OPEN RIGHTS GROUP

Age Verification Guidance

Response to the draft guidance from the BBFC laid before Parliament

November 2018

Analysis of BBFC's Post-Consultation Guidance

Summary

Following the conclusion of their consultation period, the BBFC have issued new age verification guidance to be laid before Parliament, which can be found here.

The new code has some important improvements, notably the introduction of a voluntary scheme for privacy, close to or based on a GDPR Code of Conduct. This is a good idea, but should not be put in place as a voluntary arrangement. Companies may not want the attention of a regulator, or may simply wish to apply lower or different standards, and ignore it. It is unclear why, if the government now recognises that privacy protections like this are needed, the government would also leave the requirements as voluntary.

We are also concerned that the voluntary scheme may not be up and running before the AV requirement is put in place. Given that 25 million UK adults are expected to sign up to these products within a few months of its launch, this would be very unhelpful.

Parliament should now:

(1) Ask the government why the privacy scheme is to be voluntary, if the risks of relying on general data protection law are now recognised;
(2) Ask for assurance from BBFC that the voluntary scheme will cover the all of the major operators; and
(3) Ask for assurance from BBFC and DCMS that the voluntary privacy scheme will be up and running before obliging operators to put Age Verification measures in place.

Lack of Enforceability of Guidance

The Digital Economy Act does not allow the BBFC to judge age verification tools by any standard other than whether or not they sufficiently verify age. We asked that the BBFC persuade the DCMS that statutory requirements for privacy and security were required for age verification tools.

The BBFC have clearly acknowledged privacy and security concerns with age verification in their response. However, the BBFC indicate in their response that they have been working with the ICO and DCMS to create a voluntary certification scheme for age verification providers:

> "This voluntary certification scheme will mean that age-verification providers may choose to be independently audited by a third party and then certified by the Age-verification Regulator. The third party's audit will include an assessment of an age-verification solution's compliance with strict privacy and data security requirements."

The lack of a requirement for additional and specific privacy regulation in the Digital Economy Act is the cause for this voluntary approach.

While a voluntary scheme above is likely to be of some assistance in promoting better standards among age verification providers, the “strict privacy and data security requirements” which the voluntary scheme mentions are not a statutory requirement, leaving some consumers at greater risk than others.

Sensitive Personal Data

The data handled by age verification systems is sensitive personal data. Age verification services must directly identify users in order to accurately verify age. Users will be viewing pornographic content, and the data about what specific content a user views is highly personal and sensitive. This has potentially disastrous consequences for individuals and families if the data is lost, leaked, or stolen.

Following a hack affecting Ashley Madison – a dating website for extramarital affairs – a number of the site’s users were driven to suicide as a result of the public exposure of their sexual activities and interests.

For the purposes of GDPR, data handled by age verification systems falls under the criteria for sensitive personal data, as it amounts to “data concerning a natural person's sex life or sexual orientation”.

Scheduling Concerns

It is of critical importance that any accreditation scheme for age verification providers, or GDPR code of conduct if one is established, is in place and functional **before** enforcement of the age verification provisions in the Digital Economy Act commences. All of the major providers who are expected to dominate the age verification market should undergo their audit under the scheme before consumers will be expected to use the tool. This is especially true when considering the fact that MindGeek have indicated their expectation that 20-25 million UK adults will sign up to their tool within the first few months of operation. A voluntary accreditation scheme that begins enforcement *after* all these people have already signed up would be unhelpful.

Consumers should be empowered to make informed decisions about the age verification tools that they choose from the very first day of enforcement. No delays are acceptable if users are expected to rely upon the scheme to inform themselves about the safety of their data. If this cannot be achieved prior to the start of expected enforcement of the DE Act’s provisions, then the planned date for enforcement should be moved back to allow for the accreditation to be completed.

Issues with Lack of Consumer Choice

It is of vital importance that consumers, if they must verify their age, are given a choice of age verification providers when visiting a site. This enables users to choose which provider they trust with their highly sensitive age verification data and prevents one actor from

dominating the market and thereby promoting detrimental practices with data. The BBFC also acknowledge the importance of this in their guidance, noting in 3.8:

> "Although not a requirement under section 14(1) the BBFC recommends that online commercial pornography services offer a choice of age-verification methods for the end-user".

This does not go far enough to acknowledge the potential issues that may arise in a fragmented market where pornographic sites are free to offer only a single tool if they desire.

Without a statutory requirement for sites to offer all appropriate and available tools for age verification and log in purposes, it is likely that a market will be established in which one or two tools dominate. Smaller sites will then be forced to adopt these dominant tools as well, to avoid friction with consumers who would otherwise be required to sign up to a new provider.

This kind of market for age verification tools will provide little room for a smaller provider with a greater commitment to privacy or security to survive and robs users of the ability to choose who they trust with their data.

We already called for it to be made a statutory requirement that pornographic sites must offer a choice of providers to consumers who must age verify, however this suggestion has not been taken up.

We note that the BBFC has been working with the ICO and DCMS to produce a voluntary code of conduct. Perhaps a potential alternative solution would be to ensure that a site is only considered compliant if it offers users a number of tools which has been accredited under the additional privacy and security requirements of the voluntary scheme.

GDPR Codes of Conduct

A GDPR "Code of Conduct" is a mechanism for providing guidelines to organisations who process data in particular ways, and allows them to demonstrate compliance with the requirements of the GDPR.

A code of conduct is voluntary, but compliance is continually monitored by an appropriate body who are accredited by a supervisory authority. In this case, the "accredited body" would likely be the BBFC, and the "supervisory authority" would be the ICO. The code of conduct allows for certifications, seals and marks which indicate clearly to consumers that a service or product complies with the code.

Codes of conduct are expected to provide more specific guidance on exactly how data may be processed or stored. In the case of age verification data, the code could contain stipulations on:

- Appropriate pseudonymisation of stored data;

- Data and metadata retention periods;
- Data minimisation recommendations;
- Appropriate security measures for data storage;
- Security breach notification procedures;
- Re-use of data for other purposes.

The BBFC's proposed "voluntary standard" regime appears to be similar to a GDPR code of conduct, though it remains to be seen how specific the stipulations in the BBFC's standard are. A code of conduct would also involve being entered into the ICO's public register of UK approved codes of conduct, and the EPDB's public register for all codes of conduct in the EU.

Similarly, GDPR Recital 99 notes that "relevant stakeholders, including data subjects" should be consulted during the drafting period of a code of conduct - a requirement which is not in place for the BBFC's voluntary scheme.

It is possible that the BBFC have opted to create this voluntary scheme for age verification providers rather than use a code of conduct, because they felt they may not meet the GDPR requirements to be considered as an appropriate body to monitor compliance. Compliance must be monitored by a body who has demonstrated:

- Their expertise in relation to the subject-matter;
- They have established procedures to assess the ability of data processors to apply the code of conduct;
- They have the ability to deal with complaints about infringements; and
- Their tasks do not amount to a conflict of interest.

Parties Involved in the Code of Conduct Process

As noted by GDPR Recital 99, a consultation should be a public process which involves stakeholders and data subjects, and their responses should be taken into account during the drafting period:

> "When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors **should consult relevant stakeholders, including data subjects where feasible**, and have regard to submissions received and views expressed in response to such consultations."

The code of conduct must be approved by a relevant supervisory authority (in this case the ICO).

An accredited body (BBFC) that establishes a code of conduct and monitors compliance is able to establish their own structures and procedures under GDPR Article 41 to handle complaints regarding infringements of the code, or regarding the way it has been implemented. BBFC would be liable for failures to regulate the code properly under Article

41(4),[1] however DCMS appear to have accepted the principle that the government would need to protect BBFC from such liabilities.[2]

GDPR Codes of Conduct and Risk Management

Below is a table of risks created by age verification which we identified during the consultation process. For each risk, we have considered whether a GDPR code of conduct may help to mitigate the effects of it.

Risk	**CoC Appropriate?**	**Details**
User identity may be correlated with viewed content.	Partially	This risk can never be entirely mitigated if AV is to go ahead, but a CoC could contain very strict restrictions on what identifying data could be stored after a successful age verification.
Identity may be associated to an IP address, location or device.	No	It would be very difficult for a CoC to mitigate this risk as the only safe mitigation would be not to collect user identity information.
An age verification provider could track users across all the websites it's tool is offered on.	Yes	Strict rules could be put in place about what data an age verification provider may store, and what data it is forbidden from storing.
Users may be incentivised to consent to further processing of their data in exchange for rewards (content, discounts etc.)	Yes	Age verification tools could be expressly forbidden from offering anything in exchange for user consent.
Leaked data creates major risks for identified individuals and cannot be revoked or adequately compensated for.	Partially	A CoC can never fully mitigate this risk if any data is being collected, but it could contain strict prohibitions on storing certain information and specify retention periods after which data must be destroyed, which may

[1] "Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: the obligations of the monitoring body pursuant to Article 41(4)."

[2] "contingent liability will provide indemnity to the British Board of Film Classification (BBFC) against legal proceedings brought against the BBFC in its role as the age verification regulator for online pornography."
https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2018-10-10/HCWS986/

		mitigate the impacts of a data breach.
Risks to the user of access via shared computers if viewing history is stored alongside age verification data.	Yes	A CoC could specify that any accounts for pornographic websites which may track viewed content must be strictly separate and not in any visible way linked to a user's age verification account or data that confirms their identity.
Age verification systems are likely to trade off convenience for security. (No 2FA, auto-login, etc.)	Yes	A CoC could stipulate that login cookies that "remember" a returning user must only persist for a short time period, and should recommend or enforce two-factor authentication.
The need to re-login to age verification services to access pornography in "private browsing" mode may lead people to avoid using this feature and generate much more data which is then stored.	No	A CoC cannot fix this issue. Private browsing by nature will not store any login cookies or other objects and will require the user to re-authenticate with age verification providers every time they wish to view adult content.
Users may turn to alternative tools to avoid age verification, which carry their own security risks. (Especially "free" VPN services or peer-to-peer networks).	No	Many UK adults, although over 18, will be uncomfortable with the need to submit identity documents to verify their age and will seek alternative means to access content. It is unlikely that many of these individuals will be persuaded by an accreditation under a GDPR code.
Age verification login details may be traded and shared among teenagers or younger children, which could lead to bullying or "outing" if such details are linked to viewed content.	Yes	Strict rules could be put in place about what data an age verification provider may store, and what data it is forbidden from storing.
Child abusers could use their access to age verified content as an adult as leverage to create and exploit relationships with	No	This risk will exist as long as age verification is providing a successful barrier to accessing such content for under-18s who wish to do so.

children and teenagers seeking access to such content (grooming).		
The sensitivity of content dealt with by age verification services means that users who fall victim to phishing scams or fraud have a lower propensity to report it to the relevant authorities.	Partially	A CoC or education campaign may help consumers identify trustworthy services, but it can not fix the core issue, which is that users are being socialised into it being “normal” to input their identity details into websites in exchange for pornography. Phishing scams resulting from age verification will appear and will be common, and the sensitivity of the content involved is a disincentive to reporting it.
The use of credit cards as an age verification mechanism creates an opportunity for fraudulent sites to engage in credit card theft.	No	Phishing and fraud will be common. A code of conduct which lists compliant sites and tools externally on the ICO website may be useful, but a phishing site may simply pretend to be another (compliant) tool, or rely on the fact that users are unlikely to check with the ICO every time they wish to view pornographic content.
The rush to get age verification tools to market means they may take significant shortcuts when it comes to privacy and security.	Yes	A CoC could assist in solving this issue if tools are given time to be assessed for compliance **before the age verification regime commences**.
A single age verification provider may come to dominate the market, leaving users little choice but to accept whatever terms the provider offers.	Partially	Practically, a CoC could mitigate some of the effects of an age verification tool monopoly if the dominant tool is accredited under the Code. However, this relies on users being empowered to demand compliance with a CoC, and it is possible that users will instead be left with a “take it or leave it” situation where the dominant tool is not CoC accredited.
Allowing pornography	Partially	As the BBFC note in their

“monopolies” such as MindGeek to operate age verification tools is a conflict of interest.		consultation response, it would not be reasonable to prohibit a pornographic content provider from running an age verification service as it would prevent any site from running their own tool. However, under a CoC it is possible that a degree of separation could be enforced that requires an age verification tools to adhere to strict rules about the use of data, which could mitigate the effects of a large pornographic content provider attempting to collect as much user data as possible for their own business purposes.