only a small minority (18 per cent) have actually changed their settings so that fewer people can view their profile on social media.[11]

19. Research suggests that many children continue to consider their accounts as 'private spaces', even though their personal information, posts and content may be viewed by any other user if the account is in public mode.[12] This introduces clear safety risks, with 'public by default' profile modes providing opportunities for groomers to contact significant numbers of children on open platforms.

[9] Information Commissioner's Office (2018). *Children and the GDPR Guidance.* p.25.
[10] NSPCC (2018) NetAware, full findings available on request.
[11] UKCCIS (2017) Children's online activities, risks and safety: a literature review by the UKCCIS Evidence Group
[12] Ofcom (2016) Children's Media Lives: Year 2 Findings

20. Given the growth of livestreaming sites, and the adoption of live video functionality in most major social networking sites, the code should require that children can only livestream to their approved friends and contacts.

21. While the default high privacy settings that we recommend could be reversed by a child if they sought to do so, existing user behaviour suggests that a majority of children would retain the higher privacy settings were it to be provided by default.[13] Sites should not present design challenges to prevent or frustrate children who wish to modify their privacy settings. As the Norwegian Consumer Council has demonstrated,[14] major platforms have designed significantly longer user journeys for users that wish to raise their privacy settings. Sites should be considered in breach of the code if they take such steps to frustrate or hinder children seeking to adopt the most appropriate privacy settings to keep themselves safe.

22. We would welcome the ICO undertaking further research to assess how children understand, and can be encouraged to take up, privacy mechanisms with a view to informing the development of the code.

Location Sharing and Settings

23. A large, and rising, number of children access the internet using mobile phones or tablets.[15] Many of the most popular online services, such as Snapchat, offer location features as an integral part of app design, and many of these sites build and record huge amounts of location data as a core part of their design, often without users being fully or at all aware. In our view, the code must feature methods of mitigating the risks associated with location sharing for children.

24. The most obvious risk is from a perpetrator known to a child who could use the feature to track the child's location and facilitate in-person contact. A perpetrator with frequent access could also use the feature to track a child's movements to build up a profile for the purposes of grooming or coercion. Location sharing poses particular risks in relation to coercive and exploitative situations by offering abusers an opportunity to monitor and manipulate their

[13] For example, Dhingra et al (2012) documented a 'default pull' in respect of technology use. Dhingra, N et (2012.) The default pull: An experimental demonstration of subtle default effects on preferences. *Judgemental Decision Making.* 7, 1 (2012), 69–76.
[14] Norwegian Consumer Council / Forbrukerradet (2018) Deceived by Design: how tech companies use dark patterns to discourage us from exercising our rights to privacy
[15] *Ofcom (2017) Children and Parents: Media use and Attitudes Report*

victims.[16] Services that broadcast a child's location publicly can also put children at risk of bullying by, for instance, revealing that they have travelled to somewhere that they do not wish their peers to know about.

25. Even when location information is not shared with other users, the routine collection of such data poses risks. Some apps are known to track smartphone-users not only when the app is in active use, but on an ongoing basis, unless the user disables an obscure setting. If this data were hacked, perpetrators would have access to a comprehensive location history for potential misuse.

26. The design code should require services to implement a number of solutions. First, location sharing should be turned off by default for children, with easy-to-access settings to maintain the off-setting. Second, location sharing should never automatically return to on-mode following a reset or software update. Third, services should not track users when not in active use. It should also be made very obvious when a service is tracking a user. For example, a clear and accessible privacy notice could pop up to notify a user when a tracking period starts and ends.

27. The code should also specify that a child should not be disadvantaged as a result of disabling location features. A child's decision not to allow an online service to track their location should not be a basis for excluding them from a service or deliberately downgrading their experience.

Right of Erasure

28. If it is implemented correctly, the right of erasure in the GDPR has the potential to be an effective tool for reducing the availability of self-generated sexualised images of children. However, online services are dragging their heels, and some services are waiting for the development of case law before determining what actions to take. In the meantime, children will struggle to exercise their right to erasure and be left at risk of abuse and re-victimisation. The existing ICO guidance, *Children and the GDPR*, provides a clear interpretation of the GDPR's requirements, but it is not directly enforceable. For this reason, we recommend that the Guidance relating to Right of Erasure is expressly included in this legally enforceable code.

29. Prior to the introduction of the GDPR, in order to remove a sexualised image of themselves from the internet, a child had to:

[16] This has been researched in domestic abuse situations, where similar dynamics of coercion and control apply. For example, see UCL's Gender and Internet of Things programme.

- show identification to prove that they were under 18;
- report the image to the Internet Watch Foundation (IWF); and
- have the image judged as illegal by the IWF.

30. It can be difficult for children to prove their age (as they will only rarely have access to official documents) and the need to make an official report, even anonymously, would put off many children. Even then, in order for an image to be removed, the image would need to meet the legal threshold of indecency. Under this system, children face a significant possibility of having their take-down request rejected.

31. In the absence of any real enforceable right of erasure, the NSPCC has created a simpler process for children to remove their sexualised images.[17] But this process is only of limited use for children who are not able to prove their age, or who have lost control of an intimate image which doesn't cross the legal threshold.

32. In order to ensure that the right is implemented to its full potential, the code must require services to build simple and effective standalone tools that children can readily access, which would allow them to meaningfully exercise their legal right of erasure, even where images have been screenshotted and shared by other users. Through the incorporation of the GDPR guidance, the code should require that these mechanisms make it as easy to remove data as it is to upload it in the first place.

Minimising collection of children's data

33. It is not appropriate to design online services for children that actively encourage children to share as much data as possible. Such design features are often known as 'time-extension mechanisms'.[18] While these are not directly an abuse issue, some mechanisms are known to disincentivise children from weighing up the risks of sharing appropriate amounts of data by, for example, harnessing peer pressure to garner as many likes and friends or followers as possible.

34. This pursuit of social kudos risks may encourage children to post more information (or images), and to accept inappropriate friend and follower requests from unknown or potentially malicious users, opening them up to abuse.

[17] https://contentreporting.childline.org.uk
[18] Kidron, B. (2018). Disrupted Childhood: the Cost of Persuasive Design. London: 5 Rights

35. The design code must require designers to prioritise the safeguarding of children, over maximising data collection for primarily commercial gain.

Other Issues

Gradations of protection for younger children

36. Children need more protection than adults online, just as they do in the offline world. Throughout children's real-life spaces, that protection is graded to their age and developmental stage. For example, playgrounds for pre-schoolers have softer equipment than those for pre-teens. In respect of online platforms, the protections required for a six-year-old, who is likely to be trusting of adult authority and looking to adults for guidance, will differ from those a seventeen year-old preparing for adulthood.

37. We recommend the ICO explore further how the code could support a graded transition into adulthood. For example, the code could place a requirement on firms that offer services to younger children, including development stages up to age 13, to assess the safeguarding implications of offering services to younger children, and to ensure their sites are designed to reflect these risks.

38. The ICO could also develop guidance on appropriate 'sharing norms' for platforms offering services to younger users. When developing such guidance, the ICO could draw on existing 'walled garden' platforms, and other examples of innovation for younger age groups. For example, Lego Life provides a walled garden social network for under-13s.[19]

Regulatory Overlap

39. The Government has announced plans to legislate on internet safety through an Online Harms Bill, the details of which will be laid out in a forthcoming White Paper. The NSPCC has campaigned for the Bill to introduce an independent regulator to ensure that online services protect children against a variety of legal and illegal harms.[20] Whatever new regulatory system emerges, it is vital that the ICO manages any regulatory overlap by establishing a memorandum of understanding between regulators.

[19] https://www.lego.com/en-gb/life, viewed 18/09/18.
[20] Our detailed proposal for a social media harm regulator will be available upon request from October 2018.

40. Such overlap is likely to emerge in online reporting systems for harmful content and behaviour. Posting an abusive or bullying photograph of a child, or tagging a child in an offensive Facebook status, may be both data protection and online harm issues. The child may object to both the information being processed and to the unpleasant experience of that information having been published. It is important that children are not deterred from reporting harmful material by any confusion about what rules apply, or who can enforce them.

Supercomplaint powers

41. Children are likely to need help to exercise their rights, especially if they are not happy with the way they have been dealt with by a large social network. Help is provided through Article 80 of the GDPR, but, again, this will require an expansive interpretation if it is to be effective for children.

42. Article 80(1) provides a means for users, including children, to appoint a third party to bring a complaint to the ICO on their behalf, or to seek legal remedies for breach of the regulation. In practice it is unlikely that children will meaningfully be able to appoint a third party to exercise their legal rights in this way. It is also not clear whether any third party body is sufficiently resourced to take up complaints on individual children's behalf.

43. Article 80(2) allows Member States to legislate to allow third parties to exercise these rights on behalf of data subjects, without the subject's permission. These so called 'supercomplaint' powers have not been implemented in the UK, although the Secretary of State is required by section 189 of the Data Protection Act to review this position within 30 months of the Act's entry into force. In the absence of the implementation of Article 80(2), we recommend that the ICO makes provision for children's organisations to make supercomplaints to ICO on behalf of children in respect of potential breaches of the code, where structural or widespread areas of non-compliance have the potential to affect significant numbers of child users.

44. This reflects the fact that such organisations may be better placed to represent the interests of children in this respect, and to address areas of non-compliance which may compromise children's safety online.

Emerging Technologies

45. The age-appropriate design code must be flexible enough to cater for emerging technologies, such as the internet of things (IoT).

46. IoT devices for children, such as connected toys, often record large amounts of personally-identifiable data, and may pose specific online safety risks for young people.[21] The nature of these devices means that children may share especially sensitive information when using them. For example, children may well tell 'secrets' to dolls and teddy bears when playing alone. Secondly, there are examples of manufacturers failing to maintain appropriate frequently exhibit lax cybersecurity standards, making it easy for sensitive and potentially risky information to be accessed.[22]

47. In the code, the ICO must ensure that the provisions apply not only in respect of traditional screen-based technologies, but are flexible enough to accommodate new and evolving technology that may facilitate or enable abuse. We would welcome further discussions with the ICO on this subject.

Conclusion

48. An effective age-appropriate design code will empower children both to be and to feel in control of their data, while ensuring that online services shoulder the responsibility for creating an environment in which young people can explore safely and without risk of technology-facilitated abuse.

49. We look forward to working closely with the ICO to develop the code in the coming months.

[21] Norwegian Consumer Council / Forbrukerradet (2016) #Toyfail: An analysis of consumer and privacy issues in three internet connected toys
[22] Norwegian Consumer Council/ Forbrukerradet (2016) Investigation of privacy and security issues with smart toys.