Analysis of BBFC Age Verification Certificate Standard
June 2019

About Open Rights Group

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

As society goes digital we wish to preserve its openness. We want a society built on laws, free from disproportionate, unaccountable surveillance and censorship. We want a society in which information flows more freely. We want a state that is transparent and accountable, where the public's rights are acknowledged and upheld.

We scrutinise and critique the policies and actions of governments, companies, and other groups as they relate to the Internet. We warn the public when policies — even well-intentioned ones — stand to undermine the freedom to use the Internet to make a better society.

Executive Summary

The BBFC's *Age-verification Certificate Standard* ("the Standard") for providers of age verification services, published in April 2019, fails to meet adequate standards of cyber security and data protection and is of little use for consumers reliant on these providers to access adult content online.

This document analyses the Standard and certification scheme and makes recommendations for improvement and remediation. It sub-divides generally into two types of concern: operational issues (the need for a statutory basis, problems caused by the short implementation time and the lack of value the scheme provides to consumers), and substantive issues (seven problems with the content as presently drafted).

The fact that the scheme is voluntary leaves the BBFC powerless to fine or otherwise discipline providers that fail to protect people's data, and makes it tricky for consumers to distinguish between trustworthy and untrustworthy providers. In our view, the

government must legislate without delay to place a statutory requirement on the BBFC to implement a mandatory certification scheme and to grant the BBFC powers to require reports and penalise non-compliant providers.

The Standard's existence shows that the BBFC considers robust protection of age verification data to be of critical importance. However, in both substance and operation the Standard fails to deliver this protection. The scheme allows commercial age verification providers to write their own privacy and security frameworks, reducing the BBFC's role to checking whether commercial entities follow *their own* rules rather than requiring them to work to a mandated set of common standards. The result is uncertainty for Internet users, who are inconsistently protected and have no way to tell which companies they can trust.

Even within its voluntary approach, the BBFC gives providers little guidance to providers as to what their privacy and security frameworks should contain. Guidance on security, encryption, pseudonymisation, and data retention is vague and imprecise, and often refers to generic "industry standards" without explanation. The supplementary Programme Guide, to which the Standard refers readers, remains unpublished, critically undermining the scheme's transparency and accountability.

Recommendations

Grant the BBFC statutory powers:

> *The BBFC Standard should be substantively revised to set out comprehensive and concrete standards for handling highly sensitive age verification data.*
>
> *The government should legislate to grant the BBFC statutory power to mandate compliance.*
>
> *The government should enable the BBFC to require remedial action or apply financial penalties for non-compliance.*
>
> *The BBFC should be given statutory powers to require annual compliance reports from providers and fine those who sign up to the certification scheme but later violate its requirements.*
>
> *The Information Commissioner should oversee the BBFC's age verification certification scheme*

Delay implementation and enforcement:

Delay implementation and enforcement of age verification until both (a) a statutory standard of data privacy and security is in place, and (b) that standard has been implemented by providers.

Improve the scheme content:

Even if the BBFC certification scheme remains voluntary, the Standard should at least contain a definitive set of precisely delineated objectives that age verification providers must meet in order to say that they process identity data securely.

Improve communication with the public:

Where a provider's certification is revoked, the BBFC should issue press releases and ensure consumers are individually notified at login.

The results of all penetration tests should be provided to the BBFC, which must publish details of the framework it uses to evaluate test results, and publish annual trends in results.

Strengthen data protection requirements:

Data minimisation should be an enforceable statutory requirement for all registered age verification providers.

The Standard should outline specific and very limited circumstances under which it's acceptable to retain logs for fraud prevention purposes. It should also specify a hard limit on the length of time logs may be kept.

The Standard should set out a clear, strict and enforceable set of policies to describe exactly how providers should "pseudonymise" or "deidentify" data.

Providers that no longer meet the Standard should be required to provide the BBFC with evidence that they have destroyed all the user data they collected while supposedly compliant.

The BBFC should prepare a standardised data protection risk assessment framework against which all age verification providers will test their systems. Providers should limit bespoke risk assessments to their specific technological implementation.

Strengthen security, testing, and encryption requirements:

Providers should be required to undertake regular internal and external vulnerability scanning and a penetration test at least every six months, followed by a supervised remediation programme to correct any discovered vulnerabilities.

Providers should be required to conduct penetration tests after any significant application or infrastructure change.

Providers should be required to use a comprehensive and specific testing standard. CBEST or GBEST could serve as guides for the BBFC to develop an industry-specific framework.

The BBFC should build on already-established strong security frameworks, such as the Center for Internet Security Cyber Controls and Resources, the NIST Cyber Security Framework, or Cyber Essentials Plus.

At a bare minimum, the Standard should specify a list of cryptographic protocols which are not adequate for certification.

Introduction

The Digital Economy Act 2017 ("DEA") requires commercial pornographic websites to implement controls that prevent individuals under the age of 18 from accessing pornographic content.

Actively verifying the age of visitors to commercial pornographic websites, as the law requires, is inherently highly sensitive, as it connects the identities of millions of UK adults to their adult content viewing choices. A data breach or cyber attack that causes information about individuals' choice of pornographic content to become public can have devastating consequences. Individuals' careers, relationships, mental health, and even lives - as shown by the 2015 Ashley Madison data breach - are at risk. Age verification (AV) providers must therefore be held to a high standard of data protection and keep the data they hold secure against external attacks and internal carelessness.

In April 2019, the British Board of Film Classification (BBFC), which the government has appointed as the AV regulator, published the "Age-verification Certificate Standard"[1] ("the Standard"). The Standard underpins a non-compulsory certification scheme ("the Scheme") which "offer[s] age-verification providers an opportunity to demonstrate to consumers that their solutions meet the BBFC's high standards in relation to age verification, particularly as regards data protection and information security". Age verification providers which meet the requirements of the certification scheme will be able to display a green 'AV' symbol on their website or app.

The BBFC clearly considers robust protection of age verification data to be of critical importance. However, in both substance and operation the Standard and Scheme entirely fail to deliver. Both are completely voluntary, the requirements placed on providers are vague and imprecise, the BBFC has no enforcement power, and full certification "does not represent a statement of compliance with either GDPR or the Data Protection Act 2018". Age verification providers are effectively allowed to write their own data protection framework and then prove only that they have implemented it. This provides little value either to consumers wishing to know which providers to trust, or to the Information Commissioner's Office (ICO), which might otherwise rely on a provider's certification status when determining whether to take regulatory action.

Developing a privacy standard and certification scheme for age verification providers is a positive endeavour. However, to be effective, any scheme needs to be fully public, be easy for consumers to understand, and contain concrete requirements for AV providers to meet - with strict penalties for non-compliance. It must be binding on all AV providers operating in the UK market and published with enough time for providers to achieve compliance before the date of enforcement - currently 15 July 2019. In our view, to meet these stipulations the government must legislate to require the BBFC to construct and develop a new, strong, mandatory certification scheme.

[1] BBFC, *Age Verification Certification Standard*, April 2019 <https://www.ageverificationregulator.com/assets/bbfc-age-verification-certificate-standard-april-2019.pdf>

Operational Issues with the BBFC Certification Scheme

Privacy standards for sensitive content beg a statutory basis

The most critical issue with the Scheme is that enrolment is voluntary. Age verification providers are not legally bound by the Standard's provisions and may choose whether to put themselves forward for assessment. The BBFC has no recourse against non-certified providers that can and will continue to operate, including both those that refuse to engage with the Standard and those that fail to achieve certification. In our view, providers that fail to meet reasonable minimum standards for customer data safety should be barred from operating at all; instead, under the Scheme they will simply be barred from carrying the regulator's green symbol. However, the Scheme does nothing to prevent scam operators from attempting to fool consumers into trusting them by posting near-copies of the symbol.

The only concrete way to ensure that age verification providers obtain trustworthy certification before processing sensitive identity data is to place a statutory requirement on the BBFC to implement a mandatory certification scheme. That this isn't already the case is due to the government's failure to incorporate the necessary provisions into the DEA in 2017. Instead, the government opted to defer to pre-existing data protection legislation as the means by which to assess whether age verification providers are providing an acceptable standard of service. As this analysis will show, this is a disastrous decision.

The BBFC could take inspiration from other data protection standards, particularly the Payment Card Industry Data Security Standard ("PCI DSS"), the information security standard mandated by the major cards to reduce fraud. In both cases the information concerned is valuable and sensitive data and in both cases motivated threat actors wish to benefit from its theft or exposure; intimate data regarding sexual and pornography preferences is known to be valuable for phishing attacks and blackmail. However, PCI DSS is a mandatory contractual requirement between merchants and acquiring banks, and it specifies technical controls that merchants must implement before processing card payments. Unless the BBFC standard is similarly made mandatory, the BBFC's certification scheme will never be able to robustly ensure the safety of highly sensitive age verification data.

As will be discussed later, implementers still struggle with PCI DSS compliance several decades after the standard was introduced. The BBFC are likely to see a similar (or worse) uphill challenge with age verification, as without a statutory basis no provider will feel any pressure to be compliant. In our view, if there is a data breach by a non-compliant provider, responsibility will lie with the government for failing to enforce appropriate statutory levels of protection.

Recommendations:

> **The BBFC Standard should be substantively revised to set out comprehensive and concrete standards for handling highly sensitive age verification data.**

The Government should legislate to grant the BBFC statutory power to mandate compliance by age verification providers with these standards.
The Government should make remedial action or financial penalties for non-compliant providers available to the BBFC.

Insufficient implementation time puts user data at risk

Enforcement of DEA age verification provisions is set to begin on 15 July 2019. The Standard was published on 26 April 2019. That gives providers a woefully insufficient 80 days to ensure their systems are compliant before enforcement begins. The time required for the BBFC to assess providers for certification purposes seems not to have been considered; if many providers apply the time needed could be extensive. This time pressure puts people's personal data at significant - and unnecessary - risk.

Again using PCI-DSS as a comparator, statistics published by Verizon in 2018 show that only 52.5% of organisations achieved full compliance more than *two decades* from the original implementation date.[2] Similarly, after four years of effort, the UK government admitted in 2018 that it had been unable to complete developing GOV.UK's "Verify" programme into its envisioned working service providing ID verification for government websites.[3] These examples demonstrate that implementing secure platforms takes time even for experts to get right.

It is critical for user privacy and security that providers have adequate time to ensure that their systems are compliant *before* age verification enforcement begins. MindGeek, one of the major age verification providers, has said it expects 20-25 million UK adults to sign up for its service in the first month.[4] Security and privacy standards *must* be in place and the BBFC must have assessed most or all providers at the time of launch for certification to be of any benefit.

Recommendation:

Implementation and enforcement of age verification must be delayed until (a) a statutory standard of data privacy and security is in place, and (b) that standard has been implemented by providers and the BBFC has assessed their implementations.

The AV certification symbol ("kitemark") lacks consumer value

The BBFC Standard states that "age-verification providers that meet the requirements of the Standard in full, as assessed by a suitably qualified independent third party, will receive certification". Certified providers will be permitted to display the specially-created "green AV symbol" to indicate their status to consumers. However, with a scheme that is voluntary and

---

[2] Verizon, *2018 Payment Security Report*, 25 September 2018 <https://enterprise.verizon.com/resources/reports/payment-security/2018/>

[3] National Audit Office, *Investigation into Verify*, 5 March 2019 <https://www.nao.org.uk/report/investigation-into-verify/>

[4] Sky News, *UK pornographers fear age verification laws may harm business*, 7 November 2017 <https://news.sky.com/story/uk-pornographers-fear-age-verification-laws-may-harm-business-11116453>

vague, this symbol approach is of little use to consumers seeking to make responsible choices about which companies to trust with their data.

The BBFC expects pornography consumers to be vigilant in their choice of age verification provider and make "responsible" choices by opting only for certified providers. However, rather than empowering consumers this approach places an unreasonable burden on them. It is unfair to expect consumers to know and understand what the BBFC green symbol is meant to convey about a provider's level of security and to exercise the continual vigilance that will be required to check for the correct green "AV" symbol. Tech-savvy consumers may routinely check their provider's compliance with the BBFC scheme before handing over their data, but they will be a small minority.

Consumers should not be expected to spend their time researching the trustworthiness of age verification providers before signing up. Instead, they should be empowered by statutory requirements to *expect* that any provider they choose will meet the high levels of data protection required for handling sensitive personal data.[5]

Even diligent consumers who take steps to fully inform themselves will struggle to do so, since the scheme's vagueness means providers are effectively writing their own rules (see below). Functionally, this renders the green symbol meaningless, as the actual level of data protection it signifies may vary significantly among certified providers. The symbol provides no information to distinguish between the minimum and maximum levels of security providers may apply.

We reiterate: any certification scheme must be mandatory and include powers of enforcement against non-compliant providers.

Consumers must be notified where providers no longer qualify for certification

By definition, pornography sites which are required to verify age are commercial operations. All commercial websites share the common goal of reducing friction as much as possible by removing any sticking points which could hinder revenue generation. Age verification introduces a point of friction, so we would expect providers to design their systems to be as unobtrusive as possible. Accordingly, users will likely be pushed to save their registration so future signins are automatic.[6]

Therefore, a user may only interact directly with an age verification provider when they first sign up, and see the BBFC green symbol only that one time. There may accordingly be no visual cue to tell a user if the provider they have registered with has lost its certification, for example

[5] We acknowledge that the reasonableness of a consumer 'expectation' of security is challenged by the inevitable existence of phishing sites which will claim to be age verification providers, however we would note that the certification scheme does not address this issue. Phishing sites will simply mimic compliant providers.

[6] AgeID's website confirms this approach, advertising: "Fast one-time verification with minimal data entry. No need to repeat verification prompts for your customers." <https://www.ageid.com/>

by failing an audit. Since the Scheme is voluntary and lacks enforcement, nothing requires the providers of either pornographic content or age verification to warn customers that a formerly certified service is now non-certified or what that means in terms of privacy or security protection. This is a poor outcome.

The Standard also makes no provision for recourse against a certified provider who experiences a data breach as a result of failing to meet the expected standard. The BBFC indicates that "penetration tests" are a requirement for certification and that providers must comply with a number of other requirements and review them "regularly" or "annually". However, the BBFC does not indicate how often it will assess compliance. Because of these gaps, providers could lapse in compliance while continuing to display the green 'certified' symbol. This is also a poor outcome for consumer protection.

Recommendations:

Providers who are deemed to no longer meet the Standard should be required to provide the BBFC with evidence that they have destroyed all user data collected during the period they were supposedly compliant.[7]

Where a provider's certification is revoked, the BBFC should ensure consumers are informed.

The BBFC should be given statutory powers to require annual compliance reports from providers and issue fines to providers who have signed up to the certification scheme but who later violate its requirements.

The Standard relies on unpublished documentation

The Standard makes repeated references to a separate "Programme Guide" and which it says contains expanded detail about the certification process, stating: "The certification process is outlined within the associated Programme Guide and this standard should be read in conjunction with the associated Programme Guide."

To date, the BBFC has not made the Programme Guide publicly available. Its lack of availability compounds the time issues already discussed.

It is possible that the BBFC is already working privately with well-established age verification providers and has made the Programme Guide directly available to them. If so, the non-public nature of this document is a problem for transparency. Lacking full information about the Scheme, consumers cannot be expected to understand what certification means, what standards age verification providers are expected to meet, or what the green symbol is supposed to mean - and consumer protection organisations cannot advise them. Consumers are therefore put in a position where they cannot make well-informed decisions. In addition, smaller age verification providers are disadvantaged if the Programme Guide document is selectively disclosed only to more established companies, an anti-competitive action that fails to support the innovation the government claims to desire.

[7] Some appropriate standards for evidence could constitute: (a) a signed letter or email from the database administrator; (b) a signed letter from a company officer; (c) an audit report from a professionally responsible third party; or (d) fragments of destroyed hard disks.

Recommendation:

> **The BBFC should immediately publish the Programme Guide and all other relevant documentation surrounding the Scheme in conformity with its commitment to transparency and accountability.**

Substantive Issues with the BBFC Certification Scheme

In terms of its content, the Standard remains fundamentally flawed and consumers can't rely on it as a reasonable guide to privacy protection. This section outlines and discusses seven specific issues we have identified.

The scheme merely holds providers to their own variable standards

The Standard sets out the following objective in Section 4: *"By meeting the requirements of the Standard age-verification providers shall be able to demonstrate that a framework of data protection and information security controls have* [sic] *been implemented, their solution has been developed by following the principles of data protection by design and by default and the privacy of users shall be maintained."*

In this, the BBFC acknowledges that the Standard does not provide an objective list of rules or principles against which an age verification provider will be measured for certification. Instead, providers are expected to independently develop and implement their own policy frameworks that maintain user privacy and security. The regulator will then simply assess whether a provider is adhering to the standards it has set for itself.

This plan immediately presents problems from a consumer perspective. If age verification providers are held only to self-defined and inconsistent standards rather than to well-defined, universally-applicable requirements, how may a consumer have confidence in the green certification symbol? This approach leaves room for vast differences in the security and privacy standards of providers, who will have no incentive to rise above baseline minimums. BBFC should be encouraging them instead to strive for maximum user protection .

We believe that this approach largely reflects the rushed and problematic nature of the age verification rollout. The BBFC has not been provided with either the time or expertise necessary to draft a robust set of objective standards that can apply to all market operators, and, as a result, has fallen back to simply monitoring and rubber-stamping whatever standard providers choose to implement.

The dangers of this approach have been vividly summarised by security researcher and Open Rights Group board member Alec Muffett: "Consider for yourself whether, if you lived in Tokyo [in an earthquake zone], you would want to live in a building designed and blueprinted by amateurs, but where they crashed cars into it occasionally to see if it is 'safe enough'."[8]

[8] Twitter, Alec Muffett tweet thread, 26 April 2019 <https://twitter.com/AlecMuffett/status/1121733258327285760>

Recommendations (reiterated from above):

The BBFC Standard should be substantively revised to set out comprehensive and concrete standards for handling highly sensitive age verification data.

The Government should legislate to grant the BBFC statutory power to mandate that age verification providers comply with these standards.

Implementation and enforcement of age verification must be delayed until (a) a statutory standard of data privacy and security is in place, and (b) that standard has been implemented by providers.

The "principles" are unhelpful and vague

The Standard provides very little guidance on what providers' policy frameworks providers should contain. It sets out no principles; it offers no examples of frameworks which would be considered compliant; and it identifies no specific issues which would automatically disqualify a framework. Instead, the BBFC defers entirely to individual providers' choices in developing these frameworks.

In Section 5, the Standard outlines four core principles which underpin the certification scheme: flexibility (so AV providers can adapt to changing technology and legislation), data protection (compliance with GDPR and the UK's 2018 Data Protection Act), security, and selection (AV providers are not tied to any particular technology or data sources). These principles are presumably intended to allow for easy adaptation to changing circumstances. However, as a result they provide very little operational detail.

The principles state that the Standard is “flexible enough to respond to developments in age-verification technology, processes and legislation'' and “will ensure the appropriate technical and organisational measures shall be in place to ensure the confidentiality, integrity and availability of age-verification solutions." This wording appears to suggest that the BBFC believes that age verification technology is likely to develop so fast that it's impractical to include concrete rules or technical suggestions in the Standard. We find instead that the vague wording makes the Standard appear rushed and watered-down. Vague standards do not promote best practice and do not empower consumers to make informed decisions about whom to trust with their highly sensitive data.

Recommendation:

Even if the BBFC certification scheme remains voluntary, the Standard should at the least contain a definitive set of precisely delineated objectives which must be achieved by age verification providers in order to say that identity data is being processed securely.

Risk assessment should be a BBFC responsibility

Section 8.1.5 of the Standard requires providers to implement a risk management framework *“for the identification, assessment, ownership and management of information security and data*

protection risks." We find it concerning that the BBFC again chooses to leave much of the work to individual age verification providers. The likelihood of attacks and the motivations of threat actors are well-known, and the adverse impact to individuals of attacks and data breaches is quantifiable. As a result, most of the risk assessment process could, and should, be conducted by the regulator itself so that all providers are working on an even footing. As the BBFC do not have prior experience in this area, they should license security consultancy companies to complete standardised risk assessments. Providers should limit bespoke risk assessments to their specific technological implementation.

The lack of definition or specificity in the risk assessment stipulation, as with the privacy framework stipulation, leaves wide scope for variation in the strictness of the data protection standards being implemented by certified providers. Again, the result is to limit the Scheme's effectiveness; as written it will not lead to high privacy standards and will not provide value to consumers .

Recommendation:

> **The BBFC should prepare a standardised data protection risk assessment framework against which all age verification providers will be tested. Risk assessments undertaken by providers individually should be limited to their technological implementation.**

Similarly, Section 8.6, *Secure Development*, contains some useful recommendations for providers to follow in developing age verification software. However, this, too, essentially reads as a vague list of "common sense", generic suggestions that apply broadly to software development. The section does not specify situations or failures which would lead BBFC to refuse certification. The BBFC could draw further inspiration from the PCI DSS standard here. In PCI DSS, ambiguity around data classification is removed. Data types are outlined and providers are instructed on how they must be treated (e.g. card numbers, sensitive authentication data, etc.). The BBFC should establish a parallel recommendation explicitly classifying the categories of data which are expected to be collected by providers, and outline how each category of data should be handled.

"Ethical hacking" is not sufficient to robustly test system security

The Standard requires age verification providers to undertake a "penetration test" in order to become certified. As it notes, penetration testing is a method of probing a computer system, web application, or network to find security vulnerabilities that an attacker could exploit. In our view, this approach is similar to other testing frameworks based on simulated attack scenarios, such as the "CBEST" cybersecurity framework developed by the Bank of England[9] and "GBEST", which is currently in vogue with regulators and the National Cyber Security Centre, and which is being rolled out across UK government departments.[10]

[9] Bank of England, *CBEST Intelligence-Led Testing: Implementation Guide Version 2.0*, 2016 <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf?la=en&hash=1BFF85C8F9E6C0E8BE478BB22B422EDDA5E00DC0>

[10] See Crest website <https://crest-approved.org/gbest/index.html>

The key distinction between the CBEST and GBEST frameworks and the BBFC's approach, however, is that those frameworks outline (in detail) specific processes which must be followed to produce a bespoke set of tests tailored to the provider. The frameworks apply consistently within their sectors, involve contracting a specialised (and expensive) expert to conduct a thorough assessment of the relevant system, and allow the relevant regulator to punish those whose results are unsatisfactory.

By contrast, the BBFC Standard outlines some categories of penetration test which must be performed and gives some specifics about which segments of a provider's network and product must be tested, but then undermines this with vague remarks about tests having to be "based on industry recognised methodologies" (here again, unhelpfully, it refers readers to the as-yet-unpublished Programme Guide for a list of these) and leaves the choice of tests to individual providers. Generally, the section is vague on the specific security weaknesses a provider will be expected to eliminate and leaves considerable room for providers to self-certify that their systems are secure. To draw further parallels, PCI DSS requires testing to be performed by "suitably qualified" persons, which could be interpreted as similarly vague. However PCI DSS is designed for implementation by a global audience while age verification requirements need only apply for the UK. For this reason, we still find it appropriate for the BBFC to outline specific frameworks which would be appropriate for use in assessing providers.

Even if robustly conducted, a single penetration test, while useful, should not be relied upon to vouch for the security of data on an age verification provider's network. A penetration test only reveals a subset of the vulnerabilities that may be present in a provider's implementation at a particular point in time. We suggest that a more appropriate approach would be to conduct regular internal and external vulnerability scanning and a penetration test at least every six months, followed by a supervised remediation programme to correct any vulnerabilities that have been discovered. Penetration tests should also be commissioned after any significant application or infrastructure change. The tests should be chosen based on a comprehensive and specific standard, as with CBEST or GBEST. The results of all penetration tests should be provided to the BBFC, which should publish the framework it uses to evaluate test results and annual trends.

The BBFC's reliance on penetration testing as the primary method of ensuring the safety of user data is questionable as it does not follow the spirit of GDPR's 'privacy by design' requirements. Instead of periodically probing systems to ensure that age verification providers are reliably securing data, it would be prudent for the BBFC to ensure that privacy requirements were front-and-centre in any certification standard. The primary focus of the document centre around ensuring that age verification providers implement systems which are private by design through the use of data minimisation, tokenisation, or other techniques. This helps to ensure that any fallout from a data breach is naturally minimised, as the user data exposed by such an event would be reduced. This is in contrast to the current approach, which focuses the primary effort on the impossible task of ensuring that such a data breach could never happen.

We accept that the suggested requirements above could be considered intensive. However, strict standards are required in order to ensure that the certification programme is functionally useful to consumers, who need to be able to have confidence in the BBFC's green symbol.

Recommendations:

Age verification providers should be required to undertake regular vulnerability scanning both internally and externally, and a penetration test at least every six months, followed by a supervised remediation programme to ensure any discovered vulnerabilities are corrected.

Providers should be required to conduct penetration tests after any significant application or infrastructure change.

Providers should be required to use a testing standard which is comprehensive and specific. CBEST or GBEST could be used as guides for the BBFC to develop an industry-specific framework.

The results of all penetration tests should be provided to the BBFC, which should publish the framework it uses for evaluating test results and annual trends.

Domains and control requirements are too basic

As a whole, Section 8, *Domains and Control Requirements*, reads like a basic, "common sense" list of requirements for maintaining general IT systems. Most of the principles outlined in this section do not apply directly to either data security or age verification, and instead focus on more basic IT challenges such as maintaining backups, implementing change management, and documenting the configuration of IT infrastructure.

Recommendation:

Rather than attempting to outline its own set of domain and control requirements from scratch, the BBFC should build on already-established strong security frameworks, such as the 20 CIS Cyber Controls and Resources,[11] or the NIST Cyber Security Framework.[12]

Greater specificity on data collection and retention is needed

Section 8.5, *Data Protection*, contains some helpful provisions, particularly with regard to data minimisation and limiting the data shared between the AV provider and the content provider's website to a pass/fail response to the age check. However, much of this section is redundant, as it merely reiterates the legally binding rules and principles enshrined in data protection law.

In terms of data collection, the Standard provides that "only the minimum amount of personal data required to verify a user's age shall be collected", and that "information about the requesting website that the user has visited shall not be collected against the user's activity".

[11] Centre for Internet Security, available here: <https://www.cisecurity.org/controls/cis-controls-list/>
[12] National Institute of Standards and Technology (US Dept of Commerce), available here: <https://www.nist.gov/cyberframework>

These are welcome restrictions, but it is disappointing that the Standard does not define reasonable "minimum" data points. Whose minimum is being applied here? Again, these restrictions are laid down only within this voluntary certification Standard, and are not enforceable by penalty.

Recommendation:

> **A provision requiring data minimisation as a rule should be an enforceable statutory requirement for any provider wishing to register as an age verification provider for the purposes of the DEA.**

Additionally, the section suggests that providers should use "industry standard pseudonymisation techniques" to control information "that can be used to re-identify an individual". However, once again the document chooses not to expand upon these techniques nor reference examples. Pseudonymisation can provide some benefit to data privacy, but a plethora of published research establishes the ease of re-identifying supposedly anonymised data.[13]

Recommendation:

> **The Standard should set out a clear, strict and enforceable set of policies to describe exactly how "data pseudonymisation" should be accomplished.**

The Standard bars AV providers from keeping data about verified users and the content they have visited, "unless required for fraud prevention and detection". However, it offers no examples of situations in which retaining age verification logs would, or would not, be appropriate. This lack of definition effectively creates a catch-all exception to the rule. Similarly, although the section stipulates that "Logs for age-verification checks shall only be retained for the length of time required to prevent or detect fraudulent activity from taking place", it does not provide any indication of what length of time might be considered reasonable, and it places no hard limits on how long logs may be kept.

Recommendation:

> **The Standard should outline specific and very limited circumstances within which the BBFC considers log retention appropriate for fraud prevention purposes. A hard limit on the amount of time that logs may be kept for should be specified.**

Bad Crypto is Worse than No Crypto

Regarding encryption, the Standard merely says: "A policy shall be implemented to ensure cryptographic controls are used to protect information used to verify an individual's age at rest and in transit." Once again, it does not stipulate which cryptographic protocols or implementations would, or would not, be considered acceptable. Providers' encryption policies should be verified and audited for the purposes of obtaining certification. The Standard's

[13] 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', Paul Ohm (2010), UCLA Law Review, https://www.uclalawreview.org/pdf/57-6-3.pdf

current wording suggests that the mere presence of a policy to encrypt data, no matter how poorly it may be implemented, will suffice for a provider to become certified.

Encryption is not a "magic bullet" that renders all data completely secure. There is always room for error in implementing cryptographic protocols, so it would be prudent for the BBFC Standard to point providers towards using tokenisation or truncation to further protect sensitive data and individuals' identities in case the provider's cryptographic protection fails.

Recommendation:

> **At a bare minimum, the Standard should identify cryptographic protocols which are no longer considered safe for use and specifically highlight that they would lead to a provider losing its certification.**
> **It would also be appropriate for the BBFC to reference an established and accepted set of cryptographic standards for providers to follow.**[14]

Some positive points

Unlike the rest of the Standard, Sections 8.2 (*Secure Workforce*), 8.3 (*Access Control*), and 8.8 (*Physical Security*) of the Standard do prescribe rules providers should follow. We feel that this is likely because these provisions largely relate to physical security, and therefore the consequences are easier for non-experts to predict, and they are easier to implement for providers. These sections contain a number of welcome rules, such as ensuring that employees sign confidentiality agreements and that providers implement access controls and terminate access to systems when employees no longer need it.

We welcome the inclusion of rules blocking the use of default passwords and credentials for systems and infrastructure. The BBFC's general password guidance is quite simplistic, however, and it would be appropriate for them to defer to industry best practice and incorporate the NCSC's 2018 guidance on passwords.[15]

Conclusion

Entrusting sensitive identity data to age verification providers places people in a vulnerable position. Cybercrime has become more common in the UK than traditional robbery or theft, and attacks are increasingly frequent and sophisticated. Age verification data is a known target, which makes it even more important for providers to handle it securely. The BBFC Standard fails to provide any real protection to consumers as it leaves age verification providers to determine for themselves what privacy and security framework they will adopt, and gives providers wide discretion to develop standards that *they* consider robust. This is simply unacceptable. Urgent measures are needed to ensure that the government does not deliver a privacy scheme that is not fit for purpose.

---

[14] One such standard that we suggest is NIST Special Publication 800-57 Pt. 1, Rev. 4 <http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>

[15] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach