# Are you over 18?

# A Snapshot of Current Age Verification Mechanisms

Chelsea Jarvie[1]
Karen Renaud[1,2,3]

[1]University of Strathclyde, Glasgow, UK
[2]Rhodes University, Grahamstown, South Africa
[3]University of South Africa, Pretoria, South Africa

karen.renaud@strath.ac.uk (Corresponding Author)

*Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, San Antonio, Texas, USA*

# ARE YOU OVER 18? A SNAPSHOT OF CURRENT AGE VERIFICATION MECHANISMS

**Chelsea Jarvie**[1], **Karen Renaud**[1,2,3]
[1]University of Strathclyde, Glasgow, UK
[2]Rhodes University, Grahamstown, Pretoria, South Africa
[3]University of South Africa, South Africa
chelsea.jarvie@strath.ac.uk, karen.renaud@strath.ac.uk

**ABSTRACT**

There are many online spaces that children should not enter to shield them from adult content, services and products. Age verification mechanisms are used to bar entry to minors. We examine the arguments for and against their use, and propose three dimensions that these kinds of mechanisms ought to judged by: (1) effectiveness & inclusivity, (2) affordability, and (3) privacy preservation. We used a systematic literature review to provide a snapshot of age verification practice in the research literature and commercial arena. We found a wide range of age verification mechanisms, ranging from "verification theatre" (box checking to confirm adulthood) to those that verify age by confirming identity. The latter elicit significant security and privacy concerns while the former clearly constitute no obstacle at all. Some mechanisms use facial biometrics to estimate age (for a fee), but the costs can easily become prohibitive for small businesses. We suggest directions for future research into solutions that can provide a more effective and affordable solution, which crucially also respect the privacy of users.

## 1 Introduction

Online safety for children is a mounting concern with more services for children, including education, being delivered online. One in three Internet users were children in 2015 [43], and during the pandemic era this percentage has surely increased with children spending far more time online since the beginning of the pandemic [24, 76].

Professor Byron [11] explains that online harms to children can be categorised into one of the three C's: (1) Content, (2) Conduct and (3) Contact.

*Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, San Antonio, Texas, USA*

With respect to *content*, a report published in 2016, by the National Society for the Prevention of Cruelty to Children (NSPCC), The Children's Commission and Middlesex University highlighted long-term concerns related to children's development if exposed to adult content online [45].

With respect to *conduct*, Thompson [75] explains how teens can engage in risky conduct online, to their detriment. Sexting, too, is a rising trend [70], with possible tragic consequences [26]. Children are also increasingly exposed to online abuse or cyber bullying [52].

With respect to *contact*, there is an obvious need to protect children from online predators [88, 52].

Given that the online environment is beset with dangers to underage users, there is a growing need and demand for effective online age verification methods to protect children from viewing inappropriate content and to protect vendors from inadvertently selling adult products to minors, and facing legal consequences. Although there are robust physical controls to prevent children from accessing offline adult content or purchasing adult products, such as alcohol and tobacco, equivalent online controls might well still be immature and ineffective.

Different countries impose a range of legal age restrictions for 'adult' activities. For example, in the UK, you have to be 18 to drink alcohol, but in the USA. drinkers have to be 21[1]. The legal age for smoking also ranges from 16 (Zambia) to 18 (most of the world) to 21 (USA)[2].

The *conduct* and *contact* risks are best managed by non-technical mentoring and monitoring measures implemented by parents and teachers [62]. With respect to *content*, there is a distinct possibility that children might access adult-only content [25, 27], and reliable age verification mechanisms could prevent this.

Perlroth [57] explains that while it may seem a simple matter to verify the age of Internet users, it is actually very challenging to do this accurately. The last review of the available online age verification mechanisms was published in 2015 [61]. Given that five years have passed, we performed a systematic literature review to assess the state of play related to age verification. We surveyed the research and grey literature to reveal the full range of online age verification mechanisms. We discovered that age verification practice ranges from non-existent or light touch (checkbox to confirm age) to highly privacy invasive. There exists a substantial gap for an effective, affordable and privacy-preserving online age verification solution [61].

In Section 2, we review arguments for and against the use of age verification mechanisms, and suggest three dimensions that age verification mechanisms should possess. In Section 3, we detail the research methodology. Section 4 reports on the results of the analysis. Section 5 suggests future research, with Section 6 discussing, reflecting and acknowledging limitations. Section 7 concludes.

[1] `https://en.wikipedia.org/wiki/Legal_drinking_age`
[2] `https://en.wikipedia.org/wiki/Smoking_age`

## 2 Background

The UK Government's efforts to tackle the issue of children accessing adult content started with the Digital Economy Bill which received Royal Assent in 2017, making it the Digital Economy Act 2017 [28]. Part 3 of the Act focused on Age Verification for online pornography and measures were due to come into force from 15th July 2019. However, it was delayed and the act subsequently dropped in 2019, with the Government promising that other measures would be put in place [6].

In 2021, the UK Government released a new bill, The Online Safety Bill, which has no reference to online age verification for pornography sites [30]. This came as a surprise to children's safety groups and the commercial pornography industry who had been expecting and preparing for an age verification requirement [6]. The Government has come under fire from groups supporting age verification for access to adult content and recently lawyers began proceedings against the UK Government, claiming they have failed to stop children watching online pornography [72].

The oft-mentioned justification for age verification is to control access to online pornography [29, 74]. However, there remains a gap when it comes to online sales of alcohol and tobacco products worldwide. In a recent survey, Gaiha *et al.* found that more youths had moved to buying e-cigarette products online while shops were closed during the COVID-19 pandemic in the USA. Over a quarter were not asked to verify their age [25].

In a study by Wood [89] into youths purchasing e-cigarette products online in Australia, he found that 50% of vendors audited had no age verification process, and the remaining 50% required the user to confirm they were over 18 or input their age or date of birth. Similarly, Williams *et al.* [87] investigated online alcohol sales in the USA. They reported that only 39% of attempted online transactions by minors failed due to age verification mechanisms detecting them. A similar study by Colbert *et al.* [12] found that in Australia, of the alcohol vendors chosen, ineffective online age verification methods were used. 49% asked the users for their dates of birth and 27% utilised a tick box method.

Schiff *et al.* [67] found that in of the youths surveyed in Los Angeles, California, few experienced age verification barriers when trying to purchase e-cigarette products online. When it came to verifying the minors age on delivery of the product, Schiff *et al.* discovered that minors were circumventing the control by having their tobacco products delivered to an older friends house.

Age verification for online sales is a global issue and in 2021, the UK Government published a call for proposals for innovators to develop a way to fulfil the requirement for online age verification on alcohol sales, given that they have to comply with the Licensing Act 2003 [31].

In addition to the work being done by the UK Government, in 2020 the Information Commissioner's Office published the Children's Code [54]. The code contains 15 standards that must be complied with when designing online services that are likely to be accessed by children under the age of 18. It is worth noting that the code still applies to online services that may not be aimed at children and one of the standards concerns age assurance [54].

Social media services are significantly used by children with most sites requiring users to be at least 13 years of age [79] but age verification has proved a challenge. Consider TikTok, which in recent years has tried a range of methods. Some have been privacy invasive and others light touch and ineffective. In 2019, TikTok made multiple changes after violating the Children's Online Privacy Protection Act (COPPA), which resulted in many accounts which they believed belonged to underage users being blocked or deleted. Customers had to send a copy of their government ID to get their account back [17]. In January 2021, TikTok came under fire again and was ordered by the country's data protection agency to recheck the age of every user in Italy [71]. To achieve this, TikTok asked customers to re-enter their date of birth, and anyone who was under 13 years of age was removed from the app. This is an easy verification process to circumvent and significantly different to the approach taken in 2019. This demonstrates, once again, the need across multiple industries for effective, inclusive, affordable and privacy-preserving online age verification.

We first present the arguments *for* (Section 2.1) and *against* (Section 2.2) the deployment of online age verification mechanisms. We then suggest three dimensions that such mechanisms ought to possess (Section 2.3).

### 2.1 Arguments *for* age verification

The 2016 study by the NSPCC, The Children's Commission and Middlesex University found that by age 16, 65% of children had seen online pornography and that a higher number of boys than girls wanted to emulate what they had seen. This, in turn, made girls feel more worried about the impact pornography had on boys' attitudes to sex and relationships [45, 14]. Adolescents who access inappropriate adult content can have their perceptions of women permanently skewed [58] and experience negative emotional, psychological, and physical health outcomes [58, 60]. Moreover, two murders by a British 15 year old were attributed at least partly to his addiction to violent pornography [51].

Parents are concerned [55] and engage in a number of strategies to protect their children [53], but their influence is limited when children access the Internet from public WiFi and devices that their parents cannot control.

### 2.2 Arguments *against* age verification

Similar to Yar [91], Blake [7] is sceptical of introducing age verification for pornography sites, believing that this control will do more harm than good. Blake argues that statistics used by the UK Government related to online pornography causing harm to children is "cherrypicked". Blake states that there is no evidence that young people are harmed by seeing sexual images and that the main under-18 users of pornography are 16 and 17 year-old's who are above the age of sexual consent anyway. Introducing age verification, Blake believes, may actually expose children to a greater risk because they might turn to the dark web to circumvent the restrictions to access these services, and be at much greater risk in this completely unregulated domain.

### 2.3 Age Verification Solution Dimensions

The previous two sections presented arguments both for and against the use of age verification mechanisms to control access to adult-only online spaces. The arguments *for* their use appear more compelling than those of the detractors,

especially since governments might well mandate their use in the future [6]. If we *do* develop age verification solutions, what should their characteristics be?

Based on the literature, the ideal age verification mechanism should demonstrate the following dimensions (Figure 1):

**(1) Effective & Inclusive:** No tool will be infallible, but the probability with which a mechanism is able to identify children should be commensurate with the sensitivity of the content and the damage such access can do to children. This can prevent children from being harmed by inappropriate content. Moreover, a solution should not exclude any population group either due to minority status or limited financial resources. This aligns with the ISO accessibility standard [36], which aims at "*making products, systems, services, environments and facilities more accessible to more people in more diverse contexts of use*". We combine effectiveness with inclusivity because a these two aspects are inter-dependent.

**(2) Affordable:** In other domains, there is a strong link between affordability and adoption [68, 42, 69]. Hence, if governments mandate age verification for online vendors selling adult products, or providing adult content, it is essential for such mechanisms to be affordable, even for small businesses. Paying per transaction is likely to reduce small businesses' already small profit margins.

**(3) Privacy Preserving:** Renaud and Maguire [61] argue that age verification ought not to collect any personally identifiable information, to ensure that people are not blackmailed or sextorted by unscrupulous vendors. The Ashley Madison case amply demonstrates the consequences if such sensitive information leaks [3].

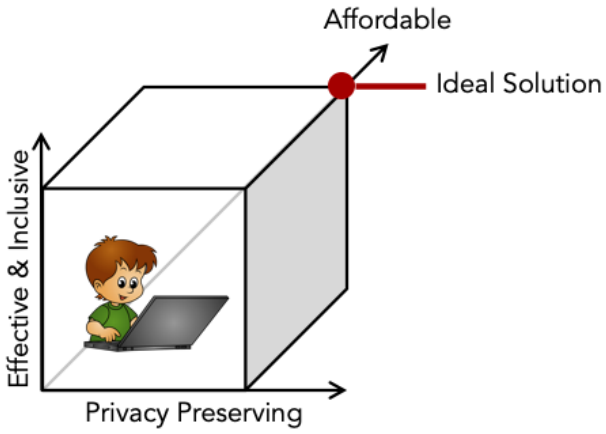


Figure 1: Age Verification Mechanism Dimensions

## 3 Research Methodology

### 3.1 Research Questions

The aim of this paper is to explore the current academic and industry position regarding online age verification, and to suggest directions for future innovative research in this space. This paper will explore the following research questions, which will inform the analysis process:

**Research Question 1 (RQ1):** *To what extent do online age verification solutions exhibit the three primary dimensions enumerated in Section 2.3?*

**Research Question 2 (RQ2):** *What other mechanisms could potentially be used to effect age verification?*

### 3.2 Systematic Literature Review

A systematic literature review was carried out to ascertain the extent to which current research could answer the two research questions posed in this paper. Our aim, in doing this research, was to reveal the state of play (RQ1) but also to determine whether the growing area of body language based deception detection [34, 64, 32] was, or could be, used to support online age verification (RQ2).

A variety of databases were used to gather relevant research including; Scopus, EBSCO, Web of Science and ProQuest, in addition to Google search engine for grey literature. Material was collected for the years between 2011 and 2021. Finally, we used an Artificial Intelligence (AI) powered tool called IRIS.AI to find any additional texts that may have been missed in previous searches. The methodology used is the approach proposed by [40] and is depicted in Figure 2.

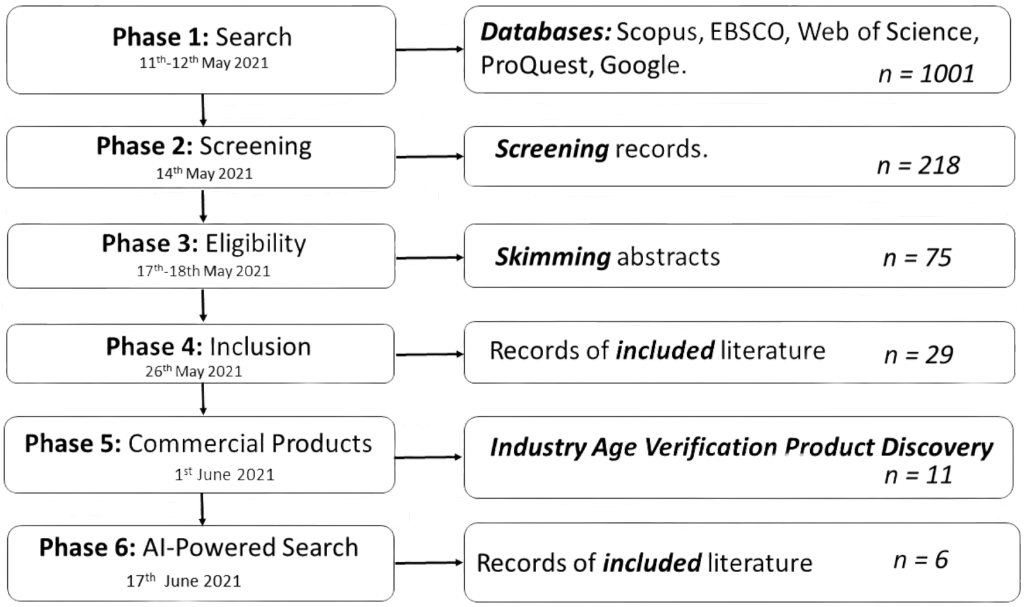


Figure 2: PRISMA of Systematic Literature Review [40]

**Phase 1 - Identification:** A total of 1001 resources were found from the databases listed using the keywords: "Cyber safety" or "online safety" and "children", "online age verification", "machine learning" and "lie detection", "online" AND "deception detection" AND "body language".

**Phase 2 - Screening:** After initial screening, it was found that 78% of the results were not relevant due to being out of scope or context. There were a considerable number of papers rejected regarding teaching children how to be safe online, cyber bullying and parental controls as these topics are not within the scope of this project. Similarly, where deception detection was based on physical measurements, papers were rejected.

**Phase 3 - Eligibility:** After reviewing the abstracts of the remaining 218 papers, 75 were retained.

**Phase 4 - Inclusion:** The remaining papers were fully structured and reviewed. The final review process eliminated all but 29 papers.

**Phase 5 - Commercial Products:** An extensive search was carried out using a search engine and the Keywords 'online age verification for businesses','online age verification' to identify as many commercial products as possible.

**Phase 6 - AI-Powered Search:** We finalised our search by using an AI powered tool called IRIS.AI. We provided it with the abstract for this paper, as well as the title: '*Age Verification Deception Detection*'. It returned 118 papers, with a graph as shown in Figure 3. We worked through each paper returned by this search to identify its relevance. A total of 6 papers were added to our original corpus. Table 1 provides the tallies of papers found in each database.

Table 1: Databases and numbers of papers found

| Database | # Papers | After Exclusion |
|---|---|---|
| EBSCO | 36 | 0 |
| Scopus | 224 | 15 |
| Web of Science | 9 | 0 |
| ProQuest | 732 | 14 |
| IRIS.AI | 118 | 6 |
| Total Analysed | 1119 | 35 |

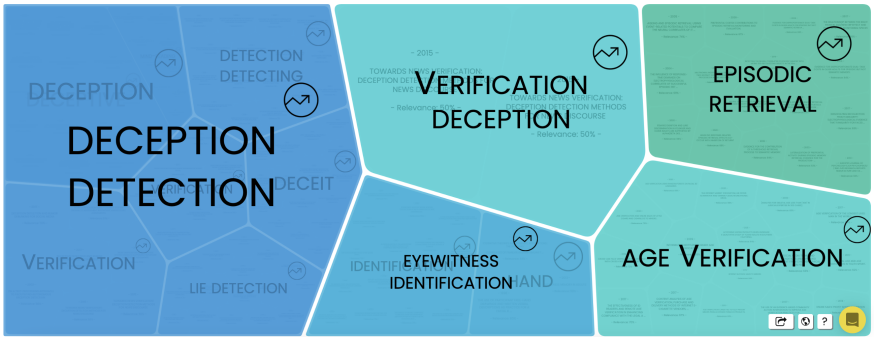


Figure 3: Result of AI-Powered Search

## 4 Findings

### 4.1 Current Processes

Although there is a push for effective online age verification, and online age verification solutions *do* exist, they vary significantly from "verification theatre" (check this box to confirm you're over 18) to highly privacy invasive (provide a copy of your passport).

Williams *et al.* [86] found the most common age verification methods used by online tobacco vendors was a checkbox asking the online user to confirm they were over 18; only accepting credit card payments, or telling them that by submitting an order, the user is implicitly verifying they were over 18. Similar methods were used by online alcohol vendors [87, 84, 12]. Moreover, Williams *et al.* identified issues throughout the adult product supply chain. Delivery companies were found to leave alcohol and tobacco packages unattended or gave them to youths without verifying ID [85, 12].

A small study by Williams *et al.* [85] revealed that, of 10 minors who tried to buy e-cigarettes online, none failed due to a working age verification process. In fact, they found that 46% of vendors used a tick box to confirm adulthood, 19% had no age verification at all and the final 35% had a strategy which failed in its core purpose in this study. In a larger study into alcohol sales carried out by Williams *et al.* into 100 alcohol orders placed by youths, only 39 failed due to age verification, with 51% of vendors having a tick box and 41% deploying no age verification solution [87]. A similar study by Colbert *et al.* [12] found that selected Australian alcohol vendors, 49% asked for a date of birth and 27% utilised the tick box method.

In summary, the most common age verification process demonstrated in these studies is the tick box, which cannot possibly be effective in preventing youths buying or accessing adult products and services. This method is essentially "verification theatre" (Figure 4). The only consideration recommending it is that it is privacy preserving. However, the balance between effective age verification and privacy is not achieved by using a tick box mechanism. Google's age verification mechanism, as shown in Figure 5, demonstrates an underlying assumption that: (1) children cannot get hold of credit cards, and (2) children cannot gain access to their parents' identity documents. Both of these are unfounded.

### 4.2 Commercial Products

Preventing children from accessing adult products, services and content online is a challenge which is highly debated politically and comes with a huge host of technical challenges. There is a small selection of commercial age verification solutions that vendors can pay for.

The available commercial products utilise a variety of methods to verify a user's age. The predominant methods use database checks or photos of the user that use AI to determine whether the user is underage or not.

Yoti uses AI to determine the user's age from a picture and also offer a digital ID scheme whereby a user uploads a government document and is provided with a QR code which can be used by vendors to prove ID. Yoti's age

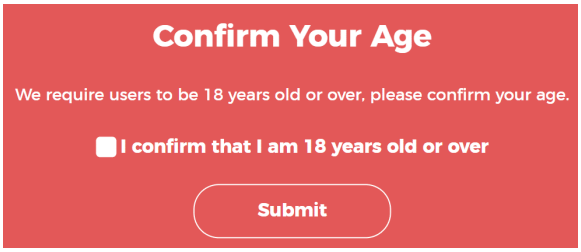


Figure 4: "Verification Theatre" Tick Box

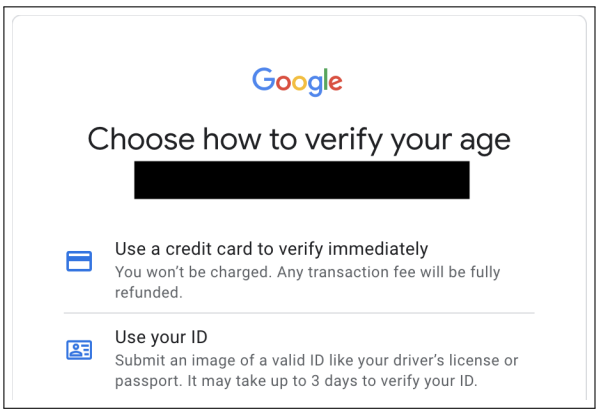


Figure 5: Google's Age Verification

verification product is the only one to be certified by the new Age Verification Regulator under the British Board of Film Classification (BBFC) age verification scheme [92]. Similar to Yoti, VerifyMyAge uses AI to estimate the age of the user [80] while AgeChecker.net and Jumio require a user to upload a selfie with their Government issued ID. AI is then utilised to determine the age of the user [37, 2].

Where some vendors accept credit cards only as a means of age verification, VeriMe allows age verification of customers who want to use a debit card [81]. This is achieved via vendors obtaining debit card information while VeriMe checks that the user's mobile number is registered to an adult over 18. AgeChecker.net, AgeChecked and VerifyMyAge also utilise a mobile number as a means of age verification [80, 2, 1]. Equifax, Experien and Trulioo rely on third-party database checks for age verification [19, 19, 78]. AgeChecked are the only vendor who claim to be able to do age verification through social media, but it is unclear how this method works in practice, and whether it is GDPR compliant. They also offer several other methods of verification [1]. Tencent [8] uses facial recognition to prevent children from entering their gaming platform.

Some commercial products estimate the age of a user from a facial biometric. Four of the most popular tools were tested by Jung *et al.* [38]. They found that none performed well when it came to age determination using a static image, making them unsuitable for online age verification. Yoti claims to have a 0.08% error rate and a Mean Absolute Error of 2.09 years [93]. Table 2 shows the range of commercial products in this space. Please note that only Business-to-Business commercial solutions which are available to purchase have been included in this table. Non-commercial age verification processes, such as the ones shown in Figures 4 and 5, are not included. Age verification, similar to authentication, also relies on: 'what you know', 'what you are', 'what you hold' and combinations of these. Because none of the commercial solutions utilize the first option, we have included a research-based solution (which was tested with over a thousand children) for the sake of completeness. This mechanism preserves privacy and is affordable, but is not effective because, while it could detect children, it also mis-classified a large percentage of adults.

We can now explain how solution types could be ranked on each of the three dimensions:

Table 2: Age Verification Products (details based on website check in June 2021)

| Solution | Checks | Price |
|---|---|---|
| **WHAT YOU KNOW** | | |
| Renaud and Maguire [61] | Knowledge and ability to identify photos of historical figures | N/A |
| **WHAT YOU ARE** | | |
| Yoti [92] | Picture (AI) | 25p per verification |
| Verify my Age [80] | Video (AI) | 45p per verification (eBay) |
| **WHAT YOU HOLD** | | |
| Yoti [92] | Government ID | 25p per verification |
| | Phone Number | |
| Verify my Age [80] | Third Party Database Check | 45p per verification |
| | Government ID | |
| | Credit Card Check | |
| | Phone Check | |
| VeriMe [81] | Phone Number Check (if using debit card) | Unknown |
| AgeChecker [2] | Third Party Database Check | $25 per month plus 50 cents per verified user |
| | Phone Number Check | |
| AgeChecked [1] | Driving Licence | Unknown |
| | Phone Number Check | |
| | Social Media | |
| | Payment Card | |
| | Address Search | |
| Trullioo [78] | Government ID | Unknown |
| | Third Party Database Check | |
| Melissa [46] | Address Check | Unknown |
| Equifax [19] | Third Party Database Check | Unknown |
| Experian [20] | Third Party Database Check | Unknown |
| **WHAT YOU HOLD & ARE** | | |
| AgeChecker [2] | Selfie with ID (AI) | $25 per month plus 50 cents per verified user |
| Jumio [37] | Selfie with ID (AI) | Unknown |
| Tencent [8] | ID Card + Facial Recognition | Unknown |

- **Effective & Inclusive:** While many age verification suppliers claim efficacy, children are likely to try a variety of ways of fooling them. For example, we used the online demo of one of the AI powered facial biometric mechanisms to test its efficacy (We do not identify this supplier because we have not been able to contact them to report this). It performed well with three adults in the over 25 age group. However, when we put a dog in front of the person's face, it estimated the age as 42-45 (see Figure 6 - we replicated this with a different dog). We contacted the company to tell them about this apparent vulnerability. They responded as follows: *We welcome and appreciate people helping us make our technology even better. Our age estimation AI simply looks at an image presented to it and provides an estimate in near real-time. While our demos will always provide a secure transfer of data, many don't have additional anti-spoofing layers. However, when Yoti's age estimation is implemented in real-world and online scenarios, we use a range of anti-spoofing techniques including face detection and liveness that prevent attempted attacks to trick the system. e.g. https://yoti.world/liveness*.

  Other mechanisms do a database lookup but a teenager could easily use a parent's name, or might even be named after a parent, impacting efficacy. A test for the person the phone is registered with might also turn up a false positive if the teenager's phone is registered in the parent's name. Government ID will indeed prove

age, but this either has to be scrutinised by a human so will also involve additional staff costs and processing delays, or by the use of pay-per-use AI techniques. Moreover, these techniques violate the user's privacy.

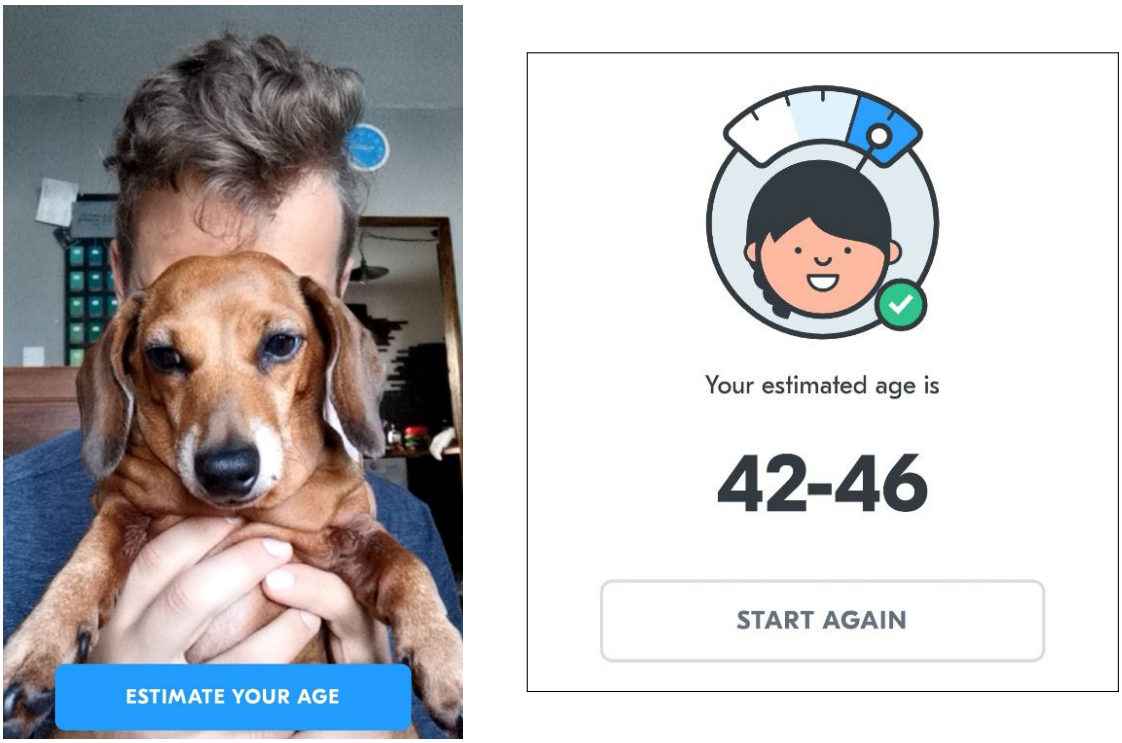


Figure 6: Fooling an Age Verification Mechanism with Ellie the dachshund

In addition to efficacy concerns, both Yar and Blake highlight the fact that age verification solutions using credit cards, passports or driving licenses exclude the economically disadvantaged [91, 7]. Those who either cannot gain access to a credit card due to limited financial resources, or those who choose not to have a credit card, will be excluded from accessing these services unless an alternative method of age verification is supported. The 2011 UK census shows that 24% of UK nationals do not have a passport and 15% do not have a driving licence [73]. Entering credit card, passport or driving license information into an adult-only website might also deter some privacy and security conscious adult users from accessing online services. The legitimate businesses trying to sell these products will suffer economically.

- **Affordable:** One of the main issues related to current commercial age verification products that could render them unsuitable is the cost to vendors. With people having to pay for each verification, costs could quickly become commercially infeasible for vendors selling low-cost products, such as beer or cigarettes. A number of online databases allow address lookup to confirm provided details, but the UK databases require payment (e.g., Royal Mail, the Electoral Roll and 192.com). Other countries probably have similar online services that offer lookups for a fee.

  Hence, for low value online services providing adult content or products, the current solutions' pricing models i.e., per verification, might well be unworkable for small and boutique businesses.

- **Privacy Respecting:** For adults looking to access online adult services or content discreetly and lawfully, entering credit card information, passport or driving license details or having their picture taken, are all privacy invasive. This is undesirable and risky.

  Yar [91] highlights the impact of the 2015 Ashley Madison breach and the concern that age verification providers might be targeted due to the sensitive and compromising information they may hold on users who have been verified through their service. Recently the rise in "extortionware" has seen people being targeted by hackers who have sought out sensitive information to extort money from them in return for ensuring the information is not leaked. This happened to an IT Director of a US company whose systems were infected with ransomware by a hacking group. In the process, hackers found a pornography collection on the IT Director's work device and posted a blog naming the Director and exposing their findings. The company did not respond to requests for comment and the blog post was removed by the hacking group, potentially implying that the ransom was paid [50].

### 4.3 Privacy Invasiveness

Very few of the commercial mechanisms preserve their users' privacy. These mechanisms use third party identity authentication mechanisms as a proxy for age verification. This is an overkill solution, which works very well for the vendors in terms of covering them from a legal perspective. Yet the user has to sacrifice their own privacy to use the service. The Ashley Madison breach made it clear what the fallout could be if usage of particular websites is leaked [4]. Ashley Madison facilitated adultery, which is not illegal, but many people consider such activities to be unacceptable and/or immoral.

Consider how age verification is achieved in the physical world. A person can walk into a bar and order a drink without identifying themselves, as long as they look old enough. If the vendor is unsure, they might ask to see proof, but no record is taken of such proof. On the Internet, it is hard to guarantee that identity documents will not be stored and potentially abused. This is why it is so important for people to be able to use adult-only services without risking identity theft or embarrassment. Moreover, children's identity data has to be protected even more than that of adults, even if they are potentially trying to access adult-only content (e.g. COPPA legislation in the USA [22] and GDPR in the European Union [35]).

### 4.4 Summary

Our review revealed that the majority of available age verification solutions are privacy-invasive, bringing the European Union's GDPR regulations and cyber security concerns into the picture, for both users and vendors. Information regarding a person's sex life or sexual orientation is classed as special category of data under the EU's GDPR regulation. This information could easily be revealed based on the websites people choose to use. Similarly, the California Privacy Rights Act (CPRA) 2020 defines government identifiers, sex life and sexual orientation as sensitive personal information

[82]. The sensitive nature of data that is potentially inferred or collected requires additional safeguards and security controls to protect it [35].

For any vendor buying a third-party age verification solution, there is a high level of due diligence required to ensure that the supply chain could not adversely impact their business. Biometric mechanisms are not privacy invasive when used to prove age and not to identify an individual but turn out not to be infallible, as we demonstrate.

## 5 Alternative Mechanisms

There is a clear requirement for more technical options to satisfy online age verification requirements, while preserving privacy. Combining the areas of age verification and deception detection may be a novel way of producing a privacy-preserving mechanism for verifying a user's age. By being able to detect, with a dependable accuracy, whether a user is deceitfully trying to access an adult service or buy an adult product, it could be judged with a high level of probability that the applicant is under 18.

### 5.1 Deception Detection

Deception detection techniques have been utilised for many years using a variety of physical cues and tools, such as lie-detector machines. It is claimed that an average person can detect deception with 54% accuracy while trained groups such as psychologists or interrogators, show approximately 60% accuracy [90]. The study of detection deception has moved on with the introduction of AI and the ability to detect deceit virtually rather than physically. Some of the techniques researched for detecting deception online include micro-expressions 'read' via the camera, pupil dilation, keyboard dynamics and mouse dynamics, all of which have varying degrees of accuracy[77, 48, 9, 47, 49].

The topic of deception detection is well researched and thoroughly critiqued. However, there is a lack of research with regards to detecting deception in children. There is also no evidence to suggest that deception detection has been used as a method for verifying age online.

### 5.2 Facial Cues

The most researched deception technique is the analysis of micro-expressions, which is based on the theories of psychologist Paul Ekman [15]. Micro-expressions are split-second facial cues which indicate emotional leakage and can be evidence of a concealed emotion [59]. Psychologists, investigators, and interrogators are turning to micro-expressions to detect whether someone is being deceitful, even marketeers are using facial expressions to enhance their market research [44, 21]. Facereader [21], for example, is a market research product that measures different variables, such as gender and age, as well as facial expressions while participants watch an advert. This information is analysed to determine how the participant reacted to the advert and ultimately how successful it may be in the wild.

Because micro-expressions are split-second facial cues, they can be difficult for the human eye to pick up. Ekman developed the Facial Action Coding Systems (FACS) which describes the criteria for observing and determining facial

muscle movements, or Action Units (AU) [13]. FACS has been used by technologists to develop a number of micro expression databases used in AI-powered deception detection systems [10]. A variety of technologies have been researched and developed to pick these up and analyse them. Wang *et al.* found that trained professionals only had a 47% accuracy rate in detecting micro-expressions [83] whereas Buhari *et al.* [10] claim that micro-expressions can be detected using AI with 65-80%.

Currently the most comprehensive micro-expression database is the Chinese Academy of Sciences Micro-Expression (CASME) II and it claims to have a 63.41% accuracy rate [83]. It has been researched and utilised by many in the psychology and AI domain but it does not seem to have been used to detect deception in children, or for age verification purposes.

### 5.3 Deception through keyboard dynamics

Because lying requires more cognitive processing than truth telling, Monaro *et al.* [47] found that they could detect a liar by means of the way they interacted with the computer keyboard with 92-94% accuracy. During their study, they posed unexpected text input questions for participants to answer. The unexpected questions put more cognitive strain on the liars, resulting in latency in their responses and a higher error rate. Monaro *et al.* [48], in previous research, also found the use of mouse dynamics and unexpected questions could detect liars with over 90% accuracy.

Given the increase in smartphone and tablet use, relying on mouse dynamics is not a future-proof solution. Similarly, many users will not interact with a traditional desktop keyboard but will instead use a soft keyboard on their smartphone or tablet. While deception detection has not been studied when soft keyboards are used, age-range prediction was investigated by Roy *et al.* [65]. Their study found that by getting youths under 18 and adults to type “Kolkata" into a smart phone, their machine learning model was able to predict the age group of the user with 80-82% accuracy. This was using keystroke dynamic motor behaviour and timing of typing as the main measurements.

### 5.4 Pupil dilation, blink rate and saccadic eye movement

Being able to detect deceit through physical cues in the eye has been researched by several psychologists and technologists in order to determine if technology can pick up subtle changes in pupil dilation, blink rate or saccadic eye movement. Pupil dilation was found by Trifiletti *et al.* [77] to be an accurate way of detecting deception. In their study, they found that pupil dilation greatly increased pre- and post- deceptive statements versus when a participant was telling the truth. This is one cue also advocated by Ekman, but cannot be used in isolation as a reliable indicator of deceit [16].

Similarly, Ekman believes that because lying requires more cognitive processing, blink rates decrease as a deceptive sign. This was investigated by Perelman *et al.* [56] and they did find that there was a difference in blink rate between liars and truth tellers. Borza *et al.* [9], using three different eye blink and facial databases (EyeBlink, Eyeblink 8 and Silesian), were unable to distinguish a correlation between blink rate and liars. However, when they developed a normalised blink rate deviation score, they were able to show which questions were answered truthfully or deceitfully.

Due to the fact blink rate decreases when more cognitive processing is required, even in truth tellers, it can be assumed that if the question is challenging or requires a thoughtful answer, this particular indicator might not deliver accurate deception cues, when used in isolation.

Borza *et al.* [9], in the same project, also investigated whether saccadic eye movements could be used as indicators of deception. Using the eye movement criteria set out by Ekman's FACS and the Silesian database, they were unable to distinguish any pattern related to saccadic eye movement and deceit.

### 5.5 Applications and Criticisms

Using techniques to detect micro-expressions in order to detect deception was trialled on a large scale recently in Europe through an AI product called iBorderCtrl. It was trialled in three European countries land borders, Greece, Latvia and Hungary, and it aimed to detect travellers who were lying about their identity or reason for travel. The project attracted significant attention and was heavily criticised by researchers and ethics groups who argued the system was not ready for *in vivo* testing [39].

Relying on Ekman's micro-expression theories, the system measured micro-expressions of travellers to determine whether the traveller showed signs that they were concealing their inner state. If the system flagged a traveller, they would be taken for further questioning by appropriate border staff [39]. With the system utilising AI, the data set used to train the model has been questioned. Sanchez and Dencik [66] highlight the fact that the iBorderCtrl developers used 32 participants to tell truthful and deceptive statements while video segments were analysed to determine a total of 38 cues labelled truthful or deceptive. Of the 32 participants, 69% were male and 69% were of White European background, calling into question the diversity of the participants used to train the AI model.

Micro-expressions, and their ability to be used for deception detection, has come under heavy fire from a variety of researchers. Lisa Feldman-Barrett [23] has criticised Ekman's work stating that Ekman 'primed' his subjects while developing his micro-expression theories by offering them a closed choice of options to classify expressions. When she repeated his experiments with open choices, she found that recognition of emotions became little better than chance. Similarly, Holmes [33] found that micro-expressions can be "squelched" by a deliberate macro-expression such as a Non-Duchenne smile [94], which would make it difficult to detect a deceptive micro-expression.

However, there remains an argument for utilising AI to detect deception. Kleinberg *et al.* found AI to be significantly more effective at detecting deceit than humans. The AI system that they tested had an overall accuracy score of 69% but when humans were asked to overrule judgements they felt the system did not correctly identify, the accuracy levels were reduced to chance [41].

## 6 Discussion

Returning to the initial research questions set out at the start of this paper:

**RQ1:** *To what extent do online age verification solutions exhibit the three primary dimensions enumerated in Section 2.3?*

A range of solutions exist, as discussed in Sections 4.1 and 4.2. There are severe limitations in terms of efficacy. Where the solution is effective, it is almost always extremely privacy invasive. Where the solution *is* privacy preserving, it tends to be ineffective. Currently, the most utilised method for age verification is a tick box for the user to confirm they are over 18 (e.g., Figure 4). Other common methods include taking a photo of the user and using AI to determine the user's age. These are not infallible, as we show in Figure 6.

Privacy invasive mechanisms dominate, including taking credit card details, requiring personal information to be provided to enable third-party database verification or having a phone number verified (e.g., Figure 5).

Considering the challenges on each of the dimensions enumerated in Section 2.3, we see that the available solutions generally fail on at least one of the dimensions, with the majority invading privacy.

**RQ2:** *What other mechanisms could potentially be used to effect age verification?*

Section 5 reviews a number of directions for future research. In particular, deception detection demonstrates promise. The main methods being researched in other domains of deception detection are the ability to detect deception through micro-expressions, blink rate and keyboard and mouse dynamics. There is significant research and development in this area that could inform its use in age verification.

### 6.1 Reflection and Future Work

Combining the current research areas of age verification and deception detection could provide a novel, privacy preserving approach to the industry problem of preventing youths accessing adults services or products online.

In order to determine whether a user is pretending to be over 18, and trying to access adult services and content online, it is proposed that they be asked to answer free-text questions as part of an age verification process. Using the built-in device camera and keyboard, a machine learning model will take both the camera and keyboard input and evaluate whether the user's behaviour is abnormal, concluding with a deception-likelihood estimate. If the user is deemed to be deceptive, it will be assumed that they are under 18 and trying to conceal this fact.

With respect to the proposed future directions for research, we do not know how inclusive the micro-expression detection will prove to be across all members of the population, including minorities, especially since other mechanisms have failed in this respect [18]. Yet, there is still some disagreement between academics such as Feldman-Barrett [23] and Ekman [16] about whether micro-expressions can be used to signal deception attempts. This is clearly an area calling out for rigorous investigation.

Rigorous age verification mechanisms might well constitute an unacceptable barrier to customers, turning them away altogether because they create too much friction. Mechanisms that are easy to traverse might not be effective in preventing children from accessing the service. The company might then have to pay a fine, which will also affect their bottom line. There is likely to be a sweet spot that has yet to be identified in this space.

### 6.2 Limitations

There has been increasing use of facial recognition for a wide range of purposes over the last few years. Law enforcement has been a particularly enthusiastic adopter [63]. Just recently, official bodies such as the Information Commissioner in the UK have expressed grave concerns about its use [5]. We should note that the kind of biometric we propose is not the same as these, which compare a face to a stored database of faces. We do not need to store any of the images. We will only use them to help us to to estimate the adulthood of an end user. We will process the face biometric to make a judgement, and then delete all artefacts gathered for processing purposes. We will also make it very clear to the user, *before* they allow us to access the camera to see their face, that we will be processing their face algorithmically, and assure them that we will not be storing it on any of our databases, to ensure that we are GDPR compliant [35].

## 7 Conclusion

This paper presents a snapshot of the online age verification arena. We reviewed the current solutions, both research and commercial, and highlighted the general privacy invasiveness of most. We suggest directions for the development of more privacy-protective age verification mechanisms.

We carried out this literature review to provide a snapshot of the state of play related to age verification. We aimed to trigger a discourse into whether it is feasible to come up with a solution that satisfies all dimensions, marked as the "ideal solution" in Figure 1. If not, how do we decide which sector within this three dimensional space we should aim to satisfy? Which is the most important dimension and how do we rank them? There is certainly a tension that needs to be resolved. We also welcome inputs from other researchers related to the viability of the suggested mechanisms outlined in Section 6, in crafting a better age verification solution.

## References


[1] AgeChecked. Age Checked, 2021. Retrieved 16/6/21 from: `https://www.agechecked.com/online-verification-solutions/`.

[2] AgeChecker.net. AgeChecker.net, 2021. Retrieved 29/05/21 from: `https://agechecker.net/`.

[3] C. Baraniuk. Ashley Madison: Leaked accounts fallout deepens, 2015. Retrieved 18 June 2021 from: `https://www.bbc.co.uk/news/technology-34002915`.

[4] C. Baraniuk. Ashley madison: Leaked accounts fallout deepens, 2015. Retrieved 15 August 2021 from: https://www.bbc.co.uk/news/technology-34002915.

[5] BBC. ICO watchdog 'deeply concerned' over live facial recognition, 2021. Retrieved 18 June 2021 from: https://www.bbc.co.uk/news/technology-57504717.

[6] BBC News. Porn blocker 'missing' from Online Safety Bill prompts concern, 2021. Retrieved 18/05/21 from: https://www.bbc.co.uk/news/technology-57143746.

[7] P. Blake. Age verification for online porn: more harm than good? *Porn Studies*, 6(2):228–237, 2019.

[8] M. Borak. Kids are trying to outsmart Tencent's facial recognition system by pretending to be their grandads, 2018. Retrieved 17 June from: https://www.scmp.com/abacus/tech/article/3029027/kids-are-trying-outsmart-tencents-facial-recognition-system-pretending.

[9] D. Borza, R. Itu, and R. Danescu. In the eye of the deceiver: Analyzing eye movements as a cue to deception. *Journal of Imaging*, 4(10):120, 2018.

[10] A. M. Buhari, C.-P. Ooi, V. M. Baskaran, R. C. Phan, K. Wong, and W.-H. Tan. FACS-Based Graph Features for Real-Time Micro-Expression Recognition. *Journal of Imaging*, 6(12):130, 2020.

[11] T. Byron. Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun, 2008. Retrieved 31 May 2020, from https://childcentre.info.

[12] S. Colbert, L. Thornton, and R. Richmond. Content analysis of websites selling alcohol online in Australia. *Drug and Alcohol Review*, 39(2):162–169, 2020.

[13] A. K. Davison, W. Merghani, and M. H. Yap. Objective classes for micro-facial expression recognition. *Journal of Imaging*, 4(10):119, 2018.

[14] S. Dunn and A. Petricone-Westwood. More than 'Revenge Porn' Civil Remedies for the Nonconsensual Distribution of Intimate Images. In S. Dunn and A. Petricone-Westwood, editors, *38th Annual Civil Litigation Conference*, volume 16, 2018.

[15] P. Ekman. Microexpressions, 2021. Retrieved 10/06/21 from: https://www.paulekman.com/resources/micro-expressions.

[16] P. Ekman. Signs of Lying, 2021. Retrieved 15/06/21 from: https://www.paulekman.com/blog/signs-of-lying/.

[17] engadget. TikTok's older users are being blocked after it introduced age checks, 2019. Accessed: 28/06/2021 https://www.engadget.com/2019-03-01-tiktok-age-checks-blocked-users.html.

[18] A. Engler. The Reason Auditors Are Struggling To Hold AI Accountable, 2021. Retrieved 28 January 2021 from: http://www.thelowdownblog.com/2021/01/the-reason-auditors-are-struggling-to.html Jan. 27.

[19] Equifax. Equifax Age Verification, 2021. Retrieved 29/05/21 from: https://www.equifax.co.uk/business/age-verification/en_gb/.

[20] Experien. Experien Age Verification, 2021. Retrieved 29/05/21 from: https://www.experian.co.uk/business/identity-fraud/validation/age-verification/.

[21] Facereader. Facereader Online, 2021. Accessed: 28/06/2021 https://www.facereader-online.com/f.

[22] Federal Trade Commission. Complying with COPPA: Frequently Asked Questions, 2021. Retrieved 21/05/21 from: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.

[23] L. Feldman-Barrett. *How Emotions Are Made: The Secret Life of The Brain*. Houghton Mifflin Harcourt, 2017.

[24] S. Fischer. Kids' daily screen time surges during coronavirus, 2020. Retrieved 20 June 20201 from: https://www.axios.com/kids-screen-time-coronavirus-562073f6-0638-47f2-8ea3-4f8781d6b31b.html.

[25] S. M. Gaiha, L. K. Lempert, and B. Halpern-Felsher. Underage Youth and Young Adult e-Cigarette Use and Access Before and During the Coronavirus Disease 2019 Pandemic. *JAMA Network Open*, 3(12):e2027572–e2027572, 2020.

[26] K. Geldenhuys. The link between teenage alcohol abuse, sexting & suicide. *Servamus Community-based Safety and Security Magazine*, 110(6):14–18, 2017.

[27] F. Gilbert. Age verification as a shield for minors on the internet: A quixotic search. *Shidler JL Com. & Tech.*, 5:1, 2008.

[28] GOV.UK. Digital Economy Bill receives Royal Assent, 2017. Retrieved 3/06/21 from: https://www.gov.uk/government/news/digital-economy-bill-receives-royal-assent.

[29] GOV.UK. Age Verification for Online Pornography to Begin in July, 2019. Retrieved 16/06/21 from: https://www.gov.uk/government/news/age-verification-for-online-pornography-to-begin-in-july.

[30] GOV.UK. Draft Online Safety Bill, 2021. Retrieved 12/06/21 from: https://www.gov.uk/government/publications/draft-online-safety-bill.

[31] GOV.UK. Government calls for age verification on alcohol sales, 2021. Retrieved 21/05/21 from: https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox/call-for-proposals.

[32] G. Hartley and M. Karinch. *I Can Read You Like a Book: How to Spot the Messages and Emotions People Are Really Sending with Their Body Language*. Career Press, Franklin Lakes, USA, 2007.

[33] M. Holmes. National security behavioral detection: a typography of strategies, costs, and benefits. *Journal of Transportation Security*, 4(4):361–374, 2011.

[34] C. Hughes. *Six-Minute X-Ray: Rapid Behavior Profiling*. Evergreen Press, Delaware, USA, 2020.

[35] Information Commissioners Office. Special Category Data, 2021. Retrieved 14/06/21 from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

[36] ISO. Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. ISO 9241-11:2018, 2018.

[37] Jumio. Jumio, 2021. Retrieved 16/6/21 from: https://www.jumio.com/use-case/age-verification/.

[38] S.-G. Jung, J. An, H. Kwak, J. Salminen, and B. Jansen. Assessing the accuracy of four popular face recognition tools for inferring gender, age, and race. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 12, 2018.

[39] L. M. Jupe and D. A. Keatley. Airport artificial intelligence can detect deception: or am i lying? *Security Journal*, 33(4):622–635, 2020.

[40] K. S. Khan, R. Kunz, J. Kleijnen, and G. Antes. Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine*, 96(3):118–121, 2003.

[41] B. Kleinberg and B. Verschuere. How humans impair automated deception detection performance. *Acta Psychologica*, 213:103250, 2021.

[42] P. Kumar, R. K. Rao, and N. H. Reddy. Sustained uptake of LPG as cleaner cooking fuel in rural India: Role of affordability, accessibility, and awareness. *World Development Perspectives*, 4:33–37, 2016.

[43] S. Livingstone, J. Carr, and J. Byrne. One in three: Internet governance and children's rights, 2016. UNICEF. Office of Research-Innocenti.

[44] D. Luciew, J. Mulkern, and R. Punako. Finding the truth: interview and interrogation training simulations. In *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, 2011.

[45] E. Martellozzo, A. Monaghan, J. R. Adler, J. Davidson, R. Leyva, and M. A. Horvath. "I wasn't sure it was normal to watch it..." A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people, 2016. Middlesex University, NSPCC, OCC https://www.mdx.ac.uk/__data/assets/pdf_file/0021/223266/MDX-NSPCC-OCC-pornography-report.pdf.

[46] Mellisa. Mellisa, 2021. Retrieved 16/6/21 from: https://www.melissa.com/age-verification/.

[47] M. Monaro, C. Galante, R. Spolaor, Q. Q. Li, L. Gamberini, M. Conti, and G. Sartori. Covert lie detection using keyboard dynamics. *Scientific Reports*, 8(1):1–10, 2018.

[48] M. Monaro, L. Gamberini, and G. Sartori. The detection of faked identity using unexpected questions and mouse dynamics. *PloS One*, 12(5):e0177851, 2017.

[49] T. Nahari, O. Lancry-Dayan, G. Ben-Shakhar, and Y. Pertzov. Detecting concealed familiarity using eye movements: The role of task demands. *Cognitive Research: Principles and Implications*, 4(1):1–16, 2019.

[50] B. News. 'We have your porn collection': The rise of extortionware, 2021. Retrieved 10/06/21 from: https://www.bbc.co.uk/news/technology-56570862.

[51] Newstalk. British teenager who idolised serial killer found guilty of two murders, 2016. Accessed 26 June 2021 https://www.newstalk.com/news/james-fairweather-serial-killer-britain-guilty-yorkshire-ripper-murders-601896.

[52] NSPCC. Online safety during coronavirus, 2021. Retrieved 12/06/21 from: https://learning.nspcc.org.uk/news/covid/online-safety-during-coronavirus.

[53] Ofcom. Ofcom report on Internet safety measures. Strategies of parental protection for children online, 2015. Accessed: Jan. 12, 2018 https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-Internet-safety-report.pdf.

[54] Ofcom. Childrens Code, 2020. Accessed: 19/06/2021 https://ico.org.uk/childrenscode.

[55] Ofcom. Parents' rising concern over children online, 2020. Accessed 16 June 2021 https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020.

[56] B. S. Perelman. Detecting deception via eyeblink frequency modulation. *PeerJ*, 2:e260, 2014.

[57] N. PERLROTH. Verifying Ages Online Is a Daunting Task, Even for Experts, 2012. Retrieved 15/08/21 from: https://web.archive.org/web/20180131002202/https://www.nytimes.com/2012/06/18/technology/verifying-ages-online-is-a-daunting-task-even-for-experts.html.

[58] J. Peter and P. M. Valkenburg. Adolescents' exposure to sexually explicit internet material and notions of women as sex objects: Assessing causality and underlying processes. *Journal of Communication*, 59(3):407–433, 2009.

[59] S. Porter, L. Ten Brinke, and B. Wallace. Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity. *Journal of Nonverbal Behavior*, 36(1):23–37, 2012.

[60] A. Quadara, A. El-Murr, and J. Latham. The effects of pornography on children and young people. *Australian Institute of Family Studies: Melbourne*, 2017.

[61] K. Renaud and J. Maguire. Regulating access to adult content (with privacy preservation). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 4019–4028, 2015.

[62] K. Renaud and S. Prior. The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor. *Information & Computer Security*, 29(3):526–557, 2021. https://doi.org/10.1108/ICS-07-2020-0115.

[63] K. Ringrose. Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. *Va. L. Rev. Online*, 105:57, 2019.

[64] S. Rouse and J. Ford. *Understanding Body Language: How to Decode Nonverbal Communication in Life, Love, and Work*. Rockbridhge Press, California, USA, 2021.

[65] S. Roy, U. Roy, and D. Sinha. The probability of predicting personality traits by the way user types on touch screen. *Innovations in Systems and Software Engineering*, 15(1):27–34, 2019.

[66] J. Sánchez-Monedero and L. Dencik. The politics of deceptive borders:'biomarkers of deceit'and the case of iBorderCtrl. *Information, Communication & Society*, pages 1–18, 2020.

[67] S. J. Schiff, A. Kechter, K. A. Simpson, R. C. Ceasar, J. L. Braymiller, and J. L. Barrington-Trimis. Accessing vaping products when underage: A qualitative study of young adults in southern california. *Nicotine & Tobacco Research : Official Journal of the Society for Research on Nicotine and Tobacco*, 2021.

[68] J. Schreyögg, M. Bäumler, and R. Busse. Balancing adoption and affordability of medical devices in Europe. *Health Policy*, 92(2-3):218–224, 2009.

[69] R. Shambare. The adoption of whatsapp: breaking the vicious cycle of technological poverty in south africa. *Journal of Economics and Behavioral Studies*, 6(7):542–550, 2014.

[70] V. C. Strasburger, H. Zimmerman, J. R. Temple, and S. Madigan. Teenagers, sexting, and the law. *Pediatrics*, 143(5):e20183183, 2019.

[71] Tech Crunch. TikTok will recheck the age of every user in Italy after DPA order, 2021. Accessed: 28/06/2021 `https://techcrunch.com/2021/02/03/tiktok-will-recheck-the-age-of-every-user-in-italy-after-dpa-order/?guccounter=1`.

[72] The Guardian. UK government faces action over lack of age checks on adult sites, 2021. Retrieved 15/05/21 from: `https://www.theguardian.com/society/2021/may/05/uk-government-faces-action-over-lack-of-age-checks-on-pornography-websites`.

[73] The Independent. By forcing voters show their ID, the Government has found another way to disenfranchise the poor, 2016. Retrieved 10/06/21 from: `https://www.independent.co.uk/voices/voter-id-passport-drivers-license-disenfranchise-poor-a7497801.html`.

[74] D. S. Thomas. Cyberspace pornography: Problems with enforcement. *Internet Research*, 7(3):201–207, 1997.

[75] R. Thompson. Teen girls' online practices with peers and close friends: implications for cybersafety policy. *Australian Educational Computing*, 31(2):1–16, 2016.

[76] J. Torluemke and C. Kim. NortonLifeLock Study: Majority of Parents Say Their Kids' Screen Time Has Skyrocketed During the COVID-19 Pandemic, 2020. Retrieved 20 June 20201 from: `https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2020/NortonLifeLock-Study-Majority-of-Parents-Say-Their-Kids-Screen-Time-Has-Skyrocketed-During-the-COVID-19-Pandemic/default.aspx`.

[77] E. Trifiletti, S. D'Ascenzo, L. Lugli, V. M. Cocco, G. A. Di Bernardo, C. Iani, S. Rubichi, R. Nicoletti, and L. Vezzali. Truth and lies in your eyes: Pupil dilation of White participants in truthful and deceptive responses to White and Black partners. *Plos One*, 15(10):e0239512, 2020.

[78] Trulioo. Trulioo, 2021. Retrieved 16/6/21 from: https://www.trulioo.com/.

[79] UK Safer Internet Centre. Age Restrictions on Social Media, 2018. Accessed: 28/06/2021 https://www.saferinternet.org.uk/blog/age-restrictions-social-media-services.

[80] VerifyMyAge. VerifyMyAge, 2021. Retrieved 29/05/21 from: https://www.verifymyage.co.uk/.

[81] VeriMe. VeriMe, 2021. Retrieved 29/05/21 from: https://verime.net/.

[82] T. Wallace. What is CPRA California Privacy Rights Act Basics Overview, 2021. Retrieved 21 July 2021, from https://www.the-future-of-commerce.com/2021/05/27/what-is-cpra-california-privacy-rights-act-basics-overview/.

[83] Y. Wang, J. See, Y.-H. Oh, R. C.-W. Phan, Y. Rahulamathavan, H.-C. Ling, S.-W. Tan, and X. Li. Effective recognition of facial micro-expressions with video motion magnification. *Multimedia Tools and Applications*, 76(20):21665–21690, 2017.

[84] R. S. Williams, J. Derrick, A. K. Liebman, K. LaFleur, and K. M. Ribisl. Content analysis of age verification, purchase and delivery methods of internet e-cigarette vendors, 2013 and 2014. *Tobacco Control*, 27(3):287–293, 2018.

[85] R. S. Williams, J. Derrick, and K. M. Ribisl. Electronic cigarette sales to minors via the internet. *JAMA Pediatrics*, 169(3):e1563–e1563, 2015.

[86] R. S. Williams and J. C. Derrick. Internet little cigar and cigarillo vendors: surveillance of sales and marketing practices via website content analysis. *Preventive Medicine*, 109:51–57, 2018.

[87] R. S. Williams and K. M. Ribisl. Internet alcohol sales to minors. *Archives of Pediatrics & Adolescent Medicine*, 166(9):808–813, 2012.

[88] G. M. Winters, L. E. Kaylor, and E. L. Jeglic. Sexual offenders contacting children online: an examination of transcripts of sexual grooming. *Journal of Sexual Aggression*, 23(1):62–76, 2017.

[89] N. Wood. Charlotte's accessible web: how West Australian children and adolescents can access e-cigarettes online. *Australian and New Zealand Journal of Public Health*, 45(1):81–82, 2021.

[90] M. H. Yap, H. Ugail, and R. Zwiggelaar. Facial behavioral analysis: A case study in deception detection. *British Journal of Applied Science and Technology*, 4(10):1485–1496, 2014.

[91] M. Yar. Protecting children from Internet pornography? A critical assessment of statutory age verification and its enforcement in the UK. *Policing: An International Journal*, 43(1):183–197, 2019.

[92] Yoti. Yoti, 2021. Retrieved 29/05/21 from: https://www.yoti.com/.

[93] Yoti. Yoti Age Scan, 2021. Retrieved 14/06/21 from: https://www.yoti.com/wp-content/uploads/Yoti-age-estimation-White-Paper-May-2021.pdf.

[94] M. Zloteanu. *Reconsidering Facial Expressions and Deception Detection*. FEELab Science Books, 2020.

# A Appendix A