Inquiry into AV for online wagering and online pornography

Submitted by:

Dr Rachel O'Connell, author of the PAS 1296 Age checking code of practice published by the British Standards Institution in March 2018. Founder and CEO of TrustElevate.

Question 1: Its potential as a mechanism for protecting minors online

Legislative requirements with respect to age-restricted products and services – including alcohol, tobacco, knives, fireworks, spray paints, solvents and petrol, gambling, film and gaming content – share the common objective of protecting the health, safety and wellbeing of young people. Recent advances in the technology which can be used to enable age verification has galvanised public authorities in pushing for its implementation. This is occurring alongside a global push among lawmakers for strengthened data protection and improved digital business practices. Where age verification may have formerly been seen as too great a burden for industry to shoulder, the potential for its robust implementation has grown exponentially and it is ready to be made a reality.

In fact, efforts toward standardisation, as part of the process of realisation, have led to the publication of specifications, including the PAS 1296 Age Checking code of practice. This PAS was published by the British Standards Institution in March 2018 and is due to become a global standard in the coming months. It was written to assist those businesses that are mandated to comply with legal requirements in conducting age checks. It provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the kind of solution that meet a business's specific regulatory compliance needs.

Traditionally, to verify that an individual is, for example, 18+ years of age, the collection of a significant amount of personal data, including name, address, and date of birth, is required. In effect, age verification involves a full identity verification process. Recent technology and policy innovations in the electronic identity sector mean that it is now possible for age check services to check a single attribute of an individual's identity (i.e. age-related eligibility). For this reason, the term "age checking" is used throughout the PAS 1296 to differentiate between traditional methods of age verification and those currently available on the market.

"Age check services" is an umbrella term that includes both age check providers and age check exchanges that enable a range of business sectors to meet evolving legal, self- and co-regulatory requirements so as to establish an internet user's age-related eligibility for access to content and services online. Age check services can meet the needs of a range of age-rated services that might require either a specific age or the age band into which a

customer fits, which might be for instance over 18, or under 13 years of age. An age check elicits a yes/no response to a query, for example, 'is this person over 18 years of age?' or 'is this person below 13 years of age?'.

Importantly, PAS 1296 is a code against which age-check providers can be certified today.

Strength of identity attribute proofing
In terms of proofing the identity attributes asserted by an end-user, there are different levels to which this can be done, each of which corresponds to a different level of assurance or confidence in the asserted attribute's association with an actual identity.

The legal requirements that stipulate the strength of identity attribute proofing and the number of related checks that must be applied differ in the context of online gambling, advertising age-restricted goods and services, and accessing adult content. Therefore, what is required are tech solutions that cater for granularity.

- To meet Know Your Customer (KYC) requirements stipulated in Anti-Money Laundering (AML) legislation, gambling operators must conduct robust identity verification.
- The legal requirements placed on adult content providers, where there is sensitivity about linking adult content viewing habits to an individual, requires age-related eligibility checks conducted by a certified third party, operating in an identity ecosystem.
- General audience platforms that enable, for example, online gambling adverts also require age-related eligibility checks.

These distinctions are essential to bear in mind.

How is it possible to run a pseudonymous age-related eligibility check?
Traditionally, digital identity ecosystems rely on what are known as Levels of Assurance (LoA). The LoA scale that underpins U.S. and EU digital identity schemes ties together identity proofing and the strength of the credential used to log in, presenting them as a single value. LoA binds the physical identity of a person to the digital identity in a manner that is understandable by a computer system.
However, LoA does not comfortably accommodate a great deal of granularity. J. Richer proposed that, by separating the components of the process and applying a mechanism for describing and signalling several aspects that are used to calculate trust placed in a digital identity transaction, it is possible to introduce greater granularity in a standardised manner. The orthogonal scalar approach to determining the components of the verification and the authentication processes is called Vectors of Trust (VoT), as follows:

- How strongly the person was identity proofed, which ties to their physical identity
- How resistant a given credential is to attacks like impersonation, guessing, and theft
- How strongly a given transaction's assertion is protected as it's passed between parties over the network

Vectors of Trust is now composed of four components:

1. identity proofing;
2. primary credential usage;
3. primary credential management;
4. assertion presentation.

1. *Identity proofing*

"The Identity Proofing dimension defines, overall, how strongly the set of identity attributes have been verified and vetted. In other words, this dimension describes how likely it is that a given digital identity transaction corresponds to a particular (real-world) identity subject.
This dimension SHALL be represented by the "P" demarcator and a single-character level value, such as "P0", "P1", etc. Most definitions of identity proofing will have a natural ordering, as more or less stringent proofing can be applied to an individual. In such cases it is RECOMMENDED that a digit style value be used for this component."

2. *Primary credential usage*

"The primary credential usage dimension defines how strongly the primary credential can be verified by the IdP. In other words, how easily that credential could be spoofed or stolen.
This dimension SHALL be represented by the "C" demarcator and a single-character level value, such as "Ca", "Cb", etc. Most definitions of credential usage will not have an overall natural ordering, as there may be several equivalent classes described within a trust framework. In such cases it is RECOMMENDED that a letter style value be used for this component. Multiple credential usage factors MAY be communicated simultaneously, such as when Multi-Factor Authentication is used."

3. *Primary credential management*

"The primary credential management dimension conveys information about the expected lifecycle of the primary credential in use, including its binding, rotation, and revocation. In other words, the use and strength of policies, practices, and security controls used in managing the credential at the IdP and its binding to the intended individual.
This dimension SHALL be represented by the "M" demarcator and a single-character level value, such as "Ma", "Mb", etc. Most definitions of credential management will not have an overall natural ordering, though there can be preference and comparison between values in some circumstances. In such cases it is RECOMMENDED that a letter style value be used for this component."

4. *Assertion presentation*

"The Assertion Presentation dimension defines how well the given digital identity can be communicated across the network without information leaking to unintended parties, and without spoofing. In other words, this dimension describes how likely it is that a given digital identity was actually asserted by a given identity provider for a given transaction. While this information is largely already known by the RP as a side effect of processing an identity assertion, this dimension is still very useful when the RP requests a login (and when describing the capabilities of an IdP. This dimension SHALL be represented by the "A" demarcator and a level value, such as "Aa", "Ab", etc. Most definitions of assertion presentation will not have an overall natural ordering. In such cases, it is RECOMMENDED that a letter style value be used for this component."

NOTE In the context of the Vectors of Trust definitions, the vector value "P1.Cc.Ab" translates to "pseudonymous, proof of shared key, signed browser-passed verified assertion, and no claim made toward credential management".
The vector value of "Cb.Mc.Cd.Ac" translates to "known device, full proofing required for issuance and rotation, cryptographic proof of possession of a shared key, signed back-channel verified assertion, and no claim made toward identity proofing" in the same context.

It is not only the PAS 1296 Age checking code of practice which utilises VoT. The latest version of US NIST 800-63 digital authentication guidelines refers to Vectors of Trust. The NIST guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT

systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.

Digital platforms and service providers must also take responsibility for advertising. In the case of Facebook, for example, algorithms were found to have associated hundreds of thousands of children's profiles with an 'interest' in gambling and/or alcohol, potentially exposing them to targeted advertising and driving them to participation or consumption. Recent data has revealed that 90% of 18 year old males have been exposed to pornography, and of that group, 90% the average age these young men were sexualized by pornography was between 8-11 years old.

In moving forward with age verification, it is important to frame the discussion in terms of good business practice: it is not simply about limiting children's access to specific products and services. Rather, age verification would provide children with the liberty to explore the internet freely whilst putting in the proper provisions for their protection.

Question 2: requirements of Commonwealth, state and territory government laws, policies and practices (including technical and privacy requirements) that relate to and enable improved age verification requirements.

Australia's Digital Identity Ecosystem

Australia's digital identity ecosystem is made up of agencies, private sector businesses and systems working together to deliver a secure way to prove someone's identity online to access services – a federation. The Australian Government's accredited identity exchange is run by the Department of Human Services. The identity exchange is run double-blind, ensuring that the identity service provider can't see what service the user is accessing, and digital services can't see someone's personal information.

Trust Frameworks constitute the legal underpinnings which enable the proper functioning of identity federations. They exist as multilateral agreements, the next step up from resource-intensive and friction-generating bilateral contracts. This network of multilateral agreements comes under the umbrella of an Identity Ecosystem, which must also have a set of standards stipulated in its own Framework. Australia's Trusted Digital Identity Framework (TDIF) sits across all accredited elements of the program and ensures all providers meet standards for usability, accessibility, privacy protection, security, risk management, fraud control and more.

In effect, the technical and legal architecture that can enable new and emerging privacy preserving, secure, scalable age check services is in place, in Australia. In a federated model, a "verify once, use many times" approach can reduce the cost of an age check and thereby compliance with regulatory requirements. Note, too, that the costs of age verification measures are far outweighed by the risk of incurring huge financial penalties for non-alignment with regulation.

Basic and Advanced Digital ID: Lessons from around the globe

Basic digital ID simply enables verification and authentication, whereas digital ID with advanced applications enables the storing or linking of additional information about individual

ID owners and thus can facilitate advanced data sharing, with informed user consent.
For example, when an individual pays taxes, an advanced ID system would allow the individual to give the tax authority consent to digitally access the relevant bank information, investment accounts, and employment records necessary for filing quickly and without error. In mature economies, basic digital ID programs that lack advanced data-sharing functionality have seen low adoption in the UK, Germany, and Austria. Basic digital ID that is useful in a limited number of scenarios is unlikely to be adopted. Whereas higher-functionality digital IDs which can be used to, for instance, open a business bank account, which is automatically linked with the tax office, and with which it is possible to take out a mortgage for business premises, have achieved adoption rates of more than 70% in Estonia, Sweden, and Norway, among others.

The Australian Identity Exchange, operating as per the rules stipulated in the TDIF could underpin innovative, cost effective, scalable, privacy-preserving age checking schemes and even reduce future implementation costs. There are examples of successful implementations of similar schemes, in EU member states.

Question 3: The potential benefits of further online age verification requirements, including to protect children from potential harm, and business and non-government organisations from reputation, operational and legal risks

Moving beyond the use of age verification in the case of age-restricted goods and services, it is possible to see the advantages of a digital world in which platforms and service providers know their users better. According to Pew Research Center, as of 2018, 95% of teens now report they have a smartphone or access to one. Smartphones enable accessibility and, in turn, 45% of teens now say they are online on a near-constant basis. As children and young people spend more time online, the likelihood of their exposure to age-inappropriate content or communications similarly increases.

Limits on screen time fall under parents' remit, but it is the duty of regulators and platforms alike to limit children and young people's exposure to inappropriate content. In age verifying users, it will be possible to identify the content and services that is most age-appropriate for them and deliver them, independent of the more harmful or age-inappropriate content which may still be hosted or served to older users. Age verification, then, would enable the creation of safer spaces for children to learn and explore freely without the risk of accidentally coming across that which has been designed with an adult user in mind.

As long as companies are able to say that they have implemented blocks to prevent children's access, despite children's capacity to circumvent those blocks, they can evade their duty of care toward those users who have gotten around the blocks. Indeed, if a platform or service provider is appealing to children then they should be held accountable for that appeal. If, instead, they were to reliably verify children and young people's age, they could begin to recognise their presence in the audience and cater to them, integrating the principles of safety by design.

Moreover, as time spent online increases and the number of platforms and services engaged with increases, it becomes more and more difficult for parents to have the necessary oversight over their children's activities. There is a critical distinction to be made between Intended and Actual Audiences that requires platforms to recognise children as users.

In Europe, the most common approach to the regulation of the online gambling market is through licences, although the details of these licenses vary by country. By making the legality of a gambling service dependent on a licence, the government has extensive control

over the functioning and duties of the operators that serve its population, so long as this is backed up by regular audits or enforcement checks. This allows governments to ensure that a system of oversight with respect to identification and age-verification, KYC and AML operates effectively. Denmark and Italy, for example, have developed a standard interface, which operators must include in the registration process. The personal information that is provided by the prospective gambler is checked against official government databases. Italy uses the "Fiscal Code" identifier, which is used for tax purposes, whereas Denmark uses a new identifier called NemID. A prospective gambler must go to a local Danish government office to apply for a NemID, at which point identification takes place, after which he will be sent the identifier. Similarly, in Spain, customer asserted data is checked against an eID database to which the Spanish regulator affords operators access.

In effect, age verification would be a major asset in terms of both preventing harm and avoidance of legal or financial penalties. Ultimately, that is at the heart of the issue: prevention. Age verification constitutes a distinctly effective preventive measure against the delivery of age-inappropriate content, communications, products and services and against businesses and NGOs falling foul of the law by way of insufficient checks or mishandled data.

Question 4. The potential risks and unintended consequences in further restricting age verification requirements, including, but not limited to:

a) pushing adult consumers into unregulated/illegal environments or to other legal forms of these activities;
b) privacy breaches;
c) providing false assurance to parents and carers; and
d) freedom of expression

The broad realisation of age verification measures across the internet will, no doubt, lead to some unintended consequences. The digital offerings of platforms and service providers will inevitably become adapted for a new, more inclusive landscape. The content and services they deliver will broaden in range and better serve those users that were already being appealed to. This does not mean, though, that those services and content delivered to adults will have to be made more appealing to children. Age-restricted content will not cease to exist. Core to the proposition of age verification is knowing users better and being better able to cater to their specific needs. This will foster innovation, encourage digital participation and enable segmentation such that adults and children alike have access to age-*appropriate* content.

In discussions surrounding the UK's 'porn ban', a proposed age verification barrier emerging out of the Digital Economy Act, commentators noted the potentially devastating risks associated with creating repositories of data. They anticipated these repositories holding associations between digital identities, traceable to individuals, and sexual habits and proclivities. Any breach of such data could have devastating consequences. It is not the case, though, that the collection and storage of identifying data would be necessary for the operation of age verification mechanisms. Instead of verifying an individual's age by way of an identity check, it is possible to conduct an identity attribute check – age being just one of many attributes of an individual's identity. The British Standards Institution PAS 1296 Age Checking code of practice in March 2018, describes how such age-related eligibility checks can be conducted in a secure, privacy-preserving, scalable manner.

Data minimisation is a principle, enshrined in the General Data Protection Regulation, that states that data collected and processed should not be held or further used unless this is

essential for reasons that were clearly stated in advance to support data privacy. Identity Attribute Exchanges are online internet gateways for companies to access user-asserted, permissioned, and verified attributes. The use of an Identity Attribute Exchange would enable age verification in accordance with the principle of data minimisation. An Exchange may well be leveraged by the UK government in proceeding with their efforts to age-restrict access to online pornography.

Providing assurance to parents and carers is certainly an anticipated outcome of age verification measures. The assurance provided, though, is that there are provisions in place to facilitate digital parenting by enabling greater oversight and consent management. Age verification for <16s, would not remove responsibility from parents and enforcing platforms and service providers' singular duty of care, but rather seeks to share the duty of care for children and young people across members of the digital ecosystem, of which parents are equally participants. Such measures provide tools for more proactive engagement rather than complacency. Age verification is complementary, rather than an alternative, to considered and age-appropriate advice and guidance on the part of parents, educators and others responsible for the wellbeing of children.

Further, one of the concerns that has emerged is the issue of potentially creating a walled garden which only serves to highlight to sexual predators or those seeking to harm children. However, the very fact of age verification would prevent those individuals' access. Robust implementation, in accordance with the principles of safety by design, would construct walls, supported by intelligent monitoring systems capable of both detecting and withstanding such attempted breaches.

In terms of freedom of speech, some may worry as to its limitation in some fashion. Turning to those Conventions in which such freedoms are enshrined, though, one can see that they have not been granted unconditionally. Article 10 of the European Convention on Human Rights, effective as of 1953, provides the right to freedom of expression and information, subject to certain restrictions: "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the *protection of health* or morals, for the *protection of the reputation or rights* of others". Freedom of expression, then, has long been subject to restriction as it relates to the protection of health and rights of others. Exposure to harmful content online has been found to inflict real damage on children and young people and encourage unhealthy behaviours and sexual attitudes.

Further, the United Nations Convention on the Rights of the Child's Article 17 asserts that states must "ensure that the child has access to information and material from a diversity of national and international sources". They must also "encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being". It is children's right to access information via the internet while being protected from harmful media. Restrictions on freedom of expression would only occur in such instances as to protect the health and wellbeing of children and to maintain their right to access information. Age-gating content and services would not be restricting freedom of expression but rather enabling it according the terms of the international treaty in which it is found.

Question 5: Best practice age verification requirements internationally, including standards, verification and implementation timeframes, and particularly the likely

effectiveness of the proposed age verification for access to online pornography in the United Kingdom's Digital Economy Act 2017

Part 3 of the UK's Digital Economy Act 2017 concerned age verification for online pornography. The Act instated an age verification regulator, the British Board of Film Classification (BBFC), to produce guidelines for those commercially hosting pornography to ensure that their users were 18 years of age or older. The BBFC was given the authority to investigate businesses and platforms and pursue action against those found to be non-compliant. Fines of up to £250,000 or 5% of annual turnover could have been levied against non-compliant sites. Other penalties include blocking non-compliant sites and requiring those providing financial or advertising services to non-compliant websites to cease doing so.

Much has been made of the supposed 'scrapping' of the so-called 'porn ban' over recent weeks. Nicky Morgan, the Culture Secretary, has stated that rather than the measures having been ditched, they have been stalled. In the name of coherence, the measures have been delayed and will be delivered at a later juncture "through our proposed online harms regulatory regime. This course of action will give the regulator discretion on the most effective means for companies to meet their duty of care."

She noted, too, that the current draft of the DEA "does not cover social media platforms". Those platforms hosting pornography on a non-commercial basis, then, would not have been affected by the Act. In seeking to effectively address the issue of premature exposure to adult content, incremental measures may well only have dispersed users and pushed them to other sites – the decision to delay and institute more comprehensive measures is likely for the best. In tackling the issue at once, the government will be able to more successfully align the social norms and expectations as they pertain to duty of care and age-restriction procedures with those of the digital world.

Question 6: Barriers to achieving stronger age verification requirements, including but not limited to:

a) capabilities of existing technology of business and verification providers;
b) access, adequacy and security of third-party and government databases; and
c) accurate and standardised capture of customer information

The technology is ready and available. The standards that underpin how these solutions operate and the due diligence companies need to conduct when contracting with an age-check provider are detailed in documents such as the PAS, and related technical standards. The legal contracts that underpin the deployment of a federated solution[1] can be detailed in a Trust Framework.

The accurate and standardised capture of customer information is not a barrier, but rather a requisite of any form of data processing, controlling or handling. Article 5(1)(d) of the General Data Protection Regulation asserts that, "Personal data shall be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')".

[1] Identity Federation: A protocol in which an Identity Provider (IdP) asserts a user's identity information to a Relying Party through the use of a cryptographic assertion or other verifiable mechanisms, or system implementing such a protocol. It is also referred to simply as "federation".

Question 7: Education and warning messages associated with age verification

In 1957, Dr Breault landed the position of Chief of Pediatrics and Director for the Poison Control Centre back at the Hotel Dieu Hospital. He began seeing cases of accidental childhood poisonings on a daily basis—especially children that had managed to ingest their parents' medication, often Aspirin. The annual poisoning rate steadily rose to 1,000 cases per year in the Windsor, Ontario area, with at least one fatality. Dr Breault decided to take action to try and stop these accidental poisonings and deaths.

First, he started a **public awareness campaign which failed to make an impact on the problem**. Realizing that if people wouldn't change voluntarily, he'd have to make it involuntary, he came up with the idea of child-proof containers. He formed the Ontario Association for the Control of Accidental Poisoning or O.A.C.A.P. The *child-resistant* locking closure for containers was invented in 1967 and resulted in a **91% reduction** in accidental childhood poisonings. Soon child safety caps were mandated not only in Canada but around the world. There is a wealth of information available on the efficacy of education campaigns, messaging, iconography associated with child safety caps that can be adapted to online verification.

Segmentation
The public's views of children's online safety are complicated. Parents are concerned about children's welfare online but recognize that to deny children access to the internet may impede a child's education.
Is it possible to draw parallels with the inherent contradiction in people's attitudes towards child safety online and the issue of privacy and, if so, are there lessons to be learned?
In this regard, it is useful to consider the work of the U.S. privacy academic Westin who developed the three-way segmentation of people's attitudes toward privacy.

- **Privacy pragmatists**: those who will make trade-offs on a case-by-case basis as to whether the service or enhancement of service offered is worth the information requested
- **Privacy fundamentalists:** those who are unwilling to provide personal information even in return for service enhancement
- **Privacy unconcerned:** those who are unconcerned about the collection and use of personal information about them

Are there child online safety pragmatists, fundamentalists and unconcerned, and what other segmentation might be applicable? There are valuable lessons to be learned about how people within these segments respond to marketing and educational campaigns.

Question 8. The economic impact of placing further restrictions on age verification on business, including small business, and the potential financial and administrative burden of such changes

Age verification measures may initially appear to be detrimental to many organisations' business models. Some may fear that an increase in onboarding or sign-on friction may alienate users, leading to higher drop-off rates, and that a portion of the user base may be lost due to being too young to use their services under the current regulation. That being said, many age checking solutions have made ease of use and user experience central to their services: they are actively seeking to minimise any introduced friction and, as these measures must be usable by children, ease of use is a key principle of their design. Additionally, those digital platforms and services concerned about losing a portion of their

user base are necessarily non-compliant and stand to face fines much greater than the cost of losing underage customers would be.

The commercial models that underpin an identity ecosystem can be flexible enough to enable businesses that are not generating sufficient revenue, to run checks at a lower cost, or free, which mitigates concerns around stifling innovation or the imposition of overly burdensome costs.

Regulation and properly governed age verification measures could lead to a digital landscape in which safety by design is the norm and general audience sites are capable of differentiating both their users and services. Adult users remain on the platform, as do children and young people, but the platform differentiates these users according to the age group to which they belong and adapt their services to cater to those differentiated users. One could anticipate from this an increase, rather than decrease, in the potential user base. In being more inclusive in this fashion, businesses will be able to enhance family propositions, boost customer acquisition/retention and establish brand loyalty. Such enhancement can lead to a diversification of product offerings that can create cross and upsell opportunities, yielding increased revenue streams and a return on investment.

ID programs globally have seen a massive uptick over the past few decades. With an eye toward interoperability and cost reduction in the case of cross-border eID authentication, the EU initiated the Secure idenTity acrOss boRders linKed (STORK) project. This drive toward interoperability is underpinned by the rationale that secure and reliable methods of identity and attribute verification are required for the proper functioning of the digital economy, as well as to reduce incidences of fraud and identity theft.

The findings of the STORK project also informed the drafting of the EU Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), adopted in 2014. It created a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It did so by creating a European internal market for electronic trust services. Moreover, the World Bank ID4D Findex survey25 suggests that digital ID could contribute to providing access to financial services for the 1.7 billion+ individuals who are currently excluded from access to such services. Digital ID can also help to provide access to critical government and economic services that they may currently be denied, including government benefits and labour markets

Question 9. The impact of placing further restrictions on age verification on other eSafety resourcing, education and messaging

Legislation in relation to gambling, for example the UK Gambling Act 2005, specifically singles out children as a vulnerable group who should be protected from being harmed or exploited by gambling. It follows that application of the precautionary principle should be regarded in their case as particularly important. Actions that might potentially be harmful to children and young people, now or in the future, should be avoided unless there is evidence that proves they are not harmful. Children and young people are different to adults because of their stage of physiological and psychological development, their inexperience and their position in society. They are more vulnerable to gambling-related harms; and the harms they experience are likely to have a large impact, both now and in the future. It is important therefore to identify the conditions and to reduce the hazards that might impair children's ability to grow up safely.

The precautionary principle also applies to adult content and recent advances in identity authentication and assurance mean that public authorities bear a renewed interest in the

possibility of improving protection for minors through use of technological measures to verify age. In addition, developments in the range of commercial content and services now available online, in the technological devices and platforms used and the trend towards more private but networked use, even by children (Livingstone et al. 2011), means some of the most basic assumptions about the nature and extent of risk may also now be outdated.

Therefore, in addition to mechanisms which empower schools or parents to intervene in their children's Internet use, such as parental control technologies or educational campaigns or state-led initiatives which offer or require filtering of Internet content, tech and policy innovation that enable age verification must be considered. This is an appropriate moment to revisit questions about the appropriateness and efficacy of age verification measures for protecting minors in their online transactions and experiences. E-safety resourcing, education and messaging will need to be adapted accordingly.

Question 10: Australia's international obligations

- The European Union General Data Protection Regulation (the GDPR) contains new data protection requirements that apply from 25 May 2018.
- Australian businesses of any size may need to comply if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.
    - The use of an EU language or currency (other than the language/currency in the data controller's country of establishment) with the possibility of ordering goods and services in that other language, or references to EU customers or users, may make it apparent that the data controller envisages offering goods or services to data subjects in the EU.
    - 'Monitoring behaviour' specifically includes internet tracking of data subjects (eg via cookies), especially if the gathered data is subsequently used for profiling activities, eg to enable decisions to analyse or predict personal preferences, behaviours and attitudes.
- Australia also has obligations to build an identity federation in line with international protocols and standards to enable interoperability and mutual recognition. So that people with digital identities issued in other countries can be verified when in Australia and vice versa. Thereby enabling cross-border electronic transactions, such as enrolment in a foreign university, opening a bank account, accessing electronic health records. Australian citizens moving to another country will be able to manage administrative work online, cutting out the paperwork.