JUSTIN BRASCHER
NOAH WILSON
Assistant Attorneys General
Office of Attorney General Tim Griffin
323 Center Street, Suite 200
Little Rock, Arkansas, 722901
Telephone: (501) 503-4335

Counsel for Defendants

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

FAYETTEVILLE DIVISION

NETCHOICE, LLC, Plaintiff, v. TIM GRIFFIN, in his official capacity as Attorney General of Arkansas, Defendant.	**Declaration of Tony Allen** Civil Action No. 5:23-cv-05105-TLB

1. I am over the age of 18 and have personal knowledge of the facts set forth in this Declaration.

2. I am a Chartered Trading Standards Practitioner and Global Subject Matter Expert on Age Assurance Systems. I am the Technical Editor of ISO/IEC 27566 — "Information security, cybersecurity and privacy protection — Age assurance systems — Framework". I am the author of "The Law of Age Restricted Sales in England and Wales".

3. I am also the Founder and Executive Director of the Age Check Certification Scheme, the leading UK Accreditation Service approved auditor and technology testing service for the age

assurance industry. I am also an audit member of the Age Verification Providers Association (AVPA) – a global trade association representing the age assurance industry.

4. I have personal knowledge of the history, process, and logistics of online age assurance (as defined herein).

5. I have also been closely involved in the development of age assurance legislation in the United Kingdom and elsewhere in the world, including the United States of America.

6. I have reviewed the Social Media Safety Act (the Act"), the Plaintiffs' Memorandum in support of Motion for Preliminary Injunction and Complaint for Declaratory and Injunctive Relief with its supporting declarations.

7. Based on my knowledge and experience, modern technology is capable of allowing providers of content, goods and services on the Internet to verify the ages of their consumers without jeopardizing either the providers' or consumers' interests in both free speech and privacy.

8. Further, the burden upon both providers of Internet content, goods or services, in particular social media companies, and consumers in verifying age is minimal, and reducing as technology evolves ever further.

9. Based on my knowledge and experience, software filters on devices, when properly installed, can be a useful parental tool in protecting children from specific social media platforms, but in practice only provide a partial solution. They are less effective than, and not a substitute for, online age assurance.. Software filters on devices provide parents control over the access their children have to different services, but they may not be sufficiently granular to support controls on the content and functionality of social media that may be accessed by minors.

By giving parents discretion, they do not systematically enforce laws intended to prevent all children from being exposed to harmful content where that decision has been taken by legislators.

The availability of age assurance services and how they work.

10. "Age assurance" in the context of the Act and defined more fully herein is the process by which the provider of internet content that is harmful to minors ("Content Provider") verifies that the consumer of the content is age 18 or older.[1]

11. With the growth of social media platforms on the Internet, representative governments, including multiple states in the United States and many countries around the world, have looked for ways to protect children from harmful Internet content and functionality while simultaneously protecting rights of speech and privacy.

12. The UK Parliament expects to pass the Online Safety Bill in September. This requires "highly effective" age verification or age estimation to prevent children from being exposed to "Primary Priority Content" on social media and adult sites. This content is initially to be defined as relating to suicide, self-harm dieting and pornography. As when age verification was first developed at scale to prevent minors accessing adult websites, there remains a critical focus on designing a solution that protects the privacy and data security of users, because this

[1] The Act defines "reasonable age verification" as "means to confirm that a person seeking to access a social media platform is at least eighteen (18) years old]." One of the methods is "Any commercially reasonable age verification method." *See* ARKANSAS CODE 4-88-1102. As set forth herein, there are a number of tools that a third-party age verification servicer company may use to verify age. I will further define terms, including "age assurance," to distinguish among those tools.

latest Bill is focused on children's whose personal data is particularly sensitive. Maintaining the anonymity of children is a core design principle for the age verification sector

13. The European Union has implemented the General Data Protection Regulations ("GDPR"), a strict data protection regime requiring application of the principles of privacy-by-design and data minimization. This reinforces the need to devise a way to prove a user's age without disclosing their identity. Consistent with these objectives, the Act includes a requirement not to store personal data used for the purpose of age verification. "A commercial entity or third-party vendor shall not retain any identifying information of an individual after access to the social media platform has been granted." See ARKANSAS CODE §1104(a)

14. In light of the foregoing commercial and legal considerations, the most straightforward solution is to create trusted Third-Party Servicers who would carry out the age checks, and then pass on only the outcome of those checks to the sites a user wished to visit, in the form of "pass" or "fail". GDPR insists you only collect, process, and retain the data required for the specified purpose. So, where a Third-Party Servicer obtained a consumer's personal information in order to confirm a user's age, it then had no further need to retain that data, and could delete it forthwith, storing only a user's account name, their age, and some form of password.

15. Any question about whether a social media platform is compliant with an age restricting law requires only a simple and straightforward audit of the verification process, no individual records or personal identifying information is needed.

16. Content Providers are required under the Act to contract with third-party companies ("Third-Party Services") to perform the service for a fee. See ARKANSAS CODE §4-88-1102 (c)(1)

17. When using a Third-Party Servicer, a Content Provider directs the consumer to provide personal information directly to the Third-Party Servicer who performs the verification and informs the Content Provider only of the result of the check – "pass" or "fail." It does not pass back the personal information.

18. The Third-Party Servicer does not retain a consumer's personal information other than the necessary minimum information to meet the needs of the use-case (e.g. the date of birth, a record that the user is 18+, or that they are 13-17 years-old). This is only held pseudonymously, with future access controlled by the user so that the information can also be used to respond to subsequent enquiries about that user's age from other platforms. This approach would, in my opinion, be compatible with the requirements in the Act which states that "A commercial entity or third-party vendor shall not retain any identifying information of an individual after access to the social media platform has been granted."

19. The verification process need only be performed once per user and, as discussed further herein, the verification results for any individual user may be shared among social media platforms, thereby minimizing the need for multiple age verification checks of the same individual over, for example, a period of one year.

20. Age verification is not a new or rare technology. It is widely used by thousands of sellers and their consumers on a daily basis around the world in a variety of contexts such as

alcohol and tobacco sales, gambling, gaming and, to a growing extent around the world, accessing social media platforms.

21. Further, Third-Party Servicers continue to grow in number and improve the age verification technology. The Age Verification Providers Association began in 2018 with just six members. It now has twenty-six members and there are at least forty providers competing in the global market.

22. Age verification began in rudimentary style, perhaps with a faxed copy of a driver's license, but is now far more sophisticated, far less expensive, and employs robust safeguards for privacy concerns.

Categories and definitions

23. A number of methods have been developed, initially to verify age exactly, and more recently, to estimate it with an ever-increasing degree of accuracy.

24. Previous implementations of age assurance solutions, such as in Germany (100 age assurance methods have been approved by the German age regulatory body the KJM[2]) and France, where consumers are offered a range of methods from which to choose, showed consumers vary in their preferences of age verification method. A choice of methods, rather than a single one, led to greater adoption of the age assurance.

25. A choice of methods also addresses issues that arise from inclusivity, should any one method not be suitable for an individual. The broad choices that are available increase competition in the marketplace, reducing costs and economic barriers, improving creativity and

[2] https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme

innovation and offering users with considerably improved (or increasingly less burdensome) user journeys.

26. Although people sometimes use the following terms interchangeably, it is helpful to distinguish three related phrases:

(a) "Age assurance" is the process of establishing, determining, and/or confirming either age or an age range of a natural person.

There are then two categories of age assurance[3]:

(i) "Age estimation" is age determination performed using inherent features or behaviors related to a natural person (where age determination is an indication that a natural person is over or under a certain age or within age range).(ii) "Age verification" is age determination based on the validity of a credential that provides information that allows the criterion to be tested.

27. The "level of confidence" in any single or combination of age assurance methods is a product of (1) the strength of the evidence of age and (2) authenticating that this evidence relates to the user seeking to verify their age.

28. Age verification may be achieved by reference to, inter alia, drivers' licenses, passports, electoral rolls, credit reports, cell phone network records, banking, credit card records, membership of associations where this is only open to adults and access to a trusted email domain such as that of an employer for the retrieval of authentication codes. Users may also choose to create a reusable digital identity, and selectively release just their age attributes.

[3] The draft ISO 27566 – Age Assurance Systems – Framework, also mentions "age inference" as a category of age assurance, but that is not relevant to this particular case.

29. Liveness detection, face matching and document authenticity deployed alongside age verification serves to ensure that the correct, live person is presented as the user and that any documents are bona fide.

30. Age estimation, on the other hand, can be achieved by analyzing facial images, voiceprints, behaviors, usage or game play. The most established of these, facial estimation, can be accurate to within +/-1 to 1.5 years mean absolute error, according to the latest published data by one certified age assurance provider, Yoti Limited. (https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf). My own certification team has independently verified and validated the results of this testing by Yoti whereby the image is instantly deleted, bias and accuracy is published. Further independent benchmarking of facial age estimation error rates is commencing via the National Institute of Standards and Technology (NIST)[4].

31. The value of age estimation, as described more fully below, for both Content Providers and consumers is that personal information submitted, such as a face image shown to a camera, voice print presented to a microphone or other measures of behavior, usage or gameplay, can be used for the process of estimation and then instantly discarded. This significantly reduces the risks associated with gathering and retaining personal data.

Commercially reasonable age verification methods

[4] NIST is inviting developers to provide comments and suggestions by August 3, 2023 for this concept of operations and application programming interface (API) for the evaluation of facial age estimation.

32. There are a wide range of non-exclusive methods that Content Providers and Third-Party Servicers can adopt to assure the ages of their users to varying degrees of certainty. These methods used across the full range of situations where online age checks are required, and are permitted by the Act as "Any commercially reasonable age verification method" See Arkansas Code §1102(c)(2). They include, inter alia, the following;

Review of Government Issued Documents

33. A reliable, physical identity document can be reviewed and the age details noted. Users will typically submit an image of one or more of these documents using a smartphone camera. Technology, known as optical character recognition (OCR) reads the data from the document which is then validated based on known security features built into the form of ID used. The photo on the document can also be compared to a freshly taken photo or video of the user, which is known as 1:1 image matching and can be combined with a simultaneous "liveness" check.

34. For the highest levels of assurance Near Field Communication (NFC) technology can be used to allow a smartphone to read a microchip in the document where this is available, and the image map stored on the chip compared to a fresh photo or video of the user.

Review of Credit reports and other private sector databases

35. In this method, users usually enter their name, address, and date of birth (either specifically for the purposes of age verification or as part of their account opening or a purchase process for the website they wish to access), and a search is made of credit reports or other reliable databases to confirm the details are accurate and obtain or confirm the date of birth.

Often, this form of check is used where the user will need to be located at the address claimed as part of this process, to prevent users entering the information of other people, so it is well suited to the delivery of age-restricted goods.

Review of reusable digital identity apps

36. Digital identity apps or wallets are being certified in certain parts of the world, e.g., UK, Europe, Australia, Singapore - these approaches can enable citizens to share their over or underage status; via selective disclosure, in a data minimized way.

37. Where states have issued a digitized identification card, usually in the form of a mobile drivers' license, it may have been designed to allow the user to selectively share attributes such as age or an age qualification such as "18+, either directly with social media platforms or with a third-party vendor of age verification. I understand that such a card is under development for the State of Arkansas and once available this can be a further source of reliable age attributes for social media platforms and third-party age verification providers.

Submission of Credit Card number

38. In many countries, credit cards are only issued to adults, so the possession and the ability to use a credit card (not a debit or gift card) is a potential indicator that someone is 18 or over, but it is worth noting that this is not universal.

Review of bank records

39. Banks generally require a strong level of identification check to open an account, and keep a record of their customers' dates of birth. Some banks allow trusted third-parties to confirm a date of birth supplied to by the customer with those records. Typically, the user logs

into their own online banking system, and gives approval for the data to be supplied to the third-party, which in this case would be Third-Party Servicer.

Age estimation via facial, voice, or behavioral analysis

40. It is important to be clear from the outset that age *estimation* technology is not a *recognition* technology; it detects and assesses information, to give an age estimation. This is expanded on below with a particular focus on facial age estimation.

41. A number of features and characteristics of people change with age. This allows for them to be analyzed to estimate age. An example of this is facial features. When facial age estimation is applied, users are either prompted to share a properly authenticated (bound to the user) still image, video image, or an existing profile picture, and software then estimates their age. Systems learn how to do this by reviewing thousands of images of people with a known age to spot patterns common to those of the same age, and this means the technology is becoming better by the day. A live face is detected using liveness detection (as certified by International Standards) and then a pixel level review of the face is undertaken. The image generated by this method does not uniquely recognize any individual, but in any event can and should be instantly deleted. In addition, this form of technology is not trained with associated names or addresses.

42. As stated above, facial age estimation is often falsely conflated with facial recognition technologies. In fact, the facial estimation technique described here is quite distinct from facial recognition. No 1:1 image matching process takes place for the purpose of estimating age.

43. Facial recognition may separately be used to check that a user relying on a previous age check is still the same individual who completed the check, but that is a separate

process required for "authentication" rather than age estimation. Other estimation methods use voiceprints or analysis of how a user plays a computer game.

44. Presently, to meet a specific legal requirement for a person to be prevented from accessing material or services on the internet under a given age, increased confidence in the certainty of the age of a user of a site is possible by using systems that can be set with a "buffer" of an age level over and above the legally set age requirement. This approach will return a negative result if someone is estimated to be below the buffer age rather than below the legal threshold. The size of this buffer depends on the level of accuracy required by the Web service, or any regulatory requirements. International standards have been drafted to provide guidance on how to specify and measure the degree of accuracy, which would determine the size of the buffer age, which in turn determines with statistical certainty the number of false positives, and the distribution of those either side of the real age. For instance the KJM and FSM in Germany have approved the use of facial age estimation with a five year buffer.[5]

45. This method is inclusive of people of all ages, who do not own or have access to a government issued document.

46. Age Estimation by facial or voice technology is one tool in a toolbelt. For example, for a law that requires a user to be age 18 or older, such technology may be useful for assuring that individuals are, say, 21 years or older even if the Content Provider and Third-Party Servicer does not know their exact age. For those individuals, no further inquiry is needed. For those, however, whose facial or voice estimation results indicate an age range of under 21, then another Age Assurance method described herein may be used to confirm the exact age of the

[5] https://www.yoti.com/wp-content/uploads/FSM-seal-text_English_German.pdf

user. Outside the US, facial age estimation is already used within parental consent flows to ascertain if an adult is over the age of 25 to provide parental consent. This method is currently under review by the FTC Coppa.[6]

Age estimation via behavior and usage history analysis

47. This method involves a comprehensive analysis of whether an identifying feature, behavior or usage, such as an email address, has consistently and constantly been used over a period of time in multiple contexts, which when properly authenticated to a user, can be an indicator of the age of that user.

Physical Check

48. This is where a user is enrolled into an age assurance program in person.

49. They may be asked to produce a physical proof of age which is checked by a trained member of staff, or it could be left to the judgement of staff to decide if someone looks at least 35, for example, who then certifies the user to be over 21.

Vouching

50. This is where other people with credibility are able to confirm a user's age. They may be professionals, such as teachers or doctors. It is one of the most inclusive methods of age verification, as users do not need to have any documents or particular records.

51. You can only vouch for someone if all of the following statements apply:

i. you have an existing relationship with the user;

[6] https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-seeks-comment-new-parental-consent-mechanism-under-coppa

ii. *you are sure the user is who they say they are;*

iii. *you are in a position of authority in their community; and*

iv. *you have proved your own identity*

52. The Act allows for a wide range of the "reasonable age verification" methods described above, giving users a choice that suits their own circumstances and preferences, and ensures accessibility by not narrowly defining acceptable methods which could then exclude certain groups e.g., those without government-issued ID documents

Additional methods of age assurance not used by age verification providers

53. There are other methods of age assurance that may be less reliable than those previously discussed but may nevertheless be useful as tools in the verifiers' toolkit.

Social Proofing / algorithmic profiling

54. This is another software solution which assesses the likely age of a user based on their online behavior. Estimates are based on a user's online public profile and how they interact with an online service consistently over time – their interests, their friends, their school etc. Social proofing and algorithmic profiling cannot determine an exact age and has a wider margin for error and risk of evasion, so is considered to offer a lower level of assurance than some other more reliable methods discussed above.

Attestation / self-declaration

55. This is not considered a method that provides any assurance about the age, but can provide a starting point for the process, and in some cases where there is no risk in believing the answer given is accurate, it may still be fit-for-purpose. For example, if a child declares they

are a child under 13, then it may not be a problem to assume they are being truthful and prevent them from accessing social media platforms with no further verification – no harm no foul. There are, however, sometimes good reasons to ensure children accessing websites on the internet are really children; for example, to prevent adults impersonating children online, so a more rigorous method is required.

56. Self-declaration is simply asking users to check a box, or enter their age or date of birth – without any additional checking against other data sources.

57. Technical measures can improve reliability slightly – for example, allowing any year of birth to be entered, not only the year from before which the user would meet the site's minimum age requirement, or preventing users applying trial and error by repeatedly amending their age until they are admitted.

58. These weak methods of age assurance would not, on their own, achieve the level of accuracy required for robust age verification which satisfies the principal international standard for age checks. They can be used in combination with other age assurance techniques which is why they are included in this summary but on their own, they fall outside the scope of age assurance.

Accuracy of methods

59. Each of these age verification methods, alone or in combination, verify age to a different level of certainty.

60. Regulators, or a regulated business, can determine this "level of assurance." For example, regulators or regulated businesses might use different processes for social media

platforms from that required for alcohol sales, gambling, pornography access, and knife, gun or ammunitions purchases.

Re-usability

61. Businesses can offer their users a wide-range of privacy—preserving methods to estimate their age to a level of assurance that is proportionate to the level of risk presented by a site. Once an age verification check has been completed for one site, it is technically possible to re-use the outcome of that same check across any other website through a network that enables interoperability across websites through cooperation between their age verification technology suppliers. Regulators, standards bodies, or the interoperability networks themselves may place limits on the duration for re-use.

62. This approach means the technology exists now to ensure that the Act does not threaten the principle of navigating seamlessly between many social media platforms operated by unrelated entities. In effect, it asks users to take a small step, equivalent in the real world to wearing a seatbelt and using car seats, to protect children from online harm.

63. Historically, the AV industry realized around 2020 that users may be willing to help a site assure their age if they wish to open an account that will last them a lifetime, but for social media sites they are just visiting temporarily, this could quickly become inconvenient and expensive.

64. Recognizing this, the age verification industry has invested in delivering a mechanism that allows for the re-use of one age check across multiple websites.

65. The euCONSENT project, funded by the European Commission, was a successful proof of concept where 2,000 individuals from five countries visited three age-restricted websites

in turn, relying on a check completed at the first site to access the other two. The project is now being put into live operation in Europe, and a similar solution may be made available very rapidly in the United States as many states, including Arkansas, move to require age verification.

66. Users can choose to agree to accept a token on their device that merely indicates to websites they visit later that the user has already had their age verified, so these websites don't trouble the user again but instead ask the organization which did the first age check if this user meets their age condition. All this is done without sharing any identity details; nor is the user's age stored within the token to preserve their anonymity.

67. The age verification industry has developed reusable solutions and cooperated to develop and pilot interoperability so that age-assurance processes add little to no delay to a user's access to social media platforms, as their clients do not wish to drive any users away.

68. The convenience of interoperable and reusable age checks will avoid any problematic second-order effects. For example, this approach means that new websites and apps that users do not yet trust with their personal information need not ask them to provide it, as they will be able to rely on a check completed through a site that the user already trusts.

69. Figure 1 illustrates the typical process of independent, third-party age verification, and how users may choose to allow one age check to be re-used across multiple platforms either through the same AV Provider or across a network of AV providers through interoperability arrangements such as that developed by euCONSENT. It should be noted that each AV Provider has its own technical and business model, so this diagram illustrates the fundamental principles but specific processes are not common to every AV Provider.

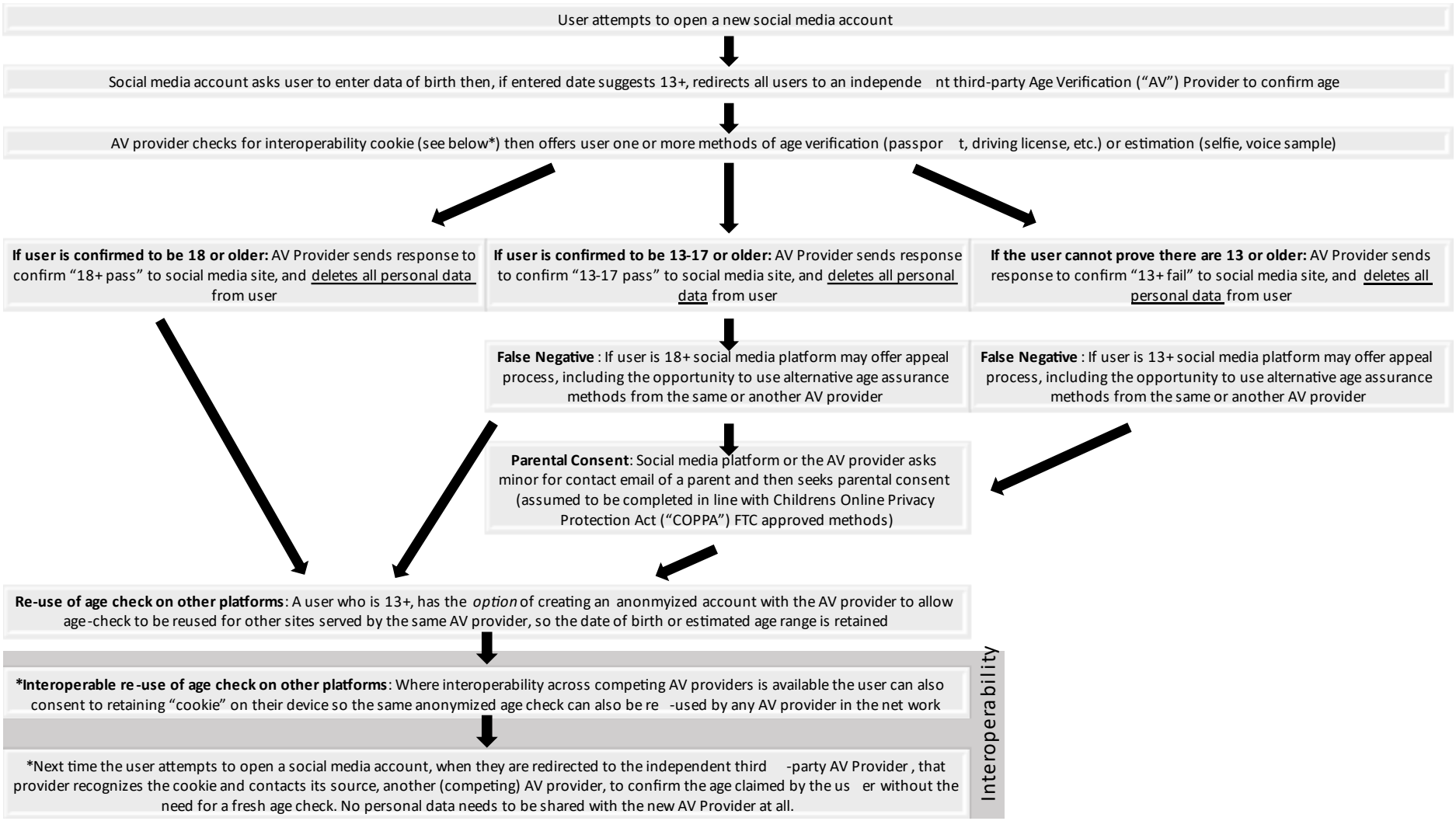

Figure 1 – How privacy-preserving, third-party age verification works, and the options for re-use and interoperability

The Cost of Age Verification

70. The leading sector requiring robust age verification was online gambling. As an industry with a strong return per customer, it tolerated relatively high costs per age check, perhaps as much as a dollar each. Naturally, as the Age Verification industry grew, competition put downward pressure on pricing, and it certainly halved relatively quickly.

71. Alongside competitive pressures, underlying costs were also falling. The earliest age verification methods almost all relied on accessing third-party databases such as credit reports for which there was a substantial cost per check. The more successful providers secured volume discounts but were still facing a high fixed cost base. Naturally, providers looked for cheaper ways to deliver their services, so they looked beyond credit reports to banking and telecoms where good quality data was available at a much lower cost, or even at no variable cost at all.

72. As a leader of an independent conformity assessment body, I cannot speak to the specific pricing offered by individual providers, but the UK Government recently published an Impact Assessment for the Online Safety Bill (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1061265/Online_Safety_Bill_impact_assessment.pdf) which estimates the cost per check to be twelve cents (converted from pence), with a caveat this cost is expected to continue to fall through innovation, competition and interoperability (Para 182, Page 44). I am aware of some providers who offer age verification at no cost to certain sectors as part of a wider digital identity service. This is particularly likely to be offered to the largest social media platforms in scope of

this Act, because of the opportunity for AV Providers to re-use those anonymized age checks with other platforms, either directly or through an interoperability network.

The security of data.

73. Age Assurance Providers who are members of AVPA and, thus sign up to its code of conduct, do not create new databases when conducting age checks for the social media companies. There are, of course, sectors such as online gambling where regulators require audit trails, but the Act requires, and indeed the industry's general practice is, *not* to retain any identifying information after an age check is completed. These audited providers do not create new databases of personal data, nor track the behavior of individuals online.

74. During age verification processes, Age Verification providers apply the same degree of security you would expect in financial transactions.

75. Specifically, age verification companies must act to protect personal data and demonstrate their adherence to this through various forms of certification (e.g., ISO 27001, SOC2, CyberEssentials, BSI PAS 1296, etc.) to ensure personal data is dealt with securely.

76. Age Verification providers share with a bank or healthcare provider the same risk of attacks during these interactions with consumers, but these risks are inherent to the Internet, not unique to age verification. However, it is worth noting that there is considerably less valuable data, if any data at all, that would be useful to a hacker being held by AV providers as opposed to that data held by banks or healthcare providers.

77. In addition to local laws, such as GDPR in the UK and EU, there is an industry-wide certification protocol, operated by government approved auditors, which tests providers against international standards. This not only assesses the efficacy of the age check, but also

data security and privacy measures. New standards are being developed by the IEEE and ISO which will ensure that age verification processes and procedures are kept up to date. Social media companies serving users in Arkansas may choose to use commercially available Age Verification providers certified by these conformity assessment bodies, not only to consolidate their defense against potential legal claims, but also to build consumer trust and confidence.

Adding the latest encryption techniques

78. In 2022, the French Data Protection Authority, published an article titled Online Age Verification: Balancing Privacy and the Protection of Minors, CNIL (Sept. 22, 2022), http://bit.ly/3EB1ISN [hereinafter CNIL Report].

79. The CNIL Report states:

> "The CNIL also recommends, more generally, the use of a trusted independent third-party to prevent the direct transmission of identifying data about the user to the site or application offering pornographic content. With its recommendations, the CNIL is pursuing the dual objective of preventing minors from viewing content that is inappropriate for their age, while minimizing the data collected on Internet users by the publishers of pornographic sites."
>
> "In order to preserve the trust between all of the stakeholders and a high level of data protection, the CNIL therefore recommends that sites subject to age verification requirements should not carry out age verification operations themselves but should rely on third-party solutions whose validity has been independently verified[7]."

[7] CNIL, Contrôle de l'âge pour l'accès aux sites pornographiques (Feb. 21, 2023), https://www.cnil.fr/fr/controle-de-lage-pour-lacces-aux-sites-pornographiques.

80. I am aware that the AVPA are engaging with CNIL to add more robust cryptographic protections into the age verification industry's standards, and to add them when agreed to the requirements placed on euCONSENT's participating providers when they are audited before joining the network, or any network mirroring this solution created elsewhere including in Arkansas.

Age Assurance around the world

81. The EU Better Internet for Kids Strategy mirrors the same desire as the Act: "Our vision is for age-appropriate digital services, with every child in Europe protected, empowered, and respected online, and no one left behind."

82. It is also worth looking at countries such as Germany, where over 100 age assurance approaches have been reviewed and approved by the KJM regulatory body (https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme). There is clearly a healthy eco system of age assurance approaches and methods and many global companies, including some of those association members of the Plaintiff, which are already deploying age assurance approaches in many parts of the world.

Effectiveness of other methods

83. Other methods exist to advance the goal of protecting children from harmful material on the internet, including parental controls and web filtering technology.

84. Parental controls themselves take a number of forms. They can be device based, applied to local routers in the home, or at the Internet Service Provider level. The last of these

perhaps offers the ability to limit parental discretion by making decisions on what to filter that cannot be overturned by parents. This is already widely applied to block Child Sexual Abuse Material (CSAM) for example.

85. But filtering applied in the home, on the router or on laptops, tablets, and smartphones through family cellular plans, is generally managed by parents. We know from repeated research by the UK's telecom's regulator, OFCOM, that many parents are unaware of this technology. Those aware of it often do not know how to use it, or discover their children also know how to use it or have circumvented it some other way. And finally, those who know about it and know how to use it, must still choose to use it, and to do so comprehensively enough to deliver the same level of protection for children as the Act intends. "Just over a quarter of parents used content filters provided by their broadband supplier, where the filters apply to all devices using that service (27%). A much larger proportion (61%) said they were aware of this feature, showing that not all parents are adopting this potentially useful control."[8] A survey of US parents by Kapersky in 2021 found just 50% used any kind of parental controls.[9] Children can be very persuasive, and parents might release the controls to allow them to play a game designed for 18+ within a social media platform, unaware the game or platform may be a portal to pornographic or other unsuitable content and dangerous functionality. Any social media site which a parent considers safe for their child under 13 can be added to a "Trusted List" of sites by a parent within

[8] (https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf)
[9] (https://usa.kaspersky.com/about/press-releases/2021_study-finds-50-of-parents-use-parental-control-apps)

the parental control software even though the state of Arkansas has legislated to prevent all children of that age group being exposed to this form of functionality and content.

86. I am aware that some social media platforms have instituted protections for minors, such as requiring users "to be at least 13 years old" or encouraging "teenagers… to use appropiate settings" or "age-gating to keep minors from seeing certain content", or banning "users under age 16 from "sending or receiving direct messages". But all of these must be prefaced with "Assuming the child does not lie about their age when opening an account…" Evidence shows that this is not a reliable assumption. "A third of children aged between 8 and 17 with a social media profile have an adult user age after signing up with a false date of birth", according to research commissioned by UK Internet regulator Ofcom[10]

What we've learned and what's changed in the last decade

87. The age-assurance methods discussed above do not necessarily add a new step to a user's visit to a new social media platform because through re-usability and interoperability, one age check can be used across multiple sites seamlessly.

88. The user need only complete the age-assurance process once before they can reach their subsequent objectives. For social media platforms where users create accounts, the users may only have to complete the age-assurance process one time. After that, the social media platform can store that the user is old enough to access it and authenticate the user when the user presents the login credentials associated with the account. Social media platforms that do not

[10] https://www.ofcom.org.uk/news-centre/2022/a-third-of-children-have-false-social-media-age-of-18#:~:text=A%20third%20of%20children%20aged,(PDF%2C%20992.6%20KB).

require that all users have accounts need not force their users to repeat age-assurance process each time the user tries to access the website or app because they can recognize when a user has previously completed an age check and rely on that check again.

89. The Act-mandated age-assurance need not require users to supply any private and sensitive information. For example, facial age estimation can be undertaken without any documentary evidence and either on a SAAS (software as a service) basis or entirely on a user's own device. The latter is offered by companies such as, Privately and Yoti.[11] There is already technology in use to detect injection attacks (where a fake computer-generated image replaces that from a webcam) and prevent spoofing. VerifyMyAge offer a solution based on a comprehensive analysis of usage of an email address, authenticated and demonstrably consistent over time, where the only identifying data the user need reveal is their email address.

90. The state of Louisiana shows examples of premium and free platforms to view adult content sites deploying age assurance technology, to comply with state laws. In each instance where AVPA members are supplying the service, the adult operator receives an anonymized over age (18+) attribute to allow access to adult content.

91. Age verification technology is clearly working at scale globally, with both small and global brands, where it does not put user privacy at greater risk or merit the other criticisms levelled by the Plaintiffs. The decision to complete the age-assurance process can be an inherently risk-free one for users—i.e., users can select methods that do not require them to disclose personal and sensitive information.

[11] *See* https://www.yoti.com/blog/safety-tech-challenge-fund-2021.

92. Since the Supreme Court ruled in *Ashcroft* and *Reno*, much has changed. Over the past 25 years, the age verification industry has developed a wider range of ways to verify age which offer users choice, including those who do not own or choose to use identity document-based approaches. They can choose, for example, age estimation techniques which do not require ownership or use of a document where the image, voice recording or email address is instantly deleted. Many hundreds of millions of age assurance checks are now undertaken globally each year. The cost has dropped dramatically, with reusability likely to lead to that trend continuing so there are no longer undue burdens on Web publishers due to the high costs of implementing age verification technologies. Nor would there necessarily be any significant loss of traffic resulting from the use of these technologies, except of course from children for whom the sites are unsuitable. The UK Government estimated in the Impact Assessment for legislation already approved by the House of Commons a cost per check of twelve cents and lower for high volume platforms, but noted cost may reduce further through interoperability and growing competition. The cost of that one 12 cent check may be defrayed across 100 websites before it might need to be repeated to maintain the ongoing integrity of the age verification ecosystem, and that is only if businesses determine that periodic re-validation is prudent.

93. Concerns about anonymity have also been addressed by developing age verification technology. The age verification sector was created specifically to enable users to access the sites they wished to access through the data minimized sharing of age. By selecting a trusted third-party, as required by the Act, even when selective disclosure from full identity document or digital identity wallet is used to prove age, the provider then only confirms "yes" or "no" when a website enquires "is this user an adult?" In Europe, users are given further

reassurance by the enforcement of the General Data Protection Regulations (GDPR) but in the United States, contractual commitments to maintain secrecy and the threat of civil damages claims if that is not applied offer similar protection.

94. And, of course, users may choose any of many other methods to prove their age, including facial age estimation or email address analysis where neither credit card numbers nor any personal data is required. Also, Age assurance standards allow for vouching where a user with no documentary proof of age can ask a respected member of their community such as a teacher or doctor to confirm their age.

95. Whether or not privacy laws apply, globally AVPA members must adhere to a Code of Conduct[12] that requires privacy and data security.

96. The Act's age-assurance provision imposes some minimal implementation costs on regulated businesses with zero to minimal lag when a user first accesses an age restricted website – and perhaps say annually to revalidate their check.

Conclusion

97. The Act does not radically change the Internet's architecture, it merely makes it age-aware. It does not require users to share their full identity to go online and engage in constitutionally protected activities. Any privacy and security risks faced by both adults and children can be managed to the extent consumers demand – to the point with certain methods where there is no greater possibility of breaching either their privacy or security than already exists today when using the Internet generally. The Act does not jeopardize First Amendment

[12] https://avpassociation.com/membership/avpa-code-of-conduct/

principles but applies the same principles for child protection we have in the real world to the growing online metaverse and should protect children from harm when taking advantage of the many benefits offered by the Internet.

DECLARATION UNDER PENALTY OF PERJURY

98. Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury that the above statements are true and based upon my personal knowledge.

Tony Allen

/s/_____
Tony Allen, Subject Matter Expert