Open Rights Group submission to the Information Commissioner's Office

The use of age assurance

3 January, 2022

1. Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 20,000 active supporters, we are a grassroots organisation with local groups across the UK.
2. ORG recognise the need to protect children in the online space, and promote a responsible attitude among service providers. We also emphasise that age assurance methods will interact and interfere with other fundamental rights. We will focus on issues arising in the field of privacy and data protection. In particular, we address the comments that the Commissioner made in "methods of age assurance" (section 2.3).
3. **In summary, we recommend that:**
    1. Self-declaration or account confirmation should not be discarded in favour of other means of age assurance, in particular where these would constitute a more serious interference with users' right to privacy.
    2. Age assurance methods based on estimation should never be mandated or justified, as they would constitute a disproportionate interference with users' right to privacy and data protection, while exposing users of all ages to certain harm.
    3. Reliance on age assurance methods based on verification should be limited to high-risk scenarios. Where age verification procedures have the potential to hinder the exercise of fundamental rights or expose users to disproportionate requests, service providers should rely on less intrusive means of age assurance. Alternatively, service providers should be asked to lower the level of risk of their activities.
4. Concerning age assurance methods based on self-declarations (2.3.4) or account confirmation (2.3.3), the Commissioner points out that these systems

are easy to circumvent, in particular for "determined or knowledgeable" children. However, this is no less true for other age assurance methods envisaged by the Commissioner. Children will be able to circumvent any age assurance process for services offered outside of the United Kingdom, either by relying on Virtual Private Networks or Proxies. Alternatively, age estimation and age verification processes meant to identify children's accounts can be circumvented with relative ease. Password protection is unlikely to dissuade children from accessing an account owned by an adult, particularly where adult and child live in the same household. Children can also easily obtain credit cards or other identifying documents from their parents, with or without their knowledge. Possible measures to reduce these risks — such as biometric monitoring — are unwarranted: they would be incredibly disproportionate, and expose children and adults to certain harm (more on §7-9).

5. Therefore, reliance on self-declaration or account confirmation should not be discarded in favour of other means of age assurance, in particular where these would constitute a more serious interference with users' right to privacy.

6. Concerning age assurance methods based on estimation (2.3.2), either employing behavioural profiling or biometric assessment, we cannot but emphasise that these methods would constitute a disproportionate interference with users' right to privacy and data protection.

7. Behavioural profiling is a particularly invasive and exploitative practice whose risks for individual rights have been thoroughly documented.[1] This led to the call to ban behavioural profiling for commercial purposes in the European Union and the United States. Likewise, several children rights organisations in the UK are calling for a ban on behavioural profiling of children.[2]

8. The use of biometric data "for the purpose of uniquely identifying a natural person" is prohibited by Article 9 of the UK GDPR, unless a suitable condition set in Article 9(2) applies. In this context, Article 9(2)g requires that the law that authorises such use "is necessary for reasons of substantial public interest", and "respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". Further, the use of biometric data to estimate users' age would inevitably constitute large scale data processing and monitoring, thus triggering the need for a Data Protection Impact Assessment under article 35 of the UK GDPR. Such an intrusive and high-risk data processing hardly constitutes a proportionate interference with article 8 of the ECHR, and represents a disproportionate approach to age assurance that would not "respect the essence of data protection". As for behavioural

1 https://neweconomics.org/2021/05/how-can-we-resist-surveillance-advertising
2 https://neweconomics.org/2021/05/ban-surveillance-advertising-to-protect-kids-online

profiling, the legitimacy of biometric systems has been challenged in the US and the EU. Likewise, legal challenges have been raised in the UK against the MET police[3] and the use of biometric recognition in schools.[4]

9. It is also worth mentioning that behavioural profiling and the use of biometric data have already proven to be error-prone and at stake with the principles of accuracy and fairness. For instance, ORG ran a subject access request project that exposed several errors and misrepresentation in political profiling in the context of the 2019 General Elections.[5] Biometric recognition software has also proven to be prone to errors, particularly where minorities or other under-represented groups are involved. In other words, these methods are unreliable and frequently based on pseudoscience.[6]
10. Combining these factors makes age estimation systems intrusive from a data protection perspective, inaccurate, and potentially discriminatory from an equality perspective. Rather than protecting children, such measures would expose them to privacy harms and discrimination. Internet users would risk being denied services based on unfair and arbitrary estimates' of their age.
11. Concerning age assurance methods based on verification, we share the Commissioner's view that their use should be limited to high-risk scenarios. We also emphasise that privacy risks and the potential of these processes to interfere with individuals' rights should be taken into account, in particular:
    1. Verification processes could constitute a barrier to the exercise of fundamental rights, such as the right of free speech, free association and anonymity.
    2. Verification processes could expose Internet users to disproportionate requests, such as to hand over bank statements, utility contracts or other information that is revealing of their social status or could be exploited for commercial purposes.
12. Where age verification had the potential to expose Internet users to the issues mentioned above, service providers should rely on less intrusive means of age assurance, such as self-declaration or account confirmation.
13. Alternatively, service providers should be asked to lower the level of risk of their activities. In particular, if such activities consist in large scale profiling, invisible processing, tracking and targeting (section 3.2), users' rights should prevail. Asking children to undergo yet another privacy-intrusive procedure to avoid or mitigate risks they are not responsible for would be fundamentally

3 https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/

4 https://www.euronews.com/next/2021/10/18/schools-in-scotland-start-using-facial-recognition-on-children-paying-for-lunch

5 See page 9 at https://www.openrightsgroup.org/app/uploads/2020/07/200619%E2%80%94org%E2%80%94report.pdf

6 https://medium.com/viewpoints/cambridge-analytica-and-the-big-data-panic-5029f12e1bcb

unfair, and Information Society Services should not be allowed to shift the burden of their poor privacy designs onto Internet users.

14. Open Rights Group remains available for any questions or follow up concerning this submission.