Submission of the European Digital Rights (EDRi) network, representing 50+ national and international digital human rights NGOs

To the Irish *Coimisiún na Meán* draft Online Safety Code consultation

30 January 2024

About EDRi

EDRi (European Digital Rights) is Europe's largest digital human rights network working to protect digital rights for everyone. The EDRi network is a dynamic and resilient collective of NGOs, experts, advocates and academics working to defend and advance digital rights across the continent. For over two decades, it has served as the backbone of the digital rights movement in Europe.

Our mission is to challenge private and state actors who abuse their power to control or manipulate the public. We do so by advocating for robust and enforced laws, informing and mobilising people, promoting a healthy and accountable technology market, and building a movement of organisations and individuals committed to digital rights and freedoms in a connected world.

General comments about our submission

While there are many notable elements of the draft Code, this submission is limited to one particular area of concern for EDRi: age verification. We have therefore chosen to answer only those questions which are directly relevant to our work on age verification. This does not necessarily mean that we endorse or oppose other parts of the code, but

rather that our input is strictly limited in scope. **However, we would like to express that we support the submission of EDRi affiliate, the Irish Council for Civil Liberties (ICCL), on stopping toxic recommender algorithms by default.**

Our input here is based on research conducted by EDRi and supported by nineteen other organisations, including the children's digital rights group, Defend Digital Me. This research was published in October 2023 in the form of a paper entitled 'Online age verification and children's rights'.[1] **This research paper forms a key part of our submission, and therefore we ask the Commission to consider it as an integral part of our submission. We also reference it throughout.**

The aim of protecting children online is a very important one. Drawing from many years of work to contest the disproportionate power of online platform, EDRi therefore supports the introduction or maintenance of clear, consistent and binding rules for online service providers and platforms. These rules must ensure that they meet their obligations to protecting their users, but also must respect the full range of EU fundamental rights, including the prohibition of general monitoring.

At the same time, we have serious concerns about age verification in general, and specifically about the age verification methods foreseen by the Code, its accompanying Statutory Guidance Materials and in public comments about the Code.

The aim of our consultation response is thus to raise awareness of the complexities surrounding age verification practices, the significant technical challenges involved in ensuring a data- and privacy-protective age verification system, the commercial interests which have influenced discourse, and most crucially, **the threats posed to the human rights of children and adults alike by all current methods of age verification that we surveyed**.

Our work is based on the rights conferred by the Charter of Fundamental Rights of the EU, and as such is rooted in a necessity and proportionality assessment of age verification methods. **We believe that there are serious questions about whether mandatory age verification can be considered proportionate, and whether systems are effective enough to meet the requirement of necessity**.

Please note that throughout this submission, unless otherwise specified, we use the term 'age verification' as a broad umbrella to include both document-based identity systems and age estimation systems.

1 https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf

Response to consultation question 9: "What is your view on the requirements in the draft Code in relation to age verification?"

Concerns about the proposed widespread age verification mandate

The draft Code requires video-sharing platform service providers "of which the principal purpose of the service or a dissociable section thereof is providing access for adults to content consisting of pornography" or "of realistic representations of, or of the effects of, gross or gratuitous violence or acts of cruelty" (Sections 11.3 and 11.4) to implement "**robust age verification**".

For service providers not falling within this scope, they must still implement "**effective age verification**" (Sections 11.6 and 11.7). Those showing alcohol adverts must also implement "**effective age verification**" (Section 12.9). These terms are not, however, defined by the Code. "Effective" is defined only in the non-binding Statutory guidance.

In addition, any service with a minimum age for opening an account (which, thanks to rules established in Article 8 of the General Data Protection Regulation (GDPR) presumably means all services), must "implement **effective measures to detect under-age users** and close their accounts" (Section 11.16).

In effect, therefore, the Code amounts to an obligation to use age verification, age estimation or another form of "detect[ion] of underage users" for practically all video-sharing platform service providers based in Ireland. Given the number of tech giants registered in Ireland, including *inter alia* widely-used service providers like YouTube and Instagram, such a decision will have a wide impact across the European Union.

The Code also allows providers to repeatedly assess the ages of their users each time they access certain content (Section 11.19(ii)). The use of such perpetual or recurring age verification measures can incentivise not just excessive collection, but also storage, of sensitive personal data. Yet the risks of such practices are not mentioned at all in the Code.

Based on research conducted in Autumn 2023, EDRi has found that all current age verification and age estimation methods that we could find fail to meet strong standards of protection of the rights to personal data and privacy. This is first of all for children themselves, but also for adults, who will invariably have their data processed by these systems too. In addition to threats to privacy and data protection, we found that these systems can also pose potentially serious limitations on the rights to free expression, free association, access to information, non-discrimination and dignity, as well as the rights of the child.

For this reason, we do not support mandatory widespread age verification or estimation, and instead recommend a case-by-case assessment to see whether age verification/estimation tools are genuinely necessary and proportionate for a given platform or service.

By presenting the genuine challenge of children's safety online as a problem that can be solved with surveillance measures, we are concerned that this encourages a slippery slope towards broader surveillance of people's internet activity, censorship, and a push to eradicate online anonymity.

The risk of this 'slippery slope' can even be seen in several alarming responses to the previous public consultation: "*In response to the call for inputs, some stakeholders proposed that the Code should also restrict the promotion of breast milk substitutes and of high fat, salt and sugar foods*" (p.15). This techno-solutionist approach also risks focusing too much on technology, rather than focusing on the broader societal context which leads to harm.

Our first recommendation for the Code is therefore that at a minimum, the potential risks and harms of age verification and estimation methods must be explicitly mentioned in the Code. Additionally, providers must be required to address each of them.

The urgent need for *ex ante* safeguards

There are no limitations or restrictions placed on the use of age verification or estimation systems by the Code. The focus is on technical accuracy ("robustness" or "effectiveness" requirements), but this eclipses a significant set of important considerations around privacy, data protection, online freedom and more. Even the accompanying Statutory Guidance Materials contain very little information or advice about safeguards, and do not set any limits on the use of age verification or estimation.

By presenting the use of age verification and estimation tools as *only* a mitigation measure, rather than as a potential risk in themselves too, the Code misses an important opportunity to ensure that such tools are used in a way which respects the rights of children and adults online.

Given the risks posed by the use of age estimation and verification systems, explained in this submission and in our aforementioned research paper, we strongly recommend the inclusion of a set of cumulative, binding safeguards incorporated into the Code itself.

Our second recommendation, therefore, is that the Code should stipulate that any age verification or estimation system must:

- Permanently prevent any linking of the internet activity or history of a person to their identity, ensuring that a person cannot be traced by the use of the system (i.e. 'zero knowledge');
- Not provide any information to the provider other than a yes/no about their age threshold; and must not facilitate any access to the person's account or information by the provider or by a parent, guardian or other actor;
- Consider using tokens instead of storing personal data, and delete personal data processed for the purpose of generating the token immediately afterwards;
- Not allow any data collected or processed to be used for any other purpose, commercial or otherwise;
- Not allow the processing of biometric data;
- Be robust and secure from a cyber-security perspective;
- Be consent-based, and not overly burdensome for those who do not want or do not have the means to verify their identity in an overly prescriptive way;
- Ensure genuine alternatives for those that do not have formal identity documents, ensuring that minoritised (marginalised) or otherwise vulnerable people will not be locked out of the internet;
- Be mindful of a potential chilling effect, in particular ensuring that access to educational and health (including reproductive health) material is not subject to age verification, which could have a chilling effect on whether or not children feel comfortable accessing this information.

Given that all available technologies that EDRi surveyed failed (significantly) to meet these requirements, it is important that providers are not forced to implement non-secure or privacy-invasive systems.

Therefore, our third recommendation is that if no technologies are available which meet these thresholds, the service provider must not be obligated to implement age verification or estimation measures.

<u>Concerns about disincentivising age self-declaration</u>

The Code states that "[s]elf-declaration of age by users of the service shall not on its own be an effective measure for the purposes of this section" (Sections 11.16 and 11.17).

However, EDRi's research has found that supplemented with other measures (focused around the principles of safety by default and by design), self-declaration currently offers the most realistic and appropriate balance of minimising intrusiveness and data collection, whilst ensuring some form of age gating. By preventing providers from being able to rely on self-declaration methods in order to meet their obligations under the Code, they will be forced to implement age verification or estimation tools, even when such tools are known to be harmful.

Our fourth recommendation is therefore that the Code should allow providers to rely on age self-declaration, so long as they ensure privacy and security by default.

Measures in the Code that we support in principle

According to the Code, violent or distressing imagery uploaded in the public interest must be rated as "not suitable for children" (11.8) as part of this system. In theory, we find that content labelling can be a useful tool, which focuses on empowering users (or in the case of younger children, their parents) to make decisions for themselves.

This is important with respect to the growing autonomy of children, the role of parents' in fulfilling the rights of the child, and the need to acknowledge that young people are not a homogenous block. There may be times where access to content is not just not harmful, but actually beneficial, for children. For example, this could include exposure to risk (within reason) in order to build resilience, or access to LGBTQI+ content for older adolescents exploring their sexuality or gender identity. This is particularly important given that the Code will have ramifications for users across the Union, including in countries where LGBTQI+ people face persecution.

Another reason to support discretionary measures such as age rating, rather than more prescriptive measures like age verification or estimation, is that it allows parents to maintain a level of oversight and support of their children's online activity. Otherwise, there is a risk that the rights of the child could be violated, by replacing parental responsibility for what content is appropriate with service provider responsibility for what content is appropriate. This is especially a risk when talking about potentially harmful, but not illegal, content.

Nevertheless, we caution that age labelling should not be linked to age estimation or verification measures, as its benefit lies in the fact that it guides and empowers, rather than restricts, users.

We further caution that the definition of "children" can be problematic in the case of content labelling. For example, several EU Member States allow people to vote at the age of 16 or 17. In order to ensure that they are able to fully participate in these democratic processes, there may be a legitimate argument for allowing them to view content that is violent or distressing, but not illegal. As a broader principle, it is frequently not appropriate to restrict the access to content of older adolescents, compared to younger children. We find it problematic that the Code does not make any such distinction.

Reporting requirements (Section 11.21) and complaint mechanisms (11.29) are in principle important measures. However, we warn that they do not replace ex ante (i.e. prior), and even substantive (i.e. prohibitive), safeguards as mentioned already in this submission.

We strongly support the provision that personal data relating to children when implementing this Code cannot be processed for commercial purposes (13.3).

The risks to adults

Whilst the aim of protecting children online is a legitimate and important goal, it is important to remember that it does not automatically take priority over all other interests. In fact, as asserted by the UN Convention on the Rights of the Child, the best interests of the child must be "a primary interest", but not the *only* interest. This means that the protection of the child must also be weighed against, *inter alia*, the risks to the rights of adults, and to a free and democratic society, if adults are prevented from being anonymous online.

Regrettably, this is not properly considered by the draft Code. Whilst, for example, Sections 11.18 and 11.20 require service providers to "set targets for the number of children (in different age ranges determined by the service provider) who are wrongly identified as adults through the service provider's age verification, age estimation or other technical measures," there is no corollary for adults who have been misidentified as children.

Furthermore, this very framing of "set[ting] targets" suggests acceptance of a relatively low level of accuracy, accepting wrong identification as a feature. However, there are many rights at stake here for children and adults alike, including access to information and freedom of expression. Therefore wrong identification should not be passively accepted, but the regulator should instead require a high degree of accuracy. This is especially the case in the event that the processing of biometric data are allowed (even though we warn against it, as the biometric data of children are especially sensitive). Estimation on the basis of biometric data has been plagued with bias and discrimination, and despite industry commitments to counter this, it remains that racialised people and people with certain disabilities are still discriminated against by these systems.

Responses to other questions in the consultation about the Code

11. What is your view on the requirements in the draft Code in relation to parental controls?

Although we regret that we have not been able to assess the parts of this Code which relate to parental controls, we would like to make some general remarks based on our research. We believe that while parental support tools can be useful, it is not appropriate for parents to 'control' the internet use of their children, especially adolescents. Therefore, the use of such tools should always be used with the full knowledge of the child, and must never allow access to the content of communications.

19. What is your view on the requirements in the draft Code in relation to ensuring the personal data of children is not processed for commercial purposes?

We strongly support this provision, and in fact would extend this to require that personal data processed for any purpose under this Code cannot be processed for another purpose. This is consistent with the purpose limitation requirement of the GDPR.

Opinion on the Statutory Guidance Materials

General

We find it problematic from the perspective of legal certainty that terms referred to in the binding code, such as "effective age verification" and "robust age verification" are used in the binding Code, but defined only in the non-binding Guidance.

Age estimation

Whether through the processing of biometric data (e.g. facial estimation) or by other forms of profiling, we find age estimation to be antithetical to the very essence of privacy and data protection. Biometric data are a special category of protected data under the GDPR. Therefore from a data protection perspective, we question the necessity and proportionality of the use of these sensitive data.

On a societal level, we are alarmed at how such measures could normalise the sharing of sensitive biometric data in order to participate in daily activities. Given that children's biometric data are *even more sensitive* than that of adults, we find that there must be an exceptionally high threshold for their use, and we are not satisfied that this has been established by the Code.

For systems which profile young people based on their usage or behaviours, this is the exact sort of toxic data collection by platforms which we have spent years fighting. It may also violate rules laid down in the EU's Digital Services Act.

The guidance materials state that age estimation must "comply … with data protection and privacy requirements" (p.68) However, no description or explanation of what this means is given. As in the Code, this is a missed opportunity to demand prescriptive safeguards.

Without such safeguards, we believe that the Code and related Guidance materials is likely to do more harm than good, and may violate the requirement under the EU Charter of Fundamental Rights that when fundamental human rights are limited by law, appropriate safeguards must also be laid down in that law. In accordance with case law from the Court of Justice of the EU, this is especially the case when it comes to the processing of biometric data.

Document-based age verification

The Guidance recommends the use of "document-based age verification at sign up and selfie or live likeness based age verification" (p.68). However, as our research has

confirmed, there is a significant risk of misuse of personal data when users are required to submit identity documents to a provider.

This may also violate the principle of data minimisation under the GDPR, as the user will be revealing not just whether they are above the age of 18, but sensitive information such as legal name, address, date of birth, nationality etc. This would not meet the requirement of proportionality under the Charter of Fundamental Rights of the EU, and also puts these data at risk of hacks. Given that the Code will also cover porn platforms, sensitive information about people's sexual orientation and preferences could also be at stake here.

As previously discussed, the use of "live likeness based" methods by definition process biometric data, which we do not find to be necessary and proportionate, and which we do not believe children should be conditioned into thinking is a 'normal' thing for accessing information and services. It is not clear what is meant by "live selfie plus biometrics", as the live selfie will already process biometric data, and it is not clear where the comparison "biometrics" would come from.

Effectiveness

The Guidance mentions the need to "minimise the error rate when children are misidentified as adult" (p.68), but the same principle should apply to adults being misidentified as children, which could see them locked out of services.

Tokenised age services

The Guidance materials state that "tokenised age services may be considered" (p.68). However, these services are frequently part of a lucrative 'age assurance' industry, and rely on users trusting a private, commercial entity. As discussed in our aforementioned research paper, the dominance of these commercial entities in policy debates about age verification has perhaps skewed perspectives, and obfuscated much-needed debates on the impacts on rights and freedoms.

If the Commission does mandate any sort of age verification or estimation measures, it should be ensured that private entities do not profit from this.

Adults' rights and freedoms

The Guidance also states: "The Commission advises video-sharing platform service providers to ensure that commercial communications which are only suitable for adults are displayed only to logged-in accounts whose holders have been identified as adults through effective age estimation or age verification techniques as appropriate" (p.72).

However, this could threaten adults' right to access the internet anonymously, jeopardising their online privacy on a massive scale. It is disappointing that the Code has paid almost no attention to the many serious risks entailed by age verification and estimation, and we look forward to an improvement in the future Code.

For more information about EDRi's work on age verification, please contact Ella Jakubowska, Senior Policy Advisor: ella.jakubowska@edri.org