White Paper

The foundations for an open, competitive and reliable global age-assurance market

May 2020

Version 1

Draft for discussion

1. Introduction

It is the UK Government's stated aim to ensure that *what is illegal offline, is also illegal online*. Increasingly, other jurisdictions are seeking to adopt the same principle, extending real world regulations across the virtual world – and, in any case, the internet has no borders so solutions need to address a global market.

Many of our laws feature age restrictions designed to protect children and young people from a wide range of harms, so a fundamental pre-requisite to achieve this parity across our legal spheres, is to be able to know with appropriate confidence, the age, or age-range, of individuals irrespective of whether they are operating online or in the real world.

For this reason, many parts of government are already considering age-assurance techniques for use on the internet.

Age Verification Providers Association (AVPA) members are global leaders in the field of age-assurance, and are already engaged with many government departments, regulators and other non-departmental public bodies, advising, developing and implementing age-checking solutions for a large number of goods and services around the world.

The purpose of this White Paper is to set out a vision for the application age-assurance, not only in the UK but globally, which will meet the wide-range of needs of governments within a common framework.

By basing such a framework on internationally applicable and recognised standards, it will be possible to build an open and competitive market, which:

- stimulates a vibrant new technology sector to generate innovative solutions
- meets the requirements of many diverse use-cases efficiently within a common framework
- avoids the creation of bespoke regulatory solutions for each and every purpose
- does not further entrench the oligopolies of existing technology platforms
- delivers reliable age checks with an appropriate level of robustness applicable to the risks that the checks seek to mitigate
- delivers age assurance that does not hinder daily business but recognises the responsibilities of suppliers to implement effective age verification
- allows for interoperability between AV providers, providing convenience for consumers through ubiquitous acceptance
- reduce the risk of fraudulent use of AV to misappropriate data by creating independent certified Age Verification Providers
- reduce the risk of data privacy breaches and abuse of personal data through anonymisation and data minimisation, highlighting the distinction between age verification and identity verification
- achieve comprehensive coverage of age verification, based on regulations that apply to the point of consumption not only the point of supply

2. The current state of age-assurance in the UK

There are a wide number of products which are subject to age restrictions in a physical retail sales environment that are also restricted when sold online.

Age checks are already required for many of these products and increasingly online services, supervised by a growing number of different regulatory authorities, at different levels of government – national, devolved and local.

A full list of age-restricted products and services is in Appendix 1.

Many government departments are involved in age verification for multiple purposes, and the AVPA already works with the BEIS Office for Product Safety and Standards (OPSS) through its Expert Group on Age Verification, to promote a joined-up approach.

However, at present, the requirements in the UK vary considerably, as each authority – and departments and teams within those bodies - seek to define and implement an approach to online age-assurance for each product or service separately.

- Some require 'light touch' age verification; others insist on a far higher level of robust process to ensure lower levels of error
- Some need only one check to be applied; other may require two or more to offer a cross-check and additional levels of confidence.
- Some require audit trails for age checks; others discourage audit trails and favour anonymisation/pseudonymisation.
- Some reference the only available code of conduct for AV (PAS 1296); others have created, or are in the process of creating, their own bespoke requirements or standards.

As age-assurance is adopted around the world, there is the potential for this complexity to multiply exponentially. Whilst complexity is a consequence of the multifarious applications of age verification, a complex situation due to numerous competing regulatory frameworks is not.

Developing so many regulations across so many regulators is costly to the regulators themselves and to suppliers and ultimately to consumers. It also dilutes the effectiveness of investment in quality assurance, presents consumers with a need to verify themselves on multiple occasions in multiple ways, and makes a new user-experience more confusing than it needs to be.

This is not likely to encourage user acceptance of age verification, and provides fertile ground to breed resentment towards such safeguards, often fed by campaigners opposed to any form of virtual regulation or commercial interests resistant to restricting their online sales by age.

3. The challenge of a worldwide web

The internet has no borders, so age restrictions need to be applied to all the goods and services available to consumers within a jurisdiction, not only to those supplied from that country.

One of the strongest features of the Digital Economy Act 2017 was its approach to enforcement. It correctly identified the critical points in the value chain that could be controlled domestically. These included:

- requesting that ancillary service providers withdraw services such as advertising;
- asking payment-services providers to withdraw services; and
- requiring internet service providers and mobile network operators to lock access to the non-compliant service.

In addition, fines should also be considered, as while they are hard to impose on overseas entities, the banking sector has demonstrated that it is feasible.

A common approach to enforcement will allow the organisations involved in implementing responses to breaches of regulations to develop streamlined processes to apply those sanctions, at the request of any competent authority. This will minimise costs and improve effectiveness.

There are also incentives to implement age verification. Some goods and services are currently, or may soon become, subject to blanket bans online where they may be accessed by minors. If suppliers, search engines and platforms can demonstrate they are able to restrict content to adults, then they will be able to access a wider range of revenue streams, achieving whitelist status for these supplies.

4. Developing a general standard for Age Verification

The adoption of consistent age verification standards which apply the appropriate level of assurance and audit, proportionate to the risk of each product, is a prerequisite of an efficient, competitive sector.

An important first step was the development of a Code of Practice for Online Age Verification service providers developed by the British Standards Institute and the Digital Policy Alliance. **PAS 1296** – a Publicly Available Specification – is intended to assist providers of age restricted products and services online (such as gambling, adult content or goods) with a means to adopt and demonstrate best practice and compliance.

The PAS covers:

- Methods of age verification
- Vectors of trust / Levels of Confidence
- Data protection
- Privacy
- Data minimisation

The AV industry is discussing how to develop the Code of Practice into a formal Standard, and in parallel to support the creation of a British or International Standard. Upgrading this to a formal Specification will allow for providers to be certified against it and the development into a standard is expected to be completed during 2020.

5. Beyond Standards – the AVPA Code of Conduct

In addition, the industry itself has developed a code of conduct:

The Age Verification Providers Association's Code of Conduct is a set of guiding principles our Members agree to follow when conducting business. Our aim is that these principles will drive high standards from the industry, assist in establishing best practice and create a collaborative approach to solving the problems of age verification. The key goals of the Code are:

- To promote effective age verification
- To encourage age verification adoption in a manner compliant with regulations
- To encourage sound business practice
- To promote the highest levels of data protection and data control

AVPA Code of Conduct

AVPA Member organisations agree to the following five principles:

1. Fairness and transparency

How personal data is collected and how it is used should be clearly explained to the consumer. Data should be used for age verification and not additional unspecified purposes.

2. Use of appropriate verification methods

Data sources and technical methods against which consumers are checked should be reasonable and suitable to meet the requirements of regulators and client organisations, while recognising the sensitivities around release and use of personal data.

3. Privacy and Security

Data privacy should be paramount. Members should follow 'privacy and security by design' principles and make all reasonable endeavours to maintain the security of processed or stored personal data.

4. Accuracy

Members should take all reasonable steps to ensure the accuracy of data and rectify inaccurate data to maintain the integrity of their age verification systems.

5. Responsibility

Members acknowledge that they have a collective responsibility to maintain a positive public image of the age verification sector.

6. Competitive markets

As requirements for age-assurance extend across online services, the process becomes a critical link in the value-chain. It is likely to attract the interests of major social media platforms and technology companies, seeking to gain a toehold across a wide range of online transactions.

There is a choice open to policy-makers to pre-empt this form of oligopolistic market structure by designing an open, competitive market for age-assurance based on standards, with suppliers subject to both regulation and self-regulation within a wider legal framework, supported by existing accreditation and audit infrastructure.

It is important to ensure that emerging solutions comply with competition laws.

7. Interoperability

Exchanging age attributes

PAS 1296:2018 contemplates the creation of a central attribute exchange. Under such a regime, there would be a central clearing house fed with age attribute data by all the AV Providers which could be accessed by all AV Providers and directly by merchants.

This is theoretically attractive, but there are a number of drawbacks

1. It does not address the question of how the current, competitive market evolves to this model, at least not without direct government intervention to create such an exchange from scratch.
2. A central clearing house of this sort is also likely to raise concerns from the civil liberties lobby, and doing so at the same time as the protection of AV is being rolled out across products and services could undermine age-assurance more generally
3. A single central clearing house is by definition a monopoly. Analogous markets support multiple attribute exchanges e.g. payments through either VISA or MasterCard

A more pragmatic alternative, which itself is step towards this outcome once the market and technology has matured and stabilised, is the creation of inter-provider relationships.

This already happens bilaterally, but could be easily upgraded to support multilateral exchange, using an agreed exchange protocol. At this time there are a relatively small number of attribute providers. It is unlikely that multiple central attribute exchanges could subsist today, but a common exchange protocol is the first step towards an exchange market and the subsequent development of exchanges.

Allowing the market to develop this way, mirrors the successful development of the payments markets such as UnionPay, Visa and Mastercard. Initially, banks

created bilateral relationships, but at some point, it became unmanageable and it was a natural step to create a centralised system.

It is necessary to develop trust frameworks to underpin the system, with a clear understanding of liabilities.

An analogous target inter-operating model – payment card schemes

Card schemes are payment networks linked to payment cards, such as debit or credit cards, of which a bank or any other eligible financial institution can become a member. By becoming a member of the scheme, the member then gets the possibility to issue or acquire cards operating on the network of that card scheme.

In a four-party scheme, the issuer (having the relationship with the cardholder) and the acquirer (having the relationship with the merchant) are different entities and this type of scheme is open for other institutions to join and issue their own cards. This is the type of card scheme used by brands such as Visa, Mastercard, Verve Card, UnionPay and RuPay. There are no limitations as to who may join the scheme, as long as the requirements of the scheme are met.

A staged approach

The Age Verification market should be encouraged to follow a pathway towards a similar global operating model, borrowing from the successful development process of these card networks to build and sustain an open, competitive, self-regulated market.

Stage 1 - Today

Already, AV providers have put in place bilateral arrangements which allow those with contractual relationships to allow users of one verification solution to use interact within another verification platform.

These bilateral arrangements start to reduce the friction caused by having a number of providers of age verification with largely non-interoperable systems.

They are usually underpinned by a commercial agreement for cross-charging, with payments netted off between suppliers.

Additionally, returning verified customers to sites are often able to avoid re-verification. Site operators are able to reduce customer friction by poling a number of AVPs to ascertain whether individuals are returning customers prior to requesting an age verification.

This range of poling of providers for 'recognised customers' prior to an age verification is referred to as a "cascade".

Stage 2 – A standard AV Exchange Protocol for multilateral attribute exchange (2020)

Standard AV Tokens would be created based on PAS 1296:2018 (potentially being updated during 2019).

Tokens allow a "Relying Party" to ask a question of an "AV Token Service". For example;

"Is this client over 18"

The reply could include, for example:

Answer	Yes / No
Method	Name of PAS 1296 Approved AV Provider Method of verification 1 Date of verification 1 Method of verification 2 Date of verification 1 Etc.
Date of Question	DD/MM/YYYY
Period of Validity	X days

Both questions and replies can be encrypted, and/or added to public or private ledgers.

The AVPA is in the process of defining and agreeing an AV Exchange Protocol which would allow AV Tokens to be exchanged between approved, participating AV providers.

Stage 3 –Attribute Exchange (2022)

As the market matures, with ubiquitous adoption of an international AV standard, and a critical mass of AV providers, it will be able to support AV attribute exchange.

With an interoperable protocol, attribute exchange could occur bilaterally between providers or through more centralised exchanges that operator with multiple providers. Ideally they will be more than one to maintain competition but not so many that they impact interoperability by driving users and suppliers to work separately with many different AV networks.

At this stage, users will log onto websites with an AV credential from any approved, participating AV provider. This makes possible age checking processes that are seamless for the customer, readily acceptable by website operators and compliant to regulations.

8. Quality

To return to the MasterCard and VISA analogy, there are firm restrictions on which companies can join the payments networks, to avoid the misappropriation of consumers money.

A process of AV attribute exchange offers the opportunity to apply equivalent standards, only allowing AV Providers which adopt a standard such as PAS 1296, and agree to comply with a Code of Practice, and maintain a record of wider legal compliance such as with data protection requirements, to participate.

9. The Commercial Model

The commercial arrangements underpinning each stage of development of the AV market need to be developed and agreed by participating AV providers.

Each of the steps outlined above has an effective associated commercial model to ensure the ongoing viability of an independent, high quality AV sector.

Any system needs to guarantee the durability of the AV sector. The principal risk to this is a grey market of AV credentials, with clients providing second-hand lists of consumers.

This risk can be mitigated through;

1. Fraud analytics

   AV Providers and, in due course, the Central AV Attribute Exchange, will deploy fraud analytics, similar to the technology used to detect fraudulent card payments, to identify second-hand, grey-market, or shared AV credentials. To give a simple example, the use of the same credentials in two separate geographical locations simultaneously would flag those credentials as potentially compromised and prompt the consumer to re-verify their age when they next use them.

2. Time-limits to AV validity

   Whilst in theory, once a consumer has 'proven' they are over 18 they remain an adult for life, as with any form of age verification, it is possible that the verification was achieved fraudulently. That may be through forgery or theft or borrowing someone else's credentials. Therefore, there should not be an assumption that an age attribute is definitive for all time. AV providers will continuously improve their fraud detection systems, and AV techniques will evolve over time. So, regulators can impose time limits on the validity of AV checks, just as they do for identity checks. For low risk uses, a year may be reasonable; for higher risk purchases, such as knives, then a new check may be required for each transaction.

3. Randomised validation

   In addition to fraud detection, to prevent credentials being shared, consumers can be regularly challenged to re-verify their age, or some component of their original check.

10. A competitive market

This model above also maintains a competitive market at each stage of its development.

Once it has reached the third stage, a mature market would retain similar levels of competition to existing card payment networks. This strikes a balance between an impractical number of exchanges, and a single monopoly.

As the evidence shows for the process of logging-in, or payments processing, major technology companies and social media platforms are always looking for ways to extend their share of the online value chain. Age-verification is another opportunity for them to do so but should be resisted, because it would

1. Further entrench major global oligopolies
2. Discourage the adoption of open standards
3. Mitigate the potential for external audit of age-verification processes
4. Reduce the incentive for investment in technological innovation to improve effectiveness and reduce the cost of AV

11. Regulatory approach

Adoption of this standard based approach facilitates effective regulation.

Publishers can be required by regulators to protect minors against harm. This may be done on a specific basis, identifying particular harms, or through a more general duty of care.

Regulators can then acknowledge that, in adopting particular standards, proportionately to the risk involved for each product or service, suppliers have managed those risks effectively.

Suppliers are not required to adhere to these standards, but are required to achieve an equivalent or better level of compliance.

Age verification	PAS1296:2018
Information Security	ISO 27001 (Information Security Management)
Data Security	CREST or other penetration testing
Privacy	

Effective IS protocol

SOC2

Test purchasing

This is a form of co-regulation which combines the efforts of government regulators with industry and its representative bodies.

The existing UK regulatory framework is built upon:

- The Regulator's Code
    - Economic Regulatory Departments meet regularly, and adhere to a code which ensures they adopt best practice for regulation.
- Standards
    - BSI - the British Standards Institution is the national standards body of the United Kingdom. BSI produces technical standards on a wide range of products and services and also supplies certification and standards-related services to businesses.
- Government Accreditation and Certification
    - UKAS - The United Kingdom Accreditation Service is the sole national accreditation body recognised by the British government to assess the competence of organisations that provide certification, testing, inspection and calibration services

Note that standards should be voluntary not compulsory – the regulator leaves room for alternative approaches and should be open to them.

12. Audit and Certification

The use of standards facilitates the use of existing audit and certification infrastructure in any given jurisdiction.

FOR EXAMPLE In the UK, the UKAS approves organisations which undertake audits for particular standards.

Those auditors can then check compliance of suppliers against these standards.

This process reduces the pressure on regulators to conduct direct audits of their own. It also encourages a competitive market for audits, keeping their cost down.

Users and regulators alike are given confidence that the system for age-assurance is sufficiently effective.

The use of kite-marks, or more enhanced technical certification (analogous to SSL, for example), can demonstrate which sites have be audited.

13. Conclusion

This White Paper has set out a commercially-sustainable development pathway for an open, competitive and global market that delivers proportionate and effective, and, if required, anonymised age-verification online. This will allow governments to protect children in the same way whether they are in the real world or the virtual world. It avoids any need for a government-issued digital Identity Card with all the implications and political resistance that would entail, and it increases competition on the internet, rather than further empowering existing oligopolistic platforms. It offers substantial cost-savings to regulators, suppliers and consumers, and the convenience of frictionless interoperability as the market structure matures.

The AVPA welcomes feedback on this proposition, and its members are available to cooperate on policy, regulation and standards creation to support all stakeholders in developing age-assurance – an absolutely fundamental pre-requisite of online child protection.

14. Glossary

Term	Meaning
Age Categorisation	Determining age-range e.g. 18-25, 16+ <21 13+
Age Determination	Determining exact age based on Date of Birth
Age Estimation	Estimating age without a Date of Birth – for example, using facial, biometric or social media data.
Age-Assurance	The broadest term for the process of understanding the age of users online
Age-Verification	The process for confirming to a given level of confidence based on evidence, the age or age-range of a user online
AV Attribute	A data point indicating an age or age range e.g. Date of Birth, Over 21, 13-18
AV Attribute exchange	
AV token	A coded message containing AV attributes
Bilateral AV Attribute exchange	A technical process to allow two parties to share AV tokens
Central AV attribute exchange	A technical process to allow multiple organisations to share AV tokens with multiple other organisations
Identification	The process for confirming to a given level of confidence based on evidence, the identity of a user online
Interoperability	The ability of AV providers to share AV tokens allowing each to rely on the another's AV process
Level of assurance	The confidence level required for age verification. A higher level of assurance may require the use of specific vectors of trust, or a number of vectors of trust
Multilateral AV Attribute exchange	A technical process to allow an organisation to share AV tokens with multiple other organisations
Pseudonymisation	Allocating a unique reference to an individual which can only be connected to their identity by the organisation which allocates that reference, and can be dissociated permanently from identity if desired.
Tolerance	Standards care be set within two tolerance levels T1 – a limited percentage within this range may be errors T2 – no errors should occur outside this range
Vectors of trust	The methods used for age verification. An age check may rely on one or more vectors of trust
AV Exchange Protocol	A standard for data exchange of AV attributes
Relying Party	The supplier or another AV provider which relies on the answer of an AV Token Service to conduct age verification
AV Token Service	A supplier of AV tokens containing AV attributes
AV cascade	A series of age checks designed to minimise user friction by trying those which require the least user

	involvement first, and minimising user involvement until age verification is achieved

15. About the AVPA – the global trade association for online Age Verification providers

The Age Verification Providers Association represents the main technology suppliers who have invested in the development of age verification solutions to implement age restrictions online. The UK leads the world in this technology, and many other jurisdictions are considering adopting a similar approach to making the internet a safer place for children.

Our current membership includes: AgeChecked, AgeGo, AgeID, Avyourself, Equifax, GBG, Verime and Yoti.

As an Association, we work to:

- Inform and educate the public, industry, and media, on age verification solutions and technology.
- Promote a positive image of effective age verification and the age verification industry.
- Represent the industry to regulators and law makers for the advancement of best practice, socially-responsible age verification policy.

The AVPA was formed in 2018 from organisations involved in the UK's Digital Policy Alliance age verification working group, and created and in response to a need for a uniform voice for of the industry.

The AVPA is governed by a representative Board drawn from its member organisations.

16. Appendix 1

Product / Service	Statute	Authority
Aerosol spray paint	Anti-social Behaviour Act 2003	Home Office / Local Authority
Air weapons and imitation firearms	Firearms Act 1968 Violent Crime Reduction Act 2006	Home Office / Local Authority
Alcohol	Licensing Act 2003	Home Office / Local Authority
Butane lighter refills	Cigarette Lighter Refill (Safety) Regulations 1999	Home Office / Local Authority
Cinema films	Licensing Act 2003	DCMS / Local Authority
Crossbows	Crossbows Act 1987	Home Office / Local Authority
Caps, cracker snaps, party poppers	Pyrotechnic Articles (Safety) Regulations 2015	Home Office / Local Authority
Fireworks	Pyrotechnic Articles (Safety) Regulations 2015	Home Office / Local Authority
Gambling	Gambling Act 2005	DCMS / Local Authority
National lottery	National Lottery etc Act 1993 National Lottery Regulations 1994	DCMS / Local Authority
Petrol	Petroleum (Consolidation) Regulations 2014 Health and Safety at Work etc. Act 1974	Home Office / Local Authority
Pets	Animal Welfare Act 2006	Ministry of Justice / Local Authority
Publications (considered harmful to children)	Children and Young Persons (Harmful Publications) Act 1955	Home Office / Local Authority
Sale of knives and articles with a blade or point	Offensive Weapons Act 1996 + 2019 Criminal Justice Act 1988	Home Office / Local Authority
Sunbeds	Sunbeds (Regulation) Act 2010 Sunbeds (Regulation) Act 2010 (Wales) Regulations 2011	DHSC / Local Authority
Tattooing	Tattooing of Minors Act 1969	Home Office / Local Authority

Tobacco products	Children and Young Persons Act 1933 (as amended) Children and Young Persons (Protection from Tobacco) Act 1991 Children and Young Persons (Sale of Tobacco etc.) Order 2007	DHSC / Local Authority
Video works and video games	Video Recordings Act 1984	DCMS / Local Authority