The Coming-of-Age of Technology:

Using Emerging Tech for Online Age Verifications

Carl Van der Maelen*

This article aims to introduce readers to the underexplored topic of online age verification (AV) procedures. These technical measures to bar minors' online access to age-restricted goods, content and services have returned to the limelight due to recent high-profile controversies and legislative evolutions. Two main arguments will be made. First, that current AV measures are not sufficiently accurate and efficient to effectively achieve their goal. Second, that innovative proposals to conduct age checks exist now that a market for AV mechanisms based on emerging technology is developing, but that caution must be exercised when considering them because of their possible impact on personal data protection principles and rights. In particular, profiling, the use of attributes, and voice recognition will be analysed as possible breakthroughs to achieve better age checks. Ultimately, this article will conclude that there is cause for optimism and that continued experimentation with emerging technologies to carry out AV procedures should be stimulated.

I. Introduction

Western societies impose legally enforced age limits to restrict minors' (or age brackets of minors') access to certain *goods* (eg alcohol or fireworks), *content* (eg pornography or violent media) and *services* (eg gambling, social network sites and dating services) because they might have harmful consequences for their physical or mental development. Although we take these age rules more or less for granted, the in-

ternet allows users to operate at a distance and with (a certain) anonymity, rendering the face-to-face and ID checks that retailers rely on in the physical world impossible. The goal of age verification (AV) mechanisms is to nonetheless impose a technical measure that verifies whether an internet user has the minimum age required to access age-restricted content and services, or to remotely order age-restricted goods.¹ Although the debate on the desirability and feasibility of online age verifications mostly raged in the late 90s and at the start of the millennium,² the discussion has made a remarkable comeback due to three major recent developments.

First, the United Kingdom in 2016 introduced an amendment to its Digital Economy Act that obliged anyone making 'pornographic material available on the internet to persons in the UK on a commercial basis' to carry out age verifications of their users and block anyone under 18 years. Although the policy has now been abandoned due to ongoing controversies and a lack of legal clarity, heavy financial penalties and the blocking of access to the material in question were foreseen.³

A second major development was the massive public backlash erupting in 2017 towards 'loot boxes' in the video game industry. The specialised gaming press already compared these randomised in-game

DOI: 10.21552/delphi/2019/3/4

* Carl Vander Maelen is a PhD Candidate at the Department of Law and Technology at Ghent University (Ghent, Belgium). This article is adapted from a presentation prepared for the Amsterdam Privacy Conference (September 2018). For correspondence: <Carl.VanderMaelen@UGent.be>

1 Definition based on the work of Nash et al. See: Victoria Nash and others, 'Effective Age Verification Techniques: Lessons to Be Learnt from the Online Gambling Industry' [2012] SSRN <<http://www.ssrn.com/abstract=2658038>> accessed 18 January 2019

2 See, the 1998 Child Online Protection Act (COPA) in the United States, and critical pieces such as: Amit Asaravala, 'Why Online Age Checks Don't Work' *Wired* (10 October 2002) <<https://www.wired.com/2002/10/why-online-age-checks-dont-work/>> accessed 18 January 2019

3 United Kingdom, 'Digital Economy Act 2017 c. 30 - Part 3' <<http://www.legislation.gov.uk/ukpga/2017/30/part/3/enacted>> accessed 18 January 2019

purchases to gambling,⁴ but the release of blockbuster *Star Wars Battlefront 2* saw the controversy spill over into mainstream media.⁵ One of the most interesting reactions came from the UK Gambling Commission, which suggests that a system of age verification should be installed in situations where video games would cross the line into gambling,⁶ similar to online gambling sites.⁷

The resurgence of interest in AV mechanisms coincides with a *third* major development: the European Union's legal reform of its personal data protection framework. The General Data Protection Regulation (GDPR) entered into force on 25 May 2018, reaffirming certain data protection principles of its 1995 predecessor, but also introducing novelties such as the acknowledgement that children merit specific protection with regard to their personal data. Although the GDPR nowhere explicitly mentions age verification measures, article 8 stipulates that if a data controller⁸ relies on consent as a ground of processing (under article 6, 1 (a)) when offering an information society service⁹ directly to children younger than 16,¹⁰ 'such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child'. Since the Article 29 Working Party (the former authoritative advisory body on EU personal data protection) indicated that consent given by an underage child renders the processed data unlawful,¹¹ data controllers have a strong incentive to verify users' ages.¹²

As will be demonstrated, however, current AV practices are sorely lacking in accuracy and efficiency (section II). The need thus imposes itself to consider alternative, innovative AV proposals, although these too can have important drawbacks – in particular with regard to personal data protection principles (section III).

II. Current Age Verification Procedures are Inadequate

While research shows that the online gambling industry has been largely successful in blocking minors from gambling,¹³ other sectors have long since struggled in determining an effective, standardised approach to online age checks: a questionnaire of e-commerce enterprises in the UK found that no less than 79% of them were concerned that their existing verification procedures still allowed age-restricted goods to be sold to minors.¹⁴ Legal uncertainty abound, certainly since the UK Chartered Trading Standards Institute indicated that there is no widespread consensus on the technical and procedural aspects of AV mechanisms.¹⁵

Individual websites and services have hence attempted to create their own age verification procedures. An analysis of several websites and their procedures allows us to construct a typology of five age verification methods that are currently widely em-

4 Vic Hood, 'Are Loot Boxes Gambling?' *Eurogamer* (12 October 2017) <<https://www.eurogamer.net/articles/2017-10-11-are-loot-boxes-gambling>> accessed 18 January 2019

5 Sarah E Needleman and Ben Fritz, 'Electronic Arts Pulls Microtransactions From 'Star Wars Battlefront II' After Fan Backlash' *Wall Street Journal* (17 November 2017) <<https://www.wsj.com/articles/electronic-arts-pulls-microtransactions-from-star-wars-battlefront-ii-after-fan-backlash-1510936871>> accessed 18 January 2019

6 UK Gambling Commission, Loot boxes within video games (2017), <https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Loot-boxes-within-video-games.aspx>.

7 European Commission, 'Commission Recommendation on Principles for the Protection of Consumers and Players of Online Gambling Services and for the Prevention of Minors from Gambling Online'

8 In the words of article 4(7) GDPR, a data controller is 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'

9 An information society service is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. See: European Parliament and European Council, Directive laying down a proce-

cedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (2015), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2015:241:FULL&from=EN> (last visited Jan 29, 2019), article 1, 1 (b)

10 There can be lower national age thresholds, ranging from 13 to 15. For an overview of the applicable age in every EU Member State, see: Eva Lievens and Ingrida Milkaite, 'Better Internet for Kids - GDPR: Updated State of Play of the Age of Consent across the EU' (June 2018) <<https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751>> accessed 18 January 2019

11 Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (2017) 25

12 Eva Lievens and Ingrida Milkaite, 'The Internet of Toys: Playing Games with Children's Data?', *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Play* (Palgrave Macmillan 2018)

13 See (n 1)

14 LexisNexis, 'Online Age Verification: The Issues Surrounding Age-Restricted Goods (2017)'

15 UK Chartered Trading Standards Institute, 'Online Sales of Age-Restricted Products' (July 2017) <<https://www.businesscompanion.info/en/quick-guides/distance-sales/online-sales-of-age-restricted-products>> accessed 18 January 2019

ployed. While no measure can be considered completely immune to errors or fraud, it is possible to make a distinction between 'soft' and 'hard' AV measures based on the effort for minors to circumvent or deceive the system.¹⁶ The methods have been ordered accordingly, from 'softest' (being the easiest to deceive) to 'hardest' (being the most difficult to circumvent):

1. self-certification, such as tick boxes, age affirmation pages (AAPs), and age disclaimers;
2. reliance on e-payment services by performing a small transaction;
3. reliance on credit cards, such as verifying the card information or performing a small transaction;
4. use of data aggregation services;
5. identity document scanning and eID systems (the electronic identification card of citizens).

The five identified methods will be briefly discussed regarding their respective weaknesses and strengths.

1. Self-Certification

Self-certification asks users to verify themselves that they are above a certain minimum age by ticking a box or writing their date of birth before entering a website or creating an account. Age disclaimers simply state (usually in a banner on a webpage) that the host considers anyone accessing the content and / or services to be the required minimum age.

These methods are incredibly easy to bypass and do not carry out an age 'verification' in any way. Even in the case that a minor would answer truthfully and cookies remember to bar entry to the user, session

cookies are simply undone when the browser is closed and more advanced cookies can be circumvented through incognito browsers or by adjusting browsers' cookie settings.

2. Reliance on E-Payment Services

This method grants users access on the condition that they perform a small transaction (for example of 0.01 euros) through an e-payment service. This too fails to carry out an actual verification of the user's age since merely having or using such an account is not *per se* proof of adulthood: many e-payment services (including the popular Paypal and Worldpay) can be linked to debit cards, which are also available to minors.

3. Reliance on Credit Cards

Some sites seek to verify a user's credit card information, or ask that a small credit card transaction is performed. Although this might seem similar to the second method of relying on e-payments, credit cards form part of a strictly regulated system. Because of the stringent financial and administrative conditions imposed – one of them being that minors cannot request credit cards in most jurisdictions – it is a much more reliable way to distinguish between adults and minors.

That is not to say no flaws exist. There are many examples of youngsters using the credit card of their parents without consent.¹⁷ Although any potential transactions will afterwards show up on the adult's credit statement, the child will usually have gained access to the age-restricted matter by the time the misuse is discovered. Additionally, it is possible to add children as an 'authorised user' to an adult's card, circumventing the AV measure entirely. However, this last situation highlights the role of parents in evaluating whether or not their child can be trusted with the responsibilities that come with a credit card.

Moreover, the binary results of credit card verifications raises another problem: adults without credit cards have no way to prove their age and are thus unjustly excluded.¹⁸ Studies have shown that about 75.7 percent of American consumers possess at least one credit card,¹⁹ meaning that over 20 percent of the adult American population would be denied ac-

16 Daniel Koller, *Cybersex. Die strafrechtliche Beurteilung von weicher und harter Pornographie im Internet unter Berücksichtigung der Gewaltdarstellungen* (2007) 160

17 the guardian 'Boy, 12, Steals Credit Card and Goes on Bali Holiday after Fight with Mother' *The Guardian* (23 April 2018) <<https://www.theguardian.com/australia-news/2018/apr/23/boy-12-steals-credit-card-and-goes-on-bali-holiday-after-fight-with-mother>> accessed 22 January 2019

18 Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions* (Progress & Freedom Foundation Progress on Point Paper No. 14.5) (2007) 17

19 Federal Reserve Bank of Boston, 'The 2015 Survey of Consumer Payment Choice: Summary Results' (Federal Reserve Bank of Boston, 28 September 2017) <<https://www.bostonfed.org/publications/research-data-report/2017/the-2015-survey-of-consumer-payment-choice-summary-results.aspx>> accessed 22 January 2019

cess to online content, goods and services that they should have access to.

4. Use of Data Aggregation Services

A similar scenario unfolds when companies rely on data agencies to collect and compile information from publicly available datasets such as credit history, driving license databases or electoral history.²⁰ Here too, some adults are unjustly denied access, for example because they have never applied for credit and do not possess a driving license. One source states that this process would leave around 15% of the UK's adult population unidentified.²¹

An additional shared flaw between methods three and four due to their binary outcomes is that they do not allow for any distinctions between internet users under 18. Minors cannot apply for credit, nor possess electoral information; methods three and four can therefore only conclude whether a user is an adult or not, rendering these methods useless for goods or services that have different age ratings than 18+, such as 16+ or 12+.

5. Identity Document Scanning and the Use of eIDs

The fifth method (respectively sending scans of identity documents and making use of citizens' electronic identification cards (eIDs)) are the only ones resistant to the aforementioned problems. Adults are not unjustly excluded, and precise distinctions among minors are possible (on the uncertain condition that minors receive identity documents; see *below*). Although there is always the possibility that individuals commit fraud with identity documents, the heavy penalties on identity fraud²² should act as a deterrent, while verifying the submitted information within a government database provides a strong safeguard. Method five is thus provides two reliable ways of determining an individual's age.

Nevertheless, there are drawbacks. The scanning and sending of identity documents (method 5) over unsecured lines opens the door for identity theft by third parties. While using eIDs (method 6) proves much safer in that regard, their use from consumers' homes would necessitate several crucial elements: a widespread dissemination of eID card readers to cit-

izens, the presence of a governmental infrastructure that allows a smooth interface between state administration back-ends and consumer-friendly front ends, a high level of cybersecurity, and the granting of identity documents to minors to allow for the age ranges under 18. Additionally, several jurisdictions (most notably the UK and the US) do not have the tradition of using identification documents that continental Europe has, further calling into question the large-scale feasibility of methods five and six.

Nevertheless, there are methods currently available to successfully conduct AV procedures. The British Standards Institution (BSI) has helped to develop PAS [Publicly Available Specification] 1296:2018, a code of practice to assist providers of age-restricted goods and services. The code is innovative in that it focuses on eligibility and vectors of trust, and although an extensive analysis would lead us too far here, its approach is well-considered and displays respect for personal data protection principles. Importantly, however, it does not advise on the practical implementation of an actual age checking system, let alone how to incorporate existing age check exchange programs into a corporate infrastructure – meaning that smaller business will find it difficult to translate the theoretical advice offered in the code to actual compliance.

III. An Emerging Market of Innovative Ideas

For that reason, it is advisable to cast an eye toward the emerging market of AV technology that has risen as a result of the pace of technological evolution and immense availability of personal data.²³ These solutions also seek to achieve more accurate and efficient AV mechanisms, and additionally pay extensive attention to user-friendliness – both from an online user's side, and the business perspective. However, a main concern is their impact on personal data protection principles.

20 It must be noted that conducting an age check through data aggregation is oriented towards the British and American markets, since continental European jurisdictions do not generally make this information public.

21 (n 1) 26

22 See, for example: United Kingdom, 'Fraud Act 2006' s 1(3); Belgium, 'Strafwetboek' article 210

23 MEECO, The Rise of The Attribute Economy 2.0 (2017), 24

One of the most innovative and eye-catching proposals in that regard is to use *profiling* to carry out age verifications. Profiling is a processing practice often driven by artificial intelligence (AI) that aims 'to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects'²⁴ and is most often associated with targeted advertising practices. In spite of its controversial status, several companies have begun to offer profiling as a method of age verification.²⁵ Additionally, PAS 1296:2018 encouragingly denotes the similar concept of 'social proofing', which it describes as an 'analysis, with a user's consent, of their digital footprint and the related social graphs, which can be interrogated to determine the veracity of a self-asserted identity'.²⁶

Moreover, there are strong indications that profiling children to conduct an accurate age check would not *per se* infringe personal data protection principles: this point is made by the Article 29 Working Party itself in its Guidelines on Profiling, where it notes that '[t]here may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including

profiling, ... to children, for example to protect their welfare'.²⁷ Safeguards to protect the legitimate interests of children should nevertheless remain in place.²⁸

The downside to profiling is its processing of large amounts of data – which are possibly sensitive – by private actors. A workaround would be to work with *attributes*. These can be roughly divided into immutable (unchangeable facts, such as data of birth), assigned (biographical information, such as name(s) and nationality) and related attributes (changeable information, such as address and occupation).²⁹ The strength of attributes is that, by combining several of these general attributes, a more specific profile is created which determines whether access is granted. The user is never identified, since the attributes can be applicable to a multitude of individuals. Apps that employ this approach already exist, such as IRMA: short for 'I Reveal My Attributes', this app developed by the Dutch foundation Privacy by Design lets users 'selectively disclose only relevant properties (attributes) of yourself'³⁰ and is highly consumer-friendly due to its streamlined use and portability, and business friendly due to its free and tech-light nature.

The increasing popularity of AI-powered 'smart home assistants' such as Amazon Echo and Google Home³¹ has led to the suggestion of using *voice recognition for identity verification*. Already in 2015, Amazon started developing Voice ID for Alexa, enabling the AI to distinguish between different users.³² Besides giving personalised responses, this might also block children from ordering age-restricted matters via voice assistants. Voice recognition technology, however, raises its own set of data protection questions: a recent investigation into Google Assistant revealed that users are sometimes unknowingly recorded and that human contractors transcribe some of the recordings,³³ and corporations' desire to improve their products and make purchasing recommendations based on consumer data³⁴ stands at odds with the principles of data minimisation and purpose limitation. Nonetheless, this approach certainly holds potential, mostly due to its very intuitive nature.

Inspiration for future innovative proposals might also be found in the procedures that the US Federal Trade Commission has approved to gain verifiable parental consent under the Children's Online Privacy Protection Act (COPPA). For example, *knowledge-based authentication* (KBA) asks the user to answer 'dynamic, multiple-choice questions, (...) of sufficient

24 Article 4(4) GDPR

25 See, Hello Soda, 'Age Verification Checks and Insights with PROFILE' <<https://hellosoda.com/age-verification/>> accessed 23 January 2019

26 British Standards Institution, PAS 1296:2018 – Online Age checking – Provision and Use of Online Age Check Services – Code of Practice (2018) 3

27 Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2017) 28

28 *ibid*

29 Vincent Hu and others, *Attribute Based Access Control* (2017) <<https://csrc.nist.gov/publications/detail/book/2017/attribute-based-access-control>> accessed 25 January 2019

30 Privacy By Design Foundation, 'About IRMA' (*Privacy by Design Foundation*) <<https://privacybydesign.foundation/irma-en/>> accessed 6 October 2018

31 Abrar Al-Heeti, 'Amazon Has Sold More than 100 Million Alexa Devices' *CNET* (4 January 2019) <<https://www.cnet.com/news/amazon-has-sold-more-than-100-million-alexa-devices/>> accessed 28 January 2019

32 Lisa Eadicicco, 'Amazon Developing Advanced Voice-Recognition for Alexa' *Time* (27 February 2017) <<http://time.com/4683981/amazon-echo-voice-id-feature-2017/>> accessed 28 January 2019

33 Kari Paul, 'Google Workers Can Listen to What People Say to Its AI Home Devices' *The Guardian* (11 July 2019) <<https://www.theguardian.com/technology/2019/jul/11/google-home-assistant-listen-recordings-users-privacy>> accessed 18 August 2019

34 James Vlahos, 'Smart Talking: Are Our Devices Threatening Our Privacy?' *The Guardian* (26 March 2019) <<https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy>> accessed 18 August 2019

difficulty that a child age 12 or under in the parent's household could not reasonably ascertain the answers'.³⁵ Although such an approach could indeed reasonably distinguish adults from children aged 12 or lower and the procedure excels at respecting data protection principles by processing no data at all, the question arises if KBAs could be generalized for other ages: could any list of questions truly be devised that a 19 year-old is able to answer, but not a 17 year-old?

Another FTC-approved method is '*face match to verified photo identification*' (FMVPI). Photo identification is first submitted and analysed to ensure that an authentic document is used, followed by the prompt to take a picture of one's face, which is then compared to the ID photo through facial recognition technology. As noted by the FTC '[t]he proposed method does not involve checking the government-issued identification against databases of such information, but (...) does involve verification of the identification document to ensure its authenticity'.³⁶ FMVPI hence sidesteps data protection issues and shows great potential to carry out accurate and efficient age checks. A sore point is the inability to differentiate between age brackets of minors: in jurisdictions where they are not given identity documents, this method will prove inadequate to give them access to goods and services they are eligible for.

There is also room left for innovation with regards to *out-of-band methods*. These authentication solutions are primarily proposed by the US National Institute of Standards and Technology (NIST) and boil down to two-factor authentication, with the second verification taking place through a different communication channel than the first one. The NIST guidelines used to suggest using SMS messages, but – due to the ease with which they can be intercepted or redirected – the institute now recommends to instead work with out-of-band push notifications through a secure application.³⁷ This too forms a user-friendly and accurate method that processes a minimum of personal data.

Finally, *parental tools* (at least in their current form) should not be regarded as an adequate age verification technique. Although a sizeable portion of parents use parental tools³⁸ and some genuinely innovative applications and initiatives have been debated over the years – such as the UK alcohol standards body The Portman Group's recommendation to outfit age affirmation pages with a hidden 'Nanny

Tag' recognised by parental control software to automatically block a website³⁹ – research findings on the effectiveness of parental tools are very contradictory.⁴⁰

IV. Conclusion

Although there are currently five widely-employed methods to check the age of online users, all of them have several important downsides that must be taken into account. The pace of technological innovation and the ubiquity of personal data have resulted in an emerging market of innovative age verification ideas. The use of profiling is promising, although caution is warranted when children are concerned, while voice recognition might prove the next big technological evolution. These ideas can always be combined with the creative capacity verification mechanisms adopted under COPPA, as well as NIST's suggestion to use out-of-band push notifications through secure apps.

In the search for new, innovative solutions, it should also be considered that the level of verification must not necessarily be the same across all sectors, industries and businesses;⁴¹ instead, the amount and type of information requested during the process should be proportional to the perceived risk.⁴² This would mean that content, goods or services that carry less risk for minors should also impose less of an informational burden.

Technological innovation will undoubtedly prove key to finally 'cracking the code' and achieving accurate and efficient age verification measures that can

35 US Federal Trade Commission, RE: Imperium, LLC Proposed Verifiable Parental Consent Method Application (FTC Matter No. P135419) (2013) 3

36 Federal Trade Commission, RE: Jest8 Limited's (Trading As Riyo) Application for Approval of a Verifiable Parental Consent Method (2015) 2

37 US National Institute of Standards and Technology, NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management (2017), 18

38 Pew Research Center, Parents, Teens and Digital Monitoring (2016) 3

39 Portman Group, Responsible Marketing of Alcohol Drinks in Digital Media (2009) 4

40 Bieke Zaman & Marije Nouwen, Parental controls: advice for parents, researchers and industry (2016), <http://www.lse.ac.uk/media/lse/research/EUKidsOnline/Home.aspx> (last visited Oct 6, 2018)

41 *ibid* 114

42 n 1, 5; Article 29 Working Party, *ibid* 30, 26

be adopted on a large scale. The progress made since the debate last raged in the late 90s is remarkable, and the rise of AI and the ever-increasing output of

personal data in recent years can prove catalysts for another huge leap forward and a true 'coming-of-age' for age verification technology.