



MGIF Response to the Information Commissioner's Office (ICO) Call For Evidence on Age Assurance

Summary

MGIF supports the exploration of age assurance and parental control potentialities. However, we are concerned that this call for evidence may presuppose a level of understanding and technological feasibility which does not currently exist. We hope that the below principles and observations are of utility to the ICO as part of its examination of age assurance.

Background

The Mobile Games Intelligence Forum (MGIF) welcomes the opportunity to respond to this call for evidence on the use of age assurance. In January 2020, MGIF opened dialogue with the ICO to assist Age-Appropriate Design Code compliance for the mobile games sector. We were delighted that on February 24th 2021, at our first-ever conference as a newly constituted Forum, the ICO presented on the application of the Code to mobile games.

Since then, the ICO has engaged in concerted outreach with the online games sector, which we are conscious, is merely one constituent of a vast array of providers or Information Society Services (ISS) that may fall under the rubric of the Code. In September 2021, the ICO further published a 'Sample Data Protection Impact Assessment (DPIA): Mobile Gaming App' to be read in tandem with the Code.¹

Nevertheless, two months after the passage of the enforcement deadline, outstanding areas of uncertainty remain. We understand that is, in part, a natural consequence of the sample DPIA being centred on a game intended for children between the ages of five and eight.² Uncertainty is most acute for games with potentially mixed audiences, and at the root of this, lies unsureness about age assurance expectations.

Therefore, the Forum roundly welcomes the ICO's efforts to provide additional clarity on age assurance in respect of the Code, both through the provision of an Opinion and this call for evidence. Furthermore, whilst we understand that the call for evidence is focused on age assurance as it pertains to the Code, we are mindful that the Opinion issued in parallel, indicates that the age assurance question is of domestic cross-regulatory significance, particularly in relation to the Online Safety Bill.³ As the Opinion explains:

It is likely that our work with Ofcom will become more extensive given their role as regulator for video sharing platforms (VSPs) and future regulator for online safety. We will work together with Ofcom and other regulators to ensure a coherent approach, particularly in the event that we engage with the same ISS at the same time.⁴

¹ <https://ico.org.uk/for-organisations/childrens-code-hub/additional-resources/sample-data-protection-impact-assessment-mobile-gaming-app/>

² Note: Another point of uncertainty is why content-led ratings, should act as a guiding post for compliance with a Code that is primarily about data processing risk (this is addressed at points 4 and 5).

³ <https://www.gov.uk/government/publications/draft-online-safety-bill>

⁴ <https://ico.org.uk/media/about-the-ico/documents/4018659/age-assurance-opinion-202110.pdf>
mobilegamesintelligence.com



The scope of this response to the call for evidence: In recognition of our being a participatory Forum, rather than a research team or company with specific expertise in digital identification technology, we are limiting our response to a principles and perspectives based statement:

Protecting children is essential

1. First and foremost, the Forum regards protecting the safety of younger users as of the utmost importance – recognising that children need special safeguards and care in all aspects of their life. We can definitively respond to question 19 of the call for evidence and state our willingness to participate in forthcoming roundtables. We are cognisant that the feasibility and efficacy of age verification and estimation approaches may improve significantly over the next five years. The Forum is willing to work alongside pan-European regulators, NGO's and other trade bodies in discussing age assurance possibilities.

There is no clear definition of age assurance

2. As to the current state of understanding, we wish to highlight that age assurance is an inherently nebulous concept, reflecting a topic whose parameters are fluid and ill-defined. The Opinion at 1.3, explains that age assurance refers 'collectively' to different approaches that a) provide assurance that children are unable to access content b) estimates or establish the age of a user. We are in agreement, that a diverse range of methodologies may constitute age assurance, including age verification, age estimation, account confirmation, self-declaration and parental controls.⁵
3. Differing definitions and interpretations are an inevitable consequence of a still-emerging area. There does, however, appear to be a consensus that the application of age assurance to ISS involves complex, graduated, and delicate balancing acts for which there are, yet, no agreed thresholds of proportionality, or cut and dry technological answers. Illustrative, are remarks made during a debate on the Online Safety Bill by the Australian e-Safety Commissioner, Julie Inman Grant in March 2021: *'There also are different levels of what we call age assurance. There is age gating, there's age assurance and then there's age verification, There are a lot of considerations. It's not a yes or no ... question.'*⁶

Age assurance technology is still in its infancy

4. Yet to exist, is a landmark breakthrough in digital identification or age estimation technology that squares the circle between functionality, robustness and data protection at developer level, such that the Forum can point to a universal, one size fits all, age assurance solution for mobile games. This is reflected in Recommendation 7 of the French data protection regulator (CNIL) *recommandations pour renforcer la protection*

⁵ 'There is flexibility for you to decide how to apply this standard in the context and circumstances of your online service' (Standard 3 – Age-Appropriate Application).

⁶ Remarks by Australian E-Safety Commissioner, Julie Inman Grant to the of the Environment and Communications Legislation Committee hearing into the Online Safety Bill 2021 (March 5th, 2021): *'There also are different levels of what we call age assurance. There is age gating, there's age assurance and then there's age verification, which actually verifies that that is little Johnny sitting behind the compute ... it depends on how much assurance you think you need in that particular system. There are a lot of considerations. It's not a yes or no or black or white question. It will come down to how much risk or certainty you're willing to accept.'*



des mineurs en ligne (June 2021) which acknowledges that there is no ‘miracle solution’ to age verification since available technologies are either too intrusive or ineffectual.⁷

More research is needed into differing approaches to age assurance

5. Against a backdrop of piecemeal approaches to age assurance, the Forum welcomes the ICO’s drive to undertake an exhaustive market survey of existing and proposed technologies, which will undoubtedly boost understanding. However, we respectfully suggest that a ‘call for evidence’ may be premature before more substantive research has been conducted. We are unaware of an established evidence base of peer-reviewed research on the application of age verification, age estimation, self-declaration or any other potential age assurance methodology to ISS, in respect of those areas itemised by the call for evidence: technical feasibility, accuracy, perspectives of children and parents, economic impacts, data protection risks, fairness, the avoidance of discrimination and algorithmic bias.
6. There are notable exceptions that aim to meet this research shortfall: for example, euConsent.⁸ As part of this ongoing project, a review of existing research in the field was conducted (potentially the only publicly available synopsis of existing research) - *Understanding of user needs and problems: a rapid evidence review of age assurance*.⁹ However, out of 61 studies only a single study identified by the appendix as encompassing ‘age assurance,’¹⁰ meaningfully considers the application of age verification to ISS likely to fall under the rubric of the Code – in this instance as part of a wider survey of VSP users.¹¹ This is indicative of an embryonic area of study.
7. Indeed, to the best of our knowledge, the only significant research commission that considers the application of age verification technology to online gaming was a 2012 study conducted by the University of Oxford Internet Institute. Its findings included that:
 - a. There is unlikely to be a ‘one-size fits all’ single model of age verification that suits a diversity of business needs.
 - b. The level of assurance (reliability) needed will vary across transactions and all business sectors place a value on certain core principles, most importantly proportionality.
 - c. The costs of age verification measures to be introduced must deliver enough benefit to the customer.¹²

⁷ <https://www.cnil.fr/fr/recommandation-7-verifier-lage-de-lenfant-et-laccord-des-parents-dans-le-respect-de-sa-vie-privee>.

⁸ <https://euconsent.eu/>

⁹ Smirnova S, Livingstone S and Stoilova M, (London: EuConsent, 2021)

¹⁰ Note: This is defined as a ‘means of verifying the age of users with various degrees of certainty.’

¹¹ Ofcom & Yonder (2021). User experience of potential online harms within video sharing platforms.

¹² <https://www.oii.ox.ac.uk/research/projects/effective-age-verification-techniques/#publications>
mobilegamesintelligence.com



Content ratings are not indicative of the intended audience or resulting data protections

8. We wish to address the specific problem of conflating content and data protection in respect of age assurance. Whilst content ratings¹³ are part of the wider age assurance ecosystem, they are not necessarily a reflection of the intended audience or, in any way, aligned with considerations of data protection risk. On the one hand, a game with a higher age rating, linked to platform parental controls, may indicate an older audience. Whereas, on the other hand, a game with a lower content age rating is not necessarily designed or intended for, or played by, young audiences. Instead, through the lower rating, the developer has indicated that the game does not contain explicit themes and is therefore suitable for younger audiences as distinct to being aimed at them. Moreover, neither the lower nor higher rating is a gauge of data protection risks relevant to the game: it reflects the content type.
9. For the above reasons, we respectfully question why the sample *Cooking Numbers App*, around which the *Mobile Gaming DPIA* revolves, appears to use the fact of a ‘PEGI rating of three meaning that it is suitable for all age groups,’ as such a prominent guiding post for the intended/ actual audience. By way of comparison with TV ratings, the popular Channel 4 lifestyle show *Location, Location, Location* may be considered suitable for young viewers, though they are not the intended audience. Growing confusion between data protection and content regulation is evinced by the recent misinterpretation of the ambit of the UK Code by lawmakers in the US, covered in the tech media.¹⁴
10. We also respectfully ask for further clarification as to the rationale underpinning the recent statement by ICO Commissioner, Elizabeth Denham, that ‘we have contacted Apple and Google to enquire about the extent to which the risks associated with the processing of personal data are a factor when determining the age rating for an app.’¹⁵

Mobile games require separate considerations such as platform first age assurance

11. There is a legal precedent from the United States that mobile games should be considered a distinctive sub-category of video games due to factors such as the freemium pricing model, demographics, growth rate and preponderance of the casual genre.¹⁶ It follows that the application of age assurance to mobile gaming, is likely to warrant specific considerations. For instance, the ICO should consider if the fact that casual and hyper-casual games¹⁷ dominate mobile games has a bearing on the

¹³ Note: Of the major app stores, Apple and Google use two different age rating systems to classify games. Google assigns content age ratings according to PEGI (Pan European Game Information) and Apple uses its own system. Developers must fill out a questionnaire prior to being allocated a rating. Embedded parental control tools are available across devices and platforms, restricting access in accordance with the allocated age rating.

¹⁴ Note: The Code provides: ‘You must consider the potential impact on children and any harm or damage your data processing may cause – whether physical, emotional, developmental or material. You should also specifically look at whether the processing could cause, permit or contribute to the risk.’ Nonetheless, in the US the ambit of the Code has been misinterpreted (see <https://kotaku.com/democrats-are-already-bungling-new-call-for-laws-to-pro-1847457366>).

¹⁵ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/letter-to-5rights-foundation/>

¹⁶ <https://www.leagle.com/decision/infdc020210914723>

¹⁷ **Note:** For example, casual games, the largest category of mobile games, are quick to learn, easy to play and typically played in short time bursts. For hyper-causal games, the fastest-growing category, the average playing time is just and two and a half minutes, and for ultracausal games, this can be even shorter.



proportionality of assurance methodology. Another ‘mobile games centric’ aspect of age assurance that may require detailed consideration is how approaches can operate within the context of platform ecosystems that characterise the market.

12. There may be unique complications regarding the application of potential AI-based methods to mobile games. It is easier to assess age via ads clicked or videos watched versus gameplay patterns meaning that this form of age assurance is more feasible for ad-based content providers rather than in-app purchase based, freemium models that dominate the sector. Therefore, to apply to all games, AI-based methods would have to work in concert with age information derived for credit card details and platform logins. These are just some facets of the age assurance question for mobile games that warrant further exploration.

A consistent international approach to age assurance is crucial

13. As a Forum, we are keenly interested in pan-European developments and, support a harmonised approach to regulatory guidance and self-regulation. A cursory survey of comparable children’s codes emerging across Europe, reveals that approaches to age assurance coalesce and diverge:
 - a. Although akin to the UK, the Irish *Draft Fundamentals*¹⁸ appear to require age assurance as proof of ‘actual audience’, the Swedish *Rights of Children*¹⁹ and the French *Recommendations*,²⁰ focus on the ‘intended audience.’²¹
 - b. Rather than deploy the term, ‘age assurance,’ the Swedish *Rights of Children* prefers ‘age control,’ maintaining that, ‘there are no exact rules for how to carry out age checks, but such checks should be preceded by a risk assessment and not entail any unreasonable processing of personal data.’²² Meanwhile, the Dutch *Code*,²³ aims to be more prescriptive, advising self-declaratory tools in low-risk instances, supplemented by additional measures to discourage and/or detect false age declarations.²⁴
 - c. Such age assurance guidance that could be deemed mobile games specific, has tended to acknowledge the use of platform-driven parental controls. For example, The Dutch *Code* and the Swedish *Rights*.²⁵
14. The course of implementation for much of the above European guidance and legislation has yet to be determined. Nonetheless, the downsides of a fragmented pan-European environment are worth flagging. An uncertain, prohibitive and variable compliance burden across multiple jurisdictions, may mean that innovation is stymied, and developers are disincentivised from bringing games to market.

¹⁸ [Draft Fundamentals for a Child-Oriented Approach to Data Processing](#)

¹⁹ [Rights of Children and Young People on Digital Platforms](#)

²⁰ [Recommendations Pour Renforcer la Protection des Mineurs en Ligne](#)

²¹ **Note:** The French *Recommendations* refer to the ‘publics visés’ and the Swedish *Rights* refer to the ‘average member of the intended audience.’

²²

https://www.statensmedierad.se/download/18.5d6370d1784af9360f23c50/1619597618455/The%20rights%20of%20children%20and%20young%20people%20on%20digital%20platforms_Accessible.pdf

²³ [Code Voor Kinderrechten](#)

²⁴ https://codevoorkinderrechten.nl/wp-content/uploads/2021/03/20210311_Code-voor-Kinderrechten_v1-1.pdf

²⁵ [Code Voor Kinderrechten](#), p.62; The rights of children and young people on digital platforms, p.35.



A consistent domestic approach to age assurance regulation is essential

15. The risk of domestic cross-regulatory confusion is real and pressing. Forthcoming online safety legislation may require age assurance methodologies to determine whether a service is ‘likely to be accessed’ by children – in this instance, to determine whether a commensurate duty of care applies. Equally, this could be an opportunity for the UK to set the lead in providing a consistent, non-prescriptive, flexible compliance framework in this difficult and undeveloped area, that gives space for emerging technologies and approaches to develop and crystallise over time - and we are gratified that the ICO is committed to working alongside Ofcom more extensively to ensure a coherent approach that clearly distinguishes between considerations of content and data protection.

Overly prescriptive age assurance could stifle the mobile games market

16. In the UK, mobile games developers are already deciding that the cost-benefit paradigm is weighted against granting younger audiences access to their games and yet, it is our understanding that a retreat into a walled garden of limited access to online services for minors is antithetical to the spirit of the Code. We respectfully suggest that it may be putting the horse before the cart, to seek or anticipate a prescriptive approach to age assurance, tied to regulatory enforcement, before technology and understanding has sufficiently matured. We note that the bar placed on the outcome to the call for evidence is high, despite the still-nascent state of technology and research:

This will enable us to keep up with technological developments and deepen our understanding of how industry is responding to the Code and the requirement for age assurance. It will also ensure that the guidance and support we provide is relevant and help us to regulate effectively and fairly.²⁶

17. China’s approach to age assurance has generated considerable media attention, relying upon ID checks through police databases. Since the end of 2018, it has raised concerns about user privacy and freedom.²⁷ As of September 21st 2021, additional restrictions for under 18 players were introduced by The National Press and Publication Administration (NPPA). The resulting existence of an illicit market enabling minors to circumvent age restrictions made the global tech press.²⁸ Fortnite (Epic Games) has announced its intention to exit China as of November 15th 2021.²⁹ The decision warrants further reflection as it led to an MMORPG³⁰ developer with extensive legal and compliance resources to leave a market with vast growth potentialities less than four years after it first entered (April 2018).

²⁶ <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-evidence-on-the-use-of-age-assurance/>

²⁷ [Tencent games will verify IDs to limit playing time for children](https://www.engadget.com/2018-11-27-tencent-games-will-verify-ids-to-limit-playing-time-for-children-1847627630.html) (Engadget, November 5th, 2018)

²⁸ <https://kotaku.com/chinas-new-gaming-restrictions-have-already-been-circum-1847627630>

²⁹ https://kotaku.com/fortnite-is-shutting-down-its-service-in-china-1847972821?utm_campaign=Kotaku&utm_content=1635766606&utm_medium=SocialMarketing&utm_source=twitter

³⁰ Massive multiplayer online role-playing game.



About MGIF

The Mobile Games Intelligence Forum was established in January 2020 to discuss and debate issues facing the sector and its place within the global video games industry. Rather than a representative body or a trade group, MGIF is a European focused participatory Forum, sharing mobile games insight and perspectives. A range of developers of differing sizes participate in the Forum, including King, Miniclip, Playrix, Playtika, Roblox, Rovio, Supercell, Wargaming, and Zynga. They have in common a passion for mobile games. This paper does not represent the views of any single company, rather it is a sum of knowledge shared between MGI and Forum participants.³¹

³¹ This response does NOT represent any one company's position, rather it is a sum of knowledge shared between MGI and Forum participants.