No. 23-1122

IN THE

Supreme Court of the United States

FREE SPEECH COALITION, ET AL.,

Petitioners,

v.

KEN PAXTON, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL FOR THE STATE OF TEXAS,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Fifth Circuit

JOINT APPENDIX

AARON L. NIELSON
Counsel of Record
OFFICE OF THE
ATTORNEY GENERAL
P.O. Box 12548 (MC 059)
Austin, TX 78711
(512) 936-1700
Aaron.Nielson
@oag.texas.gov

Counsel for Respondent

DEREK L. SHAFFER
Counsel of Record
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
1300 I Street NW, Ste. 900
Washington, DC 20005
(202) 538-8000
derekshaffer
@quinnemanuel.com

Counsel for Petitioners

September 16, 2024

PETITION FOR CERTIORARI FILED APRIL 12, 2024
CERTIORARI GRANTED JULY 2, 2024

TABLE OF CONTENTS

Received: 16 August 2020 | Accepted: 5 March 2021

DOI: 10.1002/poi3.250

RESEARCH ARTICLE Policy & Interest P&I Wiley

The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches

Neil Thurman[1],[2] Fabian Obster[3],[4]

Correspondence

Neil Thurman, Department of Media and Communication, LMU Munich, Oettingenstr. 67, 80538 Munich, Germany.

Email: neil.thurman@ifkw.lmu.de

Abstract

In 2017, the UK Parliament passed an Act requiring legal pornographic websites to implement 'robust' age verification checks. Although the Act inspired lawmakers elsewhere to propose similar legislation, it was never enacted, in part because it did not cover social media platforms. Instead, the UK government has turned to its Online Harms White Paper—which does target social media platforms—to protect children from online pornography. There is, however, scant evidence

[1] Department of Media and Communication, LMU Munich, Munich, Germany

[2] Department of Journalism, City, University of London, London, UK

[3] Department of Statistics, LMU Munich, Munich, Germany

[4] Department of Business Administration, Universität der Bundeswehr, Munich, Germany

on the media platforms and technologies children use to access pornography. To fill this knowledge gap, we conducted a survey of 16- and 17-year-olds in the United Kingdom. The results show that more (63%) had seen pornography on social media platforms than on pornographic web-sites (47%), suggesting the UK government was right to target such platforms in its latest proposals. However, pornography was much more frequently viewed on pornographic websites than on social media, showing how important the regulation of such sites remains. Furthermore, our finding that 46% of 16-and 17-year-olds had used a virtual private network or Tor browser adds weight to concerns that restrictions on legal internet pornography—such as age verification checks—imposed by a single country may be circumvented by those the restrictions are designed to protect.

KEYWORDS

adolescents, age verification, Digital Economy Act 2017, internet regulation, Online Harms White Paper, online pornography, VPNs, young people

INTRODUCTION

The moral panic over ‘cyberporn’ may not have begun with *Time* magazine’s eponymous 1995 cover story, but Philip Elmer-Dewitt’s infamous article certainly amplified the anxiety. Drawing on a controversial piece of research, his feature claimed that ‘trading in sexually explicit imagery ... is now one of the largest ... recreational applications of ... computer networks’ (Elmer-Dewitt, 1995). Whatever that claim’s contemporaneous veracity, some of the issues raised in the article remain relevant more than two decades later, including: How online pornography can ‘fall into the hands of’ children and adolescents; lawmakers’ ‘obligation to preserve essential civil liberties’; and the difficulties of censoring global, decentralised communications networks (ibid.).

Elmer-Dewitt’s article was published at a time when governments were starting to take positions on these issues. In some countries with weak or poorly upheld civil liberties, decisions were being taken to proscribe online pornography altogether. In the same year as the *Time* cover story, for instance, the People’s Republic of China announced such a ban (Associated Press, 1995). Two years later, when Vietnam allowed its residents to access the internet, it did so with filters that blocked pornography (AFP, 1997). Similar prohibitions are still in place in a number of countries—such as the United Arab Emirates, Uzbekistan and Pakistan (Freedom House, 2019a, 2019b, 2019c).

Most democratic countries have not tried to completely prohibit online pornography, but have tended to restrict only certain forms such as ‘child’ and ‘extreme’ pornography (Nair, 2019). Although some of their politicians have attempted to bring in wider bans on legal, adult pornography, those efforts have largely been frustrated by free speech rights (see, e.g., Carlin, 1996) and by the global nature of the internet, which makes it challenging to enforce national legislation on providers of pornography located outside a country's jurisdiction. Publishers of pornography tend to be based in territories that do not impede their operations.

The 1995 *Time* magazine cover story said 'some fairly daunting' computer skills were required to download and view pornographic images from the internet (Elmer-Dewitt, 1995). Such skills are clearly no longer necessary. In 2009, the president of the British Board of Film Classification (BBFC) talked about how a 'vast catalogue of explicit pornographic videos' was available instantly, and for free, via popular "YouTube-style" websites' (Wake, 2009). One such site, Pornhub, which was launched in 2007, is now, by one measure, the 27th most popular website in the world (Alexa, 2019).

The popularity of such so-called 'porn-tube' sites may be a reason why governments in some democracies have started to look again at their laws. In 2013, the Icelandic government proposed 'creating a national internet filter and a blacklist of websites that contain pornographic content'. That plan, however, never reached the statute book (Freedom House, 2017). Not so the United Kingdom's Digital Economy Bill, which passed into law in 2017. The Digital Economy Act, as it became, meant that the United Kingdom became one of the first democracies in the world to pass legislation that, if enacted, would limit access to legal online pornography by its residents. Part 3 of the Act required providers of online commercial pornography accessible from the United Kingdom to deploy robust age verification controls to ensure that those accessing explicit material were at least 18-years old. The law targeted pornographic sites based outside the United Kingdom. Sites based in the United Kingdom were already subject to such regulations but had next to no market share (Chorley, 2014). The body that was initially appointed to enforce the legislation would have had the power to instruct internet service providers in the United Kingdom to block sites that did not comply (BBFC, 'Frequently Asked Questions', https://www.ageverificationregulator.com/faq#10), as well as take other measures.

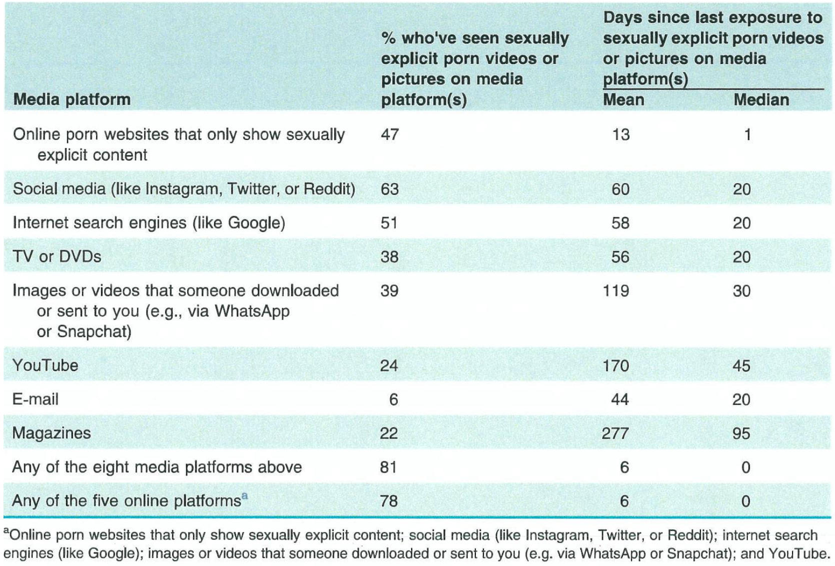
The United Kingdom's age verification legislation prompted governments in Ireland, Australia, New Zealand, and Poland to consider similar measures (Finn, 2019; Radio New Zealand, 2018; Taylor, 2020; Yagielowicz, 2019). France passed a similar law in July 2020 (Braun & Kayali, 2020) and a private member's bill that aims to restrict 'young persons' online access to sexually explicit material' received its first reading in the Canadian Senate in September 2020 (Parliament of Canada, 2020). In Germany, authorities are attempting to force internet service providers to block legal pornographic websites that do not implement age verification controls (Geiger, 2020). However, Part 3 of the Digital Economy Act has not been enacted by the UK government and looks unlikely to be, in part because it did not cover social media platforms, a potential source of pornographic content. Instead, the UK government has tabled an alternative, wider set of proposals aimed at 'tech companies' that allow 'users to share or discover user-generated content or interact with each other online'. The proposals aim to reduce 'online harms'—such as children's exposure to adult pornography—through a 'range of tools' (Gov.uk, 2020), including, but not limited to, age verification technologies. There are important differences between sexually explicit content that is user-generated and commercial pornography, and the transition in regulatory attention from a focus on commercial porn to 'harmful' user-generated content will be addressed further later in this article.

In light of the policies being formulated by elected governments to regulate legal internet pornography, this study seeks to add to the evidence from which such policies can draw and provide a baseline for future longitudinal research on the effects of any legislation that is enacted in the United Kingdom. We do this by conducting and analysing a survey of 16- and 17-year-olds in the United Kingdom (*N*=1,001). Specifically, we analyse the proportions of 16- and 17-year-olds who have been exposed to online (and offline) pornography, the frequency and duration of any such consumption, and any sociodemographic variations. As we have mentioned, the United Kingdom's original age verification legislation only targeted dedicated pornographic websites. Social media platforms, search engines, and video-sharing sites such as YouTube were exempt. The UK government's subsequent proposals do, however, target these other platforms. In light of this change, our analysis also looks at which platforms 16- and 17-year-olds in the United Kingdom use to access pornography. Questions have been raised about the effectiveness of age verification controls on online pornography because, some say, users could easily bypass such controls using technologies such as VPNs (virtual private networks) and Tor browsers (see, e.g., Matthews-King, 2018). Consequently, we also analyse the extent to which 16- and 17-year-olds in the United Kingdom are aware of and use these technologies.

Our results show that, overall, 80.5% of 16- and 17-year-olds in the United Kingdom said they had seen 'sexually explicit porn videos or pictures'. Among this large majority, their last exposure was, on average, 5.5 days previously. It was most common, however, for those 16- and 17-year-olds in the United Kingdom who had seen sexually explicit videos or pictures to have seen them on the day they completed the survey (see Table 1 and Figure 1).

A higher proportion of 16- and 17-year-olds in the United Kingdom have been exposed to sexually explicit videos or pictures on social media (63%) and search engines (51%) than on dedicated pornographic websites (47%). However, pornographic material is much more frequently viewed on dedicated pornographic websites than on social media, search engines, or YouTube (see Table 1 and Figure 1).

TABLE 1 Reach of, and recency of exposure to, sexually explicit porn videos or pictures via eight media platforms among 16- and 17-year-olds in the United Kingdom, June 2019



Media platform	% who've seen sexually explicit porn videos or pictures on media platform(s)	Days since last exposure to sexually explicit porn videos or pictures on media platform(s)	
		Mean	Median
Online porn websites that only show sexually explicit content	47	13	1
Social media (like Instagram, Twitter, or Reddit)	63	60	20
Internet search engines (like Google)	51	58	20
TV or DVDs	38	56	20
Images or videos that someone downloaded or sent to you (e.g., via WhatsApp or Snapchat)	39	119	30
YouTube	24	170	45
E-mail	6	44	20
Magazines	22	277	95
Any of the eight media platforms above	81	6	0
Any of the five online platforms[a]	78	6	0

[a] Online porn websites that only show sexually explicit content; social media (like Instagram, Twitter, or Reddit); internet search engines (like Google); images or videos that someone downloaded or sent to you (e.g. via WhatsApp or Snapchat); and YouTube.

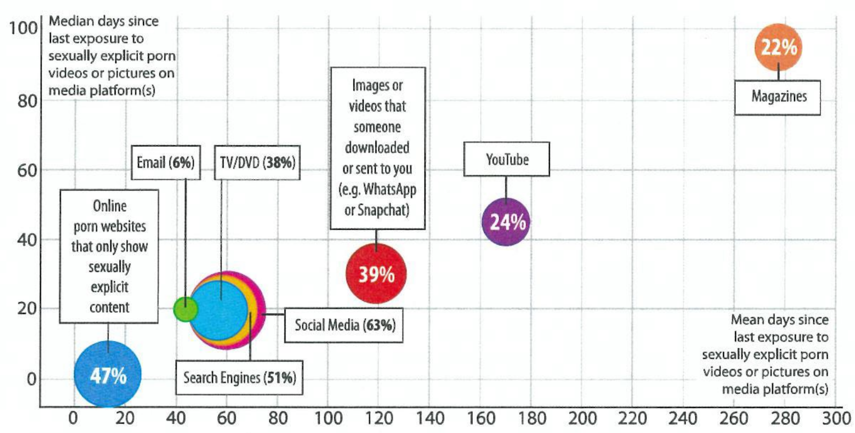


FIGURE 1 Reach of—and recency of exposure to—pornography via each of eight media platforms among 16- and 17-year-olds in the UK (*N* = 1,001). The size of the bubbles indicates the proportion who have had any exposure. The position of the bubbles indicates the mean and median days since last exposure

Regression analysis showed significant differences in the consumption of pornography by males and females and by respondents from households of different social grades.

Finally, our results also showed that 46% of 16- and 17-year-olds had used a VPN or Tor browser and another 23% knew what they were.

The study has important implications for legislators considering the regulation of legal internet pornography. First, it shows that a large majority of 16- and 17-year-olds in the United Kingdom are exposed to online pornography and that the exposure is relatively frequent. Second, it shows the targets of the United Kingdom's original age verification legislation—dedicated pornographic websites—are the most frequent source of internet pornography for 16- and 17-year-olds in the

United Kingdom, with those who use them doing so for an average of 2 h 18 min a month. However, other sources, such as social media platforms, are also important, suggesting that the UK government was right to include such platforms in its latest proposals to reduce children's exposure to legal online pornography. Third, the level of knowledge about, and use of, VPNs and Tor browsers by those under 18 in the United Kingdom adds weight to concerns that restrictions on the access to legal online pornography imposed by a single country may be circumvented by those the checks are designed to protect.

In the Literature Review, we will provide a brief history of the United Kingdom's age verification legislation and its likely successor and review some of the previous research on children and adolescents' exposure to online pornography, including such data as exists about the platforms through which they are exposed. A description of the methods used in our survey comes next, followed by the Results and Discussion.

LITERATURE REVIEW

The United Kingdom's age verification legislation and its likely successor

The Digital Economy Act of 2017 stated that legal online commercial pornography accessible from the United Kingdom must deploy age verification controls to prevent children from accessing explicit material. UK pornographic sites were already required to deploy age verification, but most pornographic sites visited by UK users are located outside the United Kingdom (Department for Digital, Culture, Media and Sport [DCMS], 2017, p. 4) and it is these sites that the Act targeted. The BBFC, the body that deals with age regulation for films and videos, was tasked with oversight. The stated intention was to apply the same age regulation that applies to legal offline pornography to legal online pornography (BBFC, 'Age-Verification under the Digital Economy Act 2017', https://www.ageverificationregulator.com/).

The Act was introduced by the Conservative government in line with a 2015 manifesto commitment (Gayle, 2018; Children's Media Foundation, 2020). The age verification measures were to be found in Part 3 of the Act, which also prohibited the availability of extreme pornographic content online (BBFC, 'Frequently Asked Questions', https://www.ageverificationregulatorcom/faq/#1).

If implemented, the age verification regulation would have required people wishing to access legal commercial online pornography to prove they are over 18. According to the BBFC, the system would not have involved personal identification of the user (BBFC, 'Age-Verification under the Digital Economy Act 2017', https://www.ageverificationregulator.com/). There would have been several age verification options, 'normally' provided by third parties so that users would not have had to share personal information directly with pornographic websites. This might have involved buying a card in a shop or using ID documents online. The BBFC stated that its main focus would be on 'commercial pornographic sites with high volumes of traffic'. It would carry out 'spot checks on less-visited sites' and also provide a means for individuals to report noncompliers (BBFC, 'Frequently Asked Questions', https://www.ageverificationregulatorcom/faq/#1).

Critics pointed out that the measures left some legal online pornography unpoliced. They did not cover 'websites on which less than a third of the content is pornographic material and where it is provided free of charge', which meant that 'blogging, social media and image-sharing services such as Imgur, Tumblr, Twitter and Reddit, which host vast quantities of pornographic content', would 'continue to be accessible without any age checks' (Gayle, 2018). Search engines too fell outside the regulations (BBFC, 'Frequently Asked Questions', https://www.ageverificationregulator.com/faq/#1).

The BBFC could have requested social media and search engines to withdraw their services from non-compliers (BBFC, 'Frequently Asked Questions', https://www.ageverificationregulator.com/faq/#1), but they would not have been obliged to do so. The same was true for payment service providers (DCMS, 2017). The BBFC would, however, have had the power to instruct internet service providers to block noncompliant pornographic services (DCMS, 2017).

Concerns were also voiced about users being pushed towards the dark web. The Open Rights Group talked of users being forced 'underground' and resorting to the use of masked means of browsing such as Tor, which anonymises usage and makes available extreme and illegal material (Wheeler, 2018).

Some critics described the regulations as 'largely unworkable', with the restrictions easily sidestepped by the use of 'a virtual private network or other software' that allows access to sites 'via an unrestricted country' (Matthews-King, 2018). It was claimed that though the scheme might help to prevent children stumbling on inappropriate sites, it would provide little impediment to 'determined teenagers' (Kelion, 2017). The government impact report acknowledged the possible use of VPNs and peer-to-peer sharing as a means of bypassing restrictions, however, the Age Verification Providers Association denied that restrictions could be ‘easily circumvented’, claiming that adult sites can block VPNs if they want, ‘just as Netflix and the BBC iPlayer already do’ (Children’s Media Foundation, 2020).

The legislation was subject to delays. In March 2018, the government stated that it needed more time to ‘get it right’ (Kleinman, 2018), and in June 2019, it announced another delay, ‘in the region of 6 months’, because it had failed to inform the European Union of the proposals as required by European law (Waterson & Hem, 2019).

In October 2019, the UK government announced that it would ‘not be commencing Part 3 of the Digital Economy Act 2017 concerning age verification for online pornography’ (Morgan, 2019). It stated that this was not due to any lessening of its desire to protect children from accessing inappropriate, harmful content, which it still believed was ‘vital’ (ibid.). Rather, it appeared to have had concerns that the age verification regulations that formed part of the Digital Economy Act were not ‘coherent’ and ‘comprehensive’, in part because they did ‘not cover social media platforms’ (ibid.). Others suggested privacy concerns may have played a part in the decision, with the companies developing the age verification procedures subject only to ‘voluntary’ privacy commitments and user details vulnerable, it was said, to a data breach (BBC News, 2020).

As an alternative, the government proposed that its ‘objective of protecting children from online pornography’ (Gov.uk, 2020) could be achieved through proposals developed as part of its Online Harms White Paper (HM Government, 2019), which it had published in April 2019. This Paper was wider in scope than the abandoned regulations. It placed a ‘duty of care on companies to improve online safety' (Morgan, 2019), with the 'harms' listed in the Paper including terrorist propaganda, cyberbullying and assisting suicide, in addition to 'underage exposure to legal content', which included 'children accessing pornography' (HM Government, 2019, p. 31). The government proposed that the regulatory framework should apply to 'companies that allow users to share or discover user-generated content or interact with each other online' and named 'social media platforms, file-hosting sites, public discussion forums, messaging services and search engines' as examples of such companies (p. 8).

In its response to the feedback it received on the Paper, the government said it would 'expect companies to use a proportionate range of tools, including age assurance and age verification technologies to prevent children from accessing age-inappropriate or harmful content' (Gov.uk, 2020). The Office of Communications (Ofcom), which regulates communications services including television and radio (Ofcom, 'What Is Ofcom?', https://www. ofcom.org.uk/about-ofcom/what-is-ofcom), is likely to be the regulator of any Online Harms Act (Gov.uk, 2020) and may have 'powers to issue substantial fines and to impose liability on individual members of senior management' (HM Government, 2019, p. 7) for noncompliance.

Research into adolescents' use of pornography, including online

Prevalence and predictors

Peter and Valkenburg's (2016) review of 20 years of research about adolescents and pornography provides a comprehensive summary of the literature that was published between 1995 and 2015. The authors reviewed 75 studies and one of their goals—to 'revisit the question of the prevalence and predictors of adolescents' use of pornography'—is relevant to this study. They found that 'findings about the prevalence of adolescents' use of pornography differ greatly'. The authors concluded that, although the studies 'suggest that at least a sizable minority of all adolescents use pornography', 'exact aggregate figures about adolescents' pornography use seem difficult to derive from the literature'.

They provide three reasons for this 'diversity of findings'. First, that the studies have varied methodologically, 'notably in terms of sampling method, sample size, sample composition, survey mode/administration, and operationalization of pornography use'. Second, that in the period under review the 'Internet has undergone dramatic changes—and with it adolescents' access to internet pornography'. Third, 'the cultural context (e.g., sex education, sexual liberalism) of studies is likely to affect how often adolescents (report to) use pornography'. Kohut et al. (2020) agree that there is little by way of a global consensus regarding the proportion of people who use pornography and the intensity of that use. They too point to differences in sample composition between studies and how those studies conceptualised and measured pornography use.

Although Peter and Valkenburg (2016) make clear that generalisations are not possible about the prevalence of adolescents' use of pornography, they do make a tentative generalisation about the predictors of such use, specifically that 'the most likely users of pornography are male, pubertally more advanced, sensation-seeking adolescents with weak or troubled family relations'. This conclusion was supported by Alexandraki et al.'s (2018) systematic review of research on adolescent pornography use, which included research published up to 1 May 2017.

Research about young people and pornography published since 2017, and therefore, not part of Peter and Valkenburg's (2016) or Alexandraki et al.'s (2018) reviews, has continued to focus on a variety of cultural contexts, to utilise differently sized and composed samples, and to define pornography in a variety of ways. It is no surprise then that these studies differ in the proportions of young people they find to have been exposed to pornography. For example, Wright et al. (2020) found that 68% of the US sample of the 14- to 18-year-olds they surveyed had viewed pornography (defined as 'sexually explicit pictures, videos, or livestreams'), whereas, in Hong Kong, Ma et al. (2017) found that only 2%-6% of their 11- to 16-year-old sample had intentionally viewed pornography and 4%-14% had come across it unintentionally.

There has been a limited amount of research on the exposure to pornography by children and adolescents in the United Kingdom. Horvath et al. (2013) identified fewer than 10 studies published between 1983 and 2013 that contained '"new" empirical evidence'. Indeed, Nash et al. (2015, p. 5) were, in 2015, unable 'to find any recent UK studies which provide clear figures for online and offline viewing of pornography for all children up to the age of 18'. Since 2015, there has, however, been one study that does provide some clear figures. An online survey commissioned by BBFC and conducted in 2019 with a representative sample (*N* 1,142) of children and adolescents in the United Kingdom found that 51% of 11- to 13-year-olds, 66% of 14- and 15-year-olds, and 79% of 16- and 17–year-olds had seen pornography at some point (BBFC, 2020, p. 15). Other than for age, the study did not report on any potential predictors of pornography use found within the survey data, for example gender or socio-economic classification.

Intensity of consumption

In addition to whether or not children and adolescents have been exposed to pornography, the intensity of any consumption—in terms of both frequency and time spent—is clearly of interest, given that there is some evidence that frequent use is associated with problem behaviours (Svedin et al., 2011), including internet pornography addiction (Harper & Hodgins, 2016).

In their review of 276 studies on pornography and children/adolescents published up to 2013, Horvath et al. (2013, p. 22) note discrepancies 'with regard to the regularity of exposure', with some research suggesting that exposure is infrequent and other studies reporting greater frequency. This contradictory evidence, the authors write, 'highlights the importance of considering frequency as well as prevalence to obtain a full picture'. According to the authors, 'few studies have considered the length of time spent viewing pornography' (p. 22).

In the context of the United Kingdom, the only quantitative data on the frequency with which pornography was consumed that was reported in the aforementioned BBFC survey related to whether exposure had been 'in the last 2 weeks' or earlier. Of those who had seen pornography, between 18% (of 11- to 13-year-olds) and 41% (of 16- and 17-year-olds) had seen it in the last 2 weeks (BBFC, 2020, p. 15). The BBFC study also conducted 36 qualitative interviews with 16- to 18-year-olds. 'Most' of the 20 boys interviewed 'reported having watched pornography daily for a period of their lives', while the amount of pornography watched by the 16 girls varied: 'Some ... reported watching pornography four times a week between the ages of 14 and 16, whereas others said they watched it a few times a month' (BBFC, 2020, p. 20).

Although the BBFC study did not report the amount of time children and adolescents spent viewing pornography, there are some recent figures from New Zealand, courtesy of a nationally representative survey (*N* = 2,071) carried out by the Office of Film and Literature Classification (OFLC)—New Zealand's equivalent of the BBFC—with 14- to 17-year-olds. The results show that most (71%) of 14- to 17-year-olds in New Zealand who had seen pornography in the last 6 months spent either 'a few minutes' or 'up to half an hour' looking at porn each time they saw it (OFLC, 2018, p. 24).

Platforms

Beyond the prevalence and intensity of pornography use among adolescents, this study is also interested in how—that is, through which media platforms—that exposure takes place. Having such data will allow us to evaluate the UK government's decision to expand its plans for the regulation of legal internet pornography to include material available on platforms other than dedicated pornographic websites, such as social media networks.

The literature on children and adolescents' use of pornography rarely pays much attention to the platforms through which that use takes place. This is understandable given that the foci of many of the previous studies—on, for example, sexual behaviour (Doornwaard et al., 2015), academic performance (Beyens et al., 2015), and sexting (Van Ouytsel et al., 2014)—were not expected to be influenced by the particular platforms through which pornography was accessed but rather the level of exposure to pornography in general.

Though some studies have collected data on the particular platforms used by young people to access pornography, that data is not always reported (see, e.g., Hardy et al., 2013). Where the data is reported, the platforms listed may overlap (see, e.g., Ma et al., 2017). As a result, it is, as Nash et al. (2015, p. 6) write, 'surprisingly complicated to determine whether pornographic content is viewed by children "online" or "offline."'

Such literature that does exist demonstrates, unsurprisingly, that 'the most common ways in which children and young people access pornography have changed in recent years, from magazines, videos, television and books ... to the internet playing a more dominant role' (Horvath et al., 2013, p. 24). This said, at least up to 2013, the use of 'DVDs, films, magazines and television' as a source was apparently 'still widespread' (ibid.). In the UK context, data from 2010 also showed that traditional mass media may have had a significant role—at that time—in children's exposure to pornography (Nash et al., 2015).

The above-mentioned BBFC study is, as of June 2020, the most recent to provide, in the context of the United Kingdom, some data on the particular *online* platforms through which young people consume pornography. The survey found that for children aged 11-17 (as well as for 16- and 17-year-olds) 'image or video search engines' were the most commonly used source to intentionally seek out pornography, followed by social media sites and dedicated pornography websites. Among 16- to 17-year-olds, 62% had intentionally sought out pornography via an image or video search engine, 46% via social media sites, and 44% via dedicated pornography websites (BBFC, 2020, p. 26). Among the—albeit small and unrepresentative—group of three dozen 16- to 18-year-olds who were interviewed for the study, 'dedicated pornography sites such as Pornhub and xHamster were the most popular source of pornography', although 'it was also very common for respondents to have seen pornography through social media', with the most common platforms being Snapchat, Instagram and Twitter (BBFC, 2020, p. 23).

The aforementioned OFLC study also provides recent data on the particular platforms through which pornography is accessed by 14- to 17-year-olds in New Zealand. The survey found that, of those who had seen pornography in the last 6 months, mobile/smart phones were the main source for 56% and computers, tablets, TVs, or other digital devices for 37%. Magazines or books were the main source for only 2% of respondents (OFLC, 2018, p. 28). In terms of how *online* pornography was accessed, 'porn websites' were the most common source (for 66%), followed by 'Google or another online search service' (28%), 'other websites' (25%) and 'social media and other online services or apps' (16%) (OFLC, 2018, p. 28).

It is notable that social media sites and search engines appear to be less frequent sources of pornography in New Zealand than in the United Kingdom, although this may be to do with the differences in the surveys' samples and methodologies.

Workaround technology

As has been mentioned, the United Kingdom's original age verification legislation was criticised by some on the grounds that users would easily be able to bypass such controls, using technologies such as VPNs and Tor browsers (see, e.g., Matthews-King, 2018). The only data we could find on the use of VPNs or Tor browsers by children was in the aforementioned BBFC study, which found that 23% of children aged 11-17 reported 'knowing how to use a potential "workaround" (i.e. a VPN… the use of Tor)' that could circumvent age verification, and this knowledge increased with age (to 33% of 16- to 17-year-olds) (BBFC, 2020, p. 56).

Hypotheses and research questions

Although this study will not engage in specific hypothesis testing, the literature suggests that 'at least a sizable minority' (Peter & Valkenburg, 2016) of UK adolescents will use pornography. Indeed, given that the United Kingdom is—compared with some other countries—relatively sexually liberal and that pornography is now easily available via the internet, the BBFC's (2020) finding that a large majority (79%) of 16- and 17-year-olds in the United Kingdom have seen pornography at some point seems plausible. In line with other research (see Peter & Valkenburg, 2016 and Alexandraki et al., 2018 for a summary), we would expect a higher level of consumption by males and also, perhaps, differences according to familial background. Recent data on the intensity with which pornography is consumed by young people in the United Kingdom is mostly anecdotal, but it does indicate regular consumption, especially by boys (BBFC, 2020, p. 20).

Little research exists on how—that is, through which media platforms—children and adolescents are exposed to pornography. However, printed books and magazines look likely to be a less frequent source than computers and, especially, smartphones (OFLC, 2018, p. 28). In the online environment, dedicated pornographic websites, social media sites, and search engines are likely to be sources of pornography (BBFC, 2020; OFLC, 2018), although the relative importance of these platforms as a source of online pornography is not clear from the literature. The extent to which children and adolescents are aware of—and use—technologies, such as VPNs and Tor browsers, that can be used to circumvent attempts to limit access to online pornography in particular jurisdictions is unclear, although one UK study indicated that a third of 16- to 17-year-olds may know how to use such technology (BBFC, 2020, p. 56).

Our first research question seeks to establish the prevalence and recency of pornography use among 16- and 17-year-olds in the United Kingdom:

RQ1: *What proportion of 16- and 17-year-olds in the United Kingdom have seen sexually explicit videos or pictures via any of eight named media platforms and how recent was any such exposure*?

Our second research question examines how—that is, through which media platforms—UK 16- and 17-year-olds are exposed to pornography:

RQ2: *Which media platforms do 16- and 17-year-olds in the United Kingdom use to view pornographic videos or pictures and how recent is the use of each platform for this purpose*?

For one particular platform, the subject of the original UK age verification legislation, we also ask:

RQ3: *How much time do 16- and 17-year-olds in the United Kingdom spend visiting dedicated pornographic websites per month and how is that* *time split between personal computers (PCs) and mobile devices (smartphones and tablets)*?

To better understand knowledge about, and use of, technology that could be used to circumvent any national limits on the access to online pornography, our final research question asks:

RQ4: *What proportions of 16- and 17-year-olds in the United Kingdom are aware of, or have used, a VPN or Tor browser*?

Although the primary focus of our study was not on differences between individuals, for each of the above research questions we also analysed whether there were any differences according to respondents' age, gender, parental social grade, and their knowledge about/use of VPNs/Tor browsers. We did this for three reasons. First, in order that our results could contribute to what is known, in general terms (see, e.g., Peter & Valkenburg, 2016; Alexandraki et al., 2018), about the individual differences in pornography use among adolescents (specifically 16- and 17-year-olds). Second, because very little, if anything, is known about individual differences in contemporary pornography use among adolescents (specifically 16- and 17-year-olds) in the UK context. Third, because one of the individual differences (knowledge about/use of VPNs/Tor browsers) speaks directly to one of the primary aims of this study—the evaluation of the potential efficacy of emerging legislative approaches.

It was decided to restrict the survey to 16- and 17-year-olds, in part because it was not possible, for ethical reasons, to question children below the age of 16 on this topic without a parent or guardian being present. The presence of a parent or guardian would likely have influenced the answers they gave, for reasons of social desirability.

METHOD

Survey instrument and procedure

The survey consisted of five questions (see online Supporting Information Material). The survey was fielded in June 2019 using YouthSight's online research panel that had, at the time, approximately 140,000 UK-based panellists aged 16-30. YouthSight's panellists are recruited via a variety of channels including social media, partnerships with 'reliable, niche organisations' (YouthSight, 2018) and websites—including their own online community, OpinionPanel. Their recruitment process is compliant with the Market Research Society's (MRS) Code of Conduct and Binding Guidelines (ibid.). Panellists are paid up to £4 for each survey they take. As with most online research panels, YouthSight does not verify the identity of its panellists face-to-face. However, a variety of steps are taken to check the veracity of the demographic data YouthSight hold. For example, the self-reported ages of panellists are regularly checked by evaluating whether they are responding as expected for someone of their age. The self-reported locations of panellists are also regularly checked, including by comparing the region from which panellists are completing a survey against their self-reported location (Hayley Adonis, Head of Project Management, YouthSight, personal communication, 15 February 2021).

YouthSight is accredited by MRS.[1] The research was carried out in line with the guidance contained within MRS's *Guidelines for Research with Children and Young People* (MRS, 2014), including gathering informed consent, offering respondents the opportunity to stop the survey at any time, and giving a 'prefer not to say' option with each question. Indeed the MRS was specifically consulted about the ethical aspects of the survey instrument and approved its fielding.

The selection of panellists for the survey aimed to achieve a final sample that matched the spread of genders and parental social grades found among the population of 16- and 17-year-olds in the United Kingdom. Parental social grade is an 'occupation-based measure of socioeconomic status' (Ally et al., 2016) that is widely used in the United Kingdom. An initial set of survey invitations were sent to eligible panellists and survey completions monitored to see how the gender and social grade quotas were being filled. Subsequent survey invitations were more targeted in an attempt to meet the required quotas (Hayley Adonis, Head of Project Management, YouthSight, personal communication, 15 February 2021). Because the required quotas were not met exactly (see Table S1), the responses were weighted by gender[2] and parental social grade[3] so that the results would be more representative of the wider population of 16- and 17-year-olds in the United Kingdom. No weighting was applied regarding age, but, as is shown in the results section, no significant differences were found between 16- and 17-year-olds regarding whether, when, and how they had been exposed to sexually explicit videos and pictures. After data cleaning, the final sample contained 1,001 responses.

Because of the different types of measures used (e.g., ever seen pornography, number of days since last exposure to pornography and time spent using pornography) and their different measurement scales (binary and count), it was necessary to vary our analysis methods. For example, we used logistic regression for the binary variable and overdispersed Poisson regression (Gardner et al., 1995) and linear regression for the count variables. All our statistical analyses are based on generalised linear models (McCullagh & Nelder, 1989). The data were analysed in R (R Core Team, 2018). In the results section, *ß* is the coefficient of either the logistic, linear, or overdispersed Poisson regression.

RESULTS

RQ1: *What proportion of 16- and 17-year-olds in the United Kingdom have seen sexually explicit videos or pictures via any of eight named media platforms and how recent was any such exposure*?

Overall, 80.5% of 16- and 17-year-olds in the United Kingdom said they had seen, at least once, sexually explicit videos or pictures on at least one of the media platforms listed in the survey[4] (see Table 1 and Figure 1).

Among the large majority who had seen sexually explicit videos or pictures, their last exposure was, on average, 5.5 days previously. However, this mean figure was raised by a long tail of respondents whose last exposure was months ago. It was most common for those 16- and 17-year-olds in the United Kingdom who had seen sexually explicit videos or pictures to have seen them on the day they completed the survey: the median number of days since their last exposure was '0' (see Table 1 and Figure 1).

We compared[5] those who had and had not, been exposed to sexually explicit videos or pictures on any of the media platforms (see Table S2). The results showed statistically significant differences between the genders, with females less likely to have been exposed ($ß$ = —1.02, p < 0.001). There were also statistically significant differences according to whether respondents knew about, or had used, a VPN or Tor browser. For example, those who had used those technologies were more likely to have been exposed than those who did not know what they were ($ß = 0.86$, $p < 0.001$). There were no statistically significant differences in exposure between 16- and 17-year-olds or between those of different social grades (see Table S2).

RQ2: *Which media platforms do 16- and 17-year-olds in the United Kingdom use to view pornographic videos or pictures and how recent is the use of each platform for this purpose*?

As Table 1 and Figure 1 show, it is more likely for 16- and 17-year-olds in the United Kingdom to have been exposed, at least once, to sexually explicit porn videos or pictures via social media platforms (63%) or internet search engines (51%) than via dedicated pornographic websites (47%). Conversely, respondents were less likely to have seen pornography on television or DVDs, on messaging apps, or, particularly, on YouTube or e-mail and in magazines than on dedicated pornographic websites.

However, although a greater proportion of 16- and 17-year-olds in the United Kingdom had seen pornography on social media and internet search engines than on dedicated pornographic websites, that exposure was, relative to dedicated pornographic websites, less recent—most commonly 20 days ago. Among those who had visited dedicated pornographic websites, their last visit was, on average, 13 days previously. However, this mean figure has been elevated due to the number of respondents whose last visit was up to 356 days ago. It was most common for 16- and 17-year-olds in the United Kingdom to have visited a dedicated pornographic website the day before they took the survey: the median number of days since the last visit was 1 (see Table 1 and Figure 1). Television or DVDs, search engines, messaging apps, e-mail, and in particular YouTube and magazines, were relatively infrequently used as sources of pornography (see Table 1 and Figure 1).

Our analysis[5] (see Tables S2 and S3) showed statistically significant differences between the genders, with females less likely than males to have seen pornography on dedicated pornographic websites ($ß$ = –1.997, $p < 0.001$), social media ($ß$ = –0.504, $p < 0.001$), search engines ($ß$ = –1.223, $p < 0.001$), YouTube ($ß$ = – 0.492, $p < 0.01$), messaging apps ($ß$ = –0.523, $p < 0.001$) and magazines ($ß$ = –0.432, $p < 0.05$), although not on TV or DVDs and e-mail.[6] There were also statistically significant differences according to whether respondents knew about, or had used, VPNs or Tor browsers. Household social grade made a significant difference to whether respondents had seen pornography on dedicated pornographic websites and YouTube. In the case of dedicated pornographic websites, respondents from households in social grade E were significantly more likely to have been exposed than respondents from the most populous social grade, C1 ($ß$ = 0.74, $p < 0.01$). In the case of YouTube, respondents from households of social grade B were significantly less likely to have been exposed than those from households in the most populous social grade, C1 ($ß$ = –0.489, $p < 0.05$). No differences were found between 16- and 17-year olds.

We found[7] no consistently significant differences between males and females, 16- and 17-year-olds, and respondents from households of different social grades in the recency of their last exposure to pornography via all but one of the listed media platforms. In the case of dedicated pornographic websites, females visited them significantly less frequently than males (see Tables S4, S5, S7, and S8).

RQ3: *How much time do 16- and 17-year-olds in the United Kingdom spend visiting dedicated pornographic websites per month and how is that time split between PCs and mobile devices (smartphones and tablets)*?

The 16- and 17-year-olds in the United Kingdom who visit dedicated pornographic websites say they do so for an average of 2 h 18 min per month. That average is raised by some who reported visiting for much longer. The most common—median—amount of time spent on such sites was 1 h/month.

Our analysis[8] (see Table S6) again showed statistically significant differences between the genders, with females spending significantly less time with dedicated pornographic websites, 88.4 fewer minutes per month (β = —88.4, $p < 0.05$). Parental social grade again also made a significant difference. For example, respondents from households of social grade E spent significantly more time, 127.49 more minutes per month, than respondents from households of the most populous social grade, C1 ($\beta = 127.49$, $p < 0.05$).

Among those who accessed dedicated pornographic websites, the vast majority of time (87% of the time) was spent accessing them via mobile devices, defined as smartphones or tablet computers, rather than via PCs (13% of the time).

RQ4: *What proportions of 16- and 17-year-olds in the United Kingdom are aware of, or have used, a VPN or Tor browser*?

VPNs and Tor browsers enable users to mask their location and, it has been claimed, may provide a means for users to circumvent country-specific controls on online pornography. Among 16- and 17-year-olds in the United Kingdom, 45.7% had used a VPN or Tor browser, 22.9% knew what they were but had not used them, and 31.4% neither knew what they were or had used them.

DISCUSSION

This study's results add to the limited evidence that exists on the prevalence and predictors of pornography use by adolescents in the United Kingdom. It confirms the BBFC's (2020, p. 15) recent finding that around 80% of 16- and 17-year-olds have been exposed to pornography at some point. In line with much of the other research (for a summary, see Peter & Valkenburg, 2016), it also confirms that male adolescents are more likely to have been exposed. We also find that respondents who had used a VPN or Tor browser were more likely to have been exposed, echoing Ševčíková et al. (2014) finding that internet pornography use was higher among those with greater digital skills.

Our results may help to clear up some of the discrepancies that Horvath et al. (2013, p. 22) note regarding the frequency with which young people are exposed to pornography. Recent anecdotal evidence from the United Kingdom (BBFC, 2020, p. 20) had shown exposure could be 'daily' for 'most' 16- to 18-year-old males. This observation is in line with our own results that show that, among the 80.5% of 16- and 17-year-olds who had seen pornography, it was most common (the median value) for their last exposure to have been 0 days ago, with the mean number of days since the last exposure 5.5.

As Nash et al. (2015) have noted, it is 'surprisingly complicated' to determine from the literature the platforms through which children view pornography. Though such data has not been a relevant variable for much previous research, it is highly relevant to the decisions currently being made about the regulation of internet pornography as well as to any future studies that may be carried out on the efficacy of such regulations. Our results confirm (see, e.g., Horvath et al., 2013, p. 24) that the ways in which young people access pornography have changed, with the internet playing a more dominant role. We found magazines were a source for less than a quarter of 16-and 17-year-olds in the United Kingdom and were used very infrequently. Although TV and DVDs were a source for a higher proportion (38%), they came some way behind dedicated pornographic websites (47%), search engines (51%), and in particular social media sites (63%)—although they were on a par with internet messaging services (39%) and ahead of YouTube (24%). That a significant majority of 16- and 17-year-olds in the United Kingdom have come across pornography on social media sites suggests the UK government was right to include such platforms in its latest proposals to reduce children's exposure to legal online pornography.

This data on exposure needs though to be contextualised with reference to how frequently such exposure takes place. Our study has shown that although a higher proportion of 16- and 17-year-olds had seen—at least once—pornography on social media sites than on dedicated porn websites, dedicated porn websites were used much more frequently as a source of pornography than social media sites. Among the 47% who had accessed dedicated porn websites, most commonly (the median value) their last exposure was just 1 day ago, with the mean number of days since last exposure 13 and the monthly visit time 2 h and 18 mins. The frequency with which dedicated pornographic websites are used shows how important such sites—the target of the United Kingdom's original age verification legislation—are as a source of pornography for adolescents. The Online Harms White Paper proposes to regulate companies that 'allow users to share or discover user-generated content or interact with each other online' (HM Government, 2019, p. 8). Though this encompasses popular 'porn-tube' sites, dedicated pornographic websites that only provide professionally made content will not be covered. This exclusion is, in the view of Sarah Connolly, Director, Security and Online Harms at the DCMS, not an issue for concern as she believes that 'in practice, there are very few commercial pornography sites that don't include some elements of user-generated content' (personal communication, 23 June 2020). Rachel Bishop, Deputy Director, Online Harms Policy at the DCMS agrees, adding that the few dedicated pornographic websites that do not include user-generated content present other barriers to children, notably paywalls that require a credit card (personal communication, 9 July 2020).

Although the United Kingdom's original age verification legislation has not been enacted, 'age verification technologies' are still a tool the UK government expects companies may use to 'prevent children from accessing age-inappropriate content' (Gov.uk, 2020). This study is the first to gather data on the proportion of 16- and 17-year-olds in the United Kingdom who have actually used—rather than being simply aware of how to use—workaround technologies, specifically VPNs and the Tor browser, that can be used to circumvent age verification controls. Our findings that 46% were already using these workaround technologies and another 23% were aware of them add weight to concerns that restrictions on the access to legal online pornography imposed by a single country may be circumvented by those the checks are designed to protect.

ACKNOWLEDGMENT

Open Access funding enabled and organized by Projekt DEAL.

CONFLICT OF INTERESTS

The authors declare that there are no conflict of interests.

ENDNOTES

[1] The Market Research Society (MRS) is the United Kingdom's professional body for market researchers. They are not related to YouthSight other than by accrediting them. To receive MRS accreditation, YouthSight have to ensure that all their staff 'understand their responsibilities under the MRS Code of Conduct and have the skills and processes in place to fulfill them'. A variety of steps have to be taken to ensure such understanding, including ensuring that the 'MRS Code of Conduct is written into employee contracts or referred to in the company handbook' (MRS, 2021).

[2] On the basis of data from the United Kingdom's Office for National Statistics.

[3] On the basis of National Readership Survey data on households' chief income earner.

[4] Dedicated pornographic websites, social media, internet search engines, TV or DVDs, messaging apps, YouTube, e-mail, and magazines.

[5] Using logistic regression.

[6] Because of the small proportion of respondents who had seen sexually explicit porn videos or pictures

via e-mail, the results of our analysis of differences within the sample for this media platform should be interpreted with care.

[7] Using both linear regression and Poisson regression with log link and overdispersion.

[8] Using linear regression.

ORCID

Neil Thurman http://orcid.org/0000-0003-3909-9565

REFERENCES

AFP. (1997, November 19). *Vietnam to provide full internet access from December 1.* Nexis online database (subscription only).

Alexa. (2019). The top 500 sites on the Web. https: //www.alexa.com/topsites

Alexandraki, K., Stavropoulos, V., Anderson, E., Latifi, M. Q., & Gomez, R. (2018). Adolescent pornography use: A systematic literature review of research trends 2000-2017. *Current Psychiatry Reviews,* 14(1), 47-58. https://doi.org/10.2174/2211556007666180606073617

Ally, A. K., Lovatt, M., Meier, P. S., Brennan, A., & Holmes, J. (2016). Developing a social practice-based typology of British drinking culture in 2009-2011: Implications for alcohol policy analysis. *Addiction*, *111(9)*, 1568-1579. https://doi.org/10.1111/add.13397

Associated Press. (1995, December 31). *China plans to block sexual materials on Internet.* Nexis online database (subscription only).

BBC News. (2020, January 24). *'Porn Block' Companies Seek £3m in Damages.* BBC News. https://www.bbc.com/news/technology-51235675

Beyens, I., Vandenbosch, L., & Eggermont, S. (2015). Early adolescent boys' exposure to internet pornography: Relationships to pubertal timing, sensation seeking, and academic performance. *Journal of Early Adolescence*, *35*(8), 1045-1068. https://doi.org/10.1177/0272431614548069

Braun, E., & Kayali, L. (2020, July 9). *France to introduce controversial age verification system for adult websites.* Politico. https://www.politico.eu/article/france-to-introduce-controversial-age-verification-system-for-adult-pornography-websites/

British Board of Film Classification (BBFC). (2020, January). Young people, pornography & age-verification. https://www.revealingreality.co.uk/wp-content/uploads/2020/01/BBFC-Young-people-and-pornography-Final-report-2401.pdf

Carlin, J. (1996, June 13). *US Judges Overturn Ban on Internet Porn.* The Independent.

Children's Media Foundation. (2020, April 10). APPG report on online harms. https://www.thechildrensmediafoundation.org/archives/8468/8468

Chorley, M. (2014, March 28). *Age checks needed to access porn, watchdog warns after finding one in 20 visitors to adult sites are under 18.* MailOnline.

Department for Digital, Culture, Media and Sport (DCMS). (2017). Particulars of proposed designation of age-verification regulator. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/669567/particulars_of_proposed_designation_of_age-verification_regulator_-_december_2017.pdf

Doornwaard, S. M., Bickham, D. S., Rich, M., ter Bogt, T. F. M., & van den Eijnden, R. J. J. M. (2015). Adolescents' use of sexually explicit internet material and their sexual attitudes and behavior: Parallel development and directional effects. *Developmental Psychology*, *51*(10), 1476-1488. https://doi.org/10.1037/dev0000040

Elmer-Dewitt, P. (1995, July 3). *Online erotica: On a screen near you.* Time magazine.

Finn, C. (2019, June 19). *Taoiseach says government will review UK's new 'Porn Block' law to see if it could work in Ireland.* TheJournal.ie. https://www.thejournal.ie/ireland-porn-block-law-age-verification-4688853-Jun2019/

Freedom House. (2017). Iceland. https://freedomhouse.org/sites/default/files/FOTN%202017_Iceland.pdf

Freedom House. (2019a). United Arab Emirates. https://freedomhouse.org/country/united-arab-emirates/freedom-net/201 9

Freedom House. (2019b). Uzbekistan. https://freedomhouse.org/country/uzbekistan/freedom-net/2019

Freedom House. (2019c). Pakistan. https://freedomhouse.org/country/pakistan/freedom-net/2019

Gardner, W., Mulvey, E. P., & Shaw, E. C. (1995). Regression analyses of counts and rates: Poisson, overdispersed Poisson, and negative binomial models. *Psychological Bulletin*, *118*(3), 392-404.

Gayle, D. (2018, October 18). *Millions of porn videos will not be blocked by UK online age checks.* The Guardian. https://www.theguardian.com/technology/2018/oct/18/millions-of-pom-videos-will-not-blocked-uk-online-age-checks

Geiger, G. (2020, October 26). *German authorities want to implement DNS blocks against major porn sites.* Motherboard. https://www.vice.com/en/article/bvx8v4/german-authorities-want-to-implement-dns-blocks-against-major-porn-sites

Gov.uk. (2020). Online Harms White Paper—Initial consultation response. https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

Hardy, S. A., Steelman, M. A., Coyne, S. M., & Ridge, R. D. (2013). Adolescent religiousness as a protective factor against pornography use. *Journal of Applied Developmental Psychology*, *34*(3), 131-139. https://doi.org/10.1016/j.appdev.2012.12.002

Harper, C., & Hodgins, D. C. (2016). Examining correlates of problematic Internet pornography use among university students. *Journal of Behavioral Addictions*, *5*(2), 179-191.

HM Government. (2019, April). Online Harms White Paper. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Horvath, M. A. H., Alys, L., Massey, K., Pina, A., Scally, M., & Adler, J. R. (2013). *Basically... porn is everywhere: A rapid evidence assessment on the effects that access and exposure to pornography has on children and young people (Project Report).* Office of the Children's Commissioner for England. http://eprints.mdx.ac.uk/10692/

Kelion, L. (2017, July 17). *Porn ID checks set to start in April 2018.* BBC News. https://www.bbc.co.uk/news/technology-40630582

Kleinman, Z. (2018, March 12). *Online porn age checks delayed in UK.* BBC News. https://www.bbc.co.uk/news/technology-43370999

Kohut, T., Balzarini, R. N., Fisher, W. A., Grubbs, J. B., Campbell, L., & Prause, N. (2020). Surveying pornography use: A shaky science resting on poor measurement foundations. *Journal of Sex Research*, *57*(6), 722-742.

Ma, C. M. S., Shek, D. T. L., & Lai, C. C. W. (2017). Individual differences in intentional and unintentional exposure to online pornography among Hong Kong Chinese adolescents. *International Journal on Disability and Human Development*, *16*(4), 417-423.

Market Research Society (MRS). (2014). MRS guidelines for research with children and young people. https://www.mrs.org.uk/pdf/2014-09-01Children%20and%20Young%20People%20Research%20Guidelines.pdf

Market Research Society (MRS). (2021). How to join. https://www.mrs.org.uk/company-partner/how-to-join

Matthews-King, A. (2018, November 13). *Porn site age verification to be in force by spring next year after delays, minister says.* The Independent. https://www.independent.co.uk/news/uk/home-news/porn-site-age-verification-uk-pornhub-sex-online-adult-video-government-id-a8631886.html

McCullagh, P., & Nelder, J. A. (1989). *Generalized linear models.* Chapman and Hall.

Morgan, N. (2019). Online harms: Written Statement-HLWS12. https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2019-10-16/HLWS12/

Nair, A. (2019). *The regulation of Internet pornography: Issues and challenges.* Routledge.

Nash, V., Adler, J. R., Horvath, M. A. H., Livingstone, S., Marston, C., Owen, G., & Wright, J. (2015). *Identifying the routes by which children view pornography online: Implications for future policy-makers seeking to limit viewing.* Department for Culture, Media and Sport. http://eprints.lse.ac.uk/65450/

OFLC. (2018). NZ youth and porn: Research findings of a survey on how and why young New Zealanders view online pornography. https://www.classificationoffice.govt.nz/assets/PDFs/NZYouthPom-OFLC-December2018- PrintVersion.pdf

Parliament of Canada. (2020). S-203. https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E%26billId=10873545

Peter, J., & Valkenburg, P. M. (2016). Adolescents and pornography: A review of 20 years of research. *Journal of Sex Research*, *53*(4-5), 509-531.

R Core Team. (2018). *R: A language and environment for statistical computing.* R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

Radio New Zealand. (2018, August 10). Systems needed to protect children from online porn, MP says. https://www.rnz.co.nz/news/political/363796/systems-needed-to-protect-children-from-online-porn-mp-says

Ševčíková, A., Šerek, J., Barbovschi, & Daneback, K. (2014). The roles of individual characteristics and liberalism in intentional and unintentional exposure to online sexual material among European youth: A multilevel approach. *Sexuality Research and Social*

Policy, *11*(2), 104-115. https://doi.org/10.1007/s13178-013-0141-6

Svedin, C. G., Akerman, I., & Priebe, G. (2011). Frequent users of pornography. A population-based epidemiological study of Swedish male adolescents. *Journal of Adolescence*, *34*(4), 779-788. https://doi.org/10.1016/j.adolescence.2010.04.010

Taylor, J. (2020, March 5). *Australia could implement mandatory age verification for pornography websites.* The Guardian. https://www.theguardian.com/culture/2020/mar/05/australia-could-implement-mandatory-age-verification-for-online-pornography-sites

van Ouytsel, J., Ponnet, K., & Walrave, M. (2014). The associations between adolescents' consumption of pornography and music videos and their sexting behavior. *Cyberpsychology, Behavior and Social Networking*, *17*(12), 772-778. https://doi.org/10.1089/cyber.2014.0365

Wake, D. (2009, June 23). *Children at risk from online porn, says film censor.* Press Association Mediapoint. Nexis online database (subscription only).

Waterson, J., & Hem, A. (2019, June 20). *UK age-verification system for porn delayed by six months.* The Guardian. https://www.theguardian.com/technology/2019/jun/20/uks-porn-age-verification-system-to-be-delayed-indefinitely

Wheeler, B. (2018, January 5). *Porn age-checks risk pushing children to dark web, officials warn.* BBC News. https://www.bbc.co.uk/news/uk-politics-42577460

Wright, P. J., Herbenick, D., & Paul, B. (2020). Adolescent condom use, parent-adolescent sexual health communication, and pornography: Findings from a US probability sample. *Health Communication*, *35*(13), 1-7. https://doi.org/10.1080/10410236.2019.1652392

Yagielowicz, S. (2019, December 23). *Poland becomes newest nation to explore online age verification.* Xbiz. https://www.xbiz.com/news/249192/poland-becomes-newest-nation-to-explore-online-age-verification

YouthSight. (2018). *Panel book.* https://www.youthsight.com/download-panel-book-2018-youthsight

SUPPORTING INFORMATION

Additional Supporting Information may be found online in the supporting information tab for this article.

How to cite this article: Thurman, N., & Obster, F. (2021). The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches. *Policy Internet,* 13, 415-432. https://doi.org/10.1002/poi3.250

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No.: 1:23-cv-917

FREE SPEECH COALITION, INC., MG PREMIUM LTD,
MG FREESITES LTD, WEBGROUP CZECH REPUBLIC,
A.S., NKL ASSOCIATES, S.R.O.,
SONESTA TECHNOLOGIES, S.R.O., SONESTA MEDIA,
S.R.O., YELLOW PRODUCTION S.R.O., PAPER STREET
MEDIA, LLC, NEPTUNE MEDIA, LLC, JANE DOE,
MEDIAME SRL, MIDUS HOLDINGS, INC.,

Plaintiffs,

vs.

ANGELA COLMENERO, in her Official Capacity as
Interim Attorney General for the State of Texas,

Defendant.

DECLARATION OF RICHARD L. SONNIER III IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

DECLARATION OF RICHARD L SONNIER III

I, Richard L Sonnier III, declare as follows:

1. I have been retained by Plaintiffs in the above captioned matter to provide technical expertise in the areas of Internet technologies and operations including age verification of users, content filtering, parental controls, family safe usage, the cost of implementing Internet technologies, the cost of operating Internet

technologies, Internet privacy, Internet standards, cybersecurity, and Internet regulations.

2. My rate for time spent preparing this declaration and for the testimony in this matter is $350 per hour.

3. My compensation in no way depends on the outcome of this litigation or the testimony or opinions that I express.

I. BACKGROUND & EXPERIENCE

4. My qualifications as an expert witness can be found in Exhibit A, which includes my CV and a list of my publications and previous testimony.

II. SUMMARY AND SCOPE OF OPINIONS

5. In my opinion, Internet age verification as required by the State of Texas (and various other US state governments) has numerous problems; and Internet content filtering is a superior solution to achieve the apparent objectives of age verification.

III. MATERIALS CONSIDERED

6. In forming the opinions expressed in this declaration, I considered and relied on my education, experience, and knowledge of the relevant fields. I also reviewed and considered the materials listed in Exhibit B.

7. I reserve the right to rely on any other information, deposition testimony, trial testimony, documents, or materials that may be provided to me or that witnesses at trial rely on if called to testify about any aspect of this matter.

IV. INTERNET TECHNOLOGIES

8. To explain the Internet technologies, I will relate them by analogy to physical postal mail. However, like

all analogies, this is imperfect. At the technical level, the operations of the physical world—that is, items or products moving through time and space between producers and consumers—are fundamentally different from the movement of services or virtual products over the Internet. All too often parties apply physical world rules, regulations, and processes to Internet commerce.

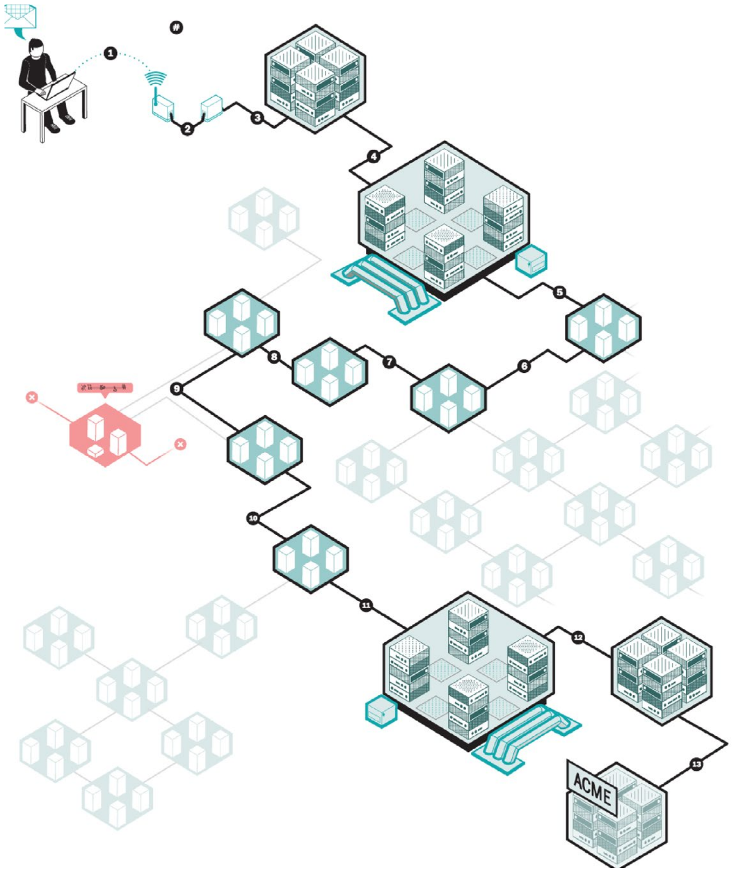
9. Physical postal mail works as follows:

Steps	**Internet Analogy**
Write the letter	Create content
Insert the letter in the envelope	Wrap the content in a packet
Address the envelope	Address by putting the sender and recipient computer locations on the Internet into the packet
Hand off to the postal service	Insert the packet into the Internet
Route through the postal service network	Route through the Internet
Delivery to addressee	Deliver to the computer location of the recipient
Open the envelope	Open the packet on that computer
Extract the letter	Extract the content

Read the letter	Use the content e.g., display it on the computer screen
If needed, reply to the letter using the return address by repeating all steps from the top	If needed, use the sender's computer location to reply by repeating all steps from the top

10. To extend the analogy further, the routing of a packet through the Internet is like the routing of an envelope through the postal service network. The packet will go through several intermediate Internet locations before reaching the recipient's computer location. At each of these intermediate locations, the recipient's computer location will be read from the packet and used to determine the next location on the way to the recipient's computer location— just like the envelope goes from postal office to postal office on its way to the addressee. In both cases, this routing can be quite complex. For example, here is an illustration from the Washington Post, May 31, 2015, showing Internet routing (each numbered black circle indicates a step in the routing)[1]:

[1] https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/



11. If you were sending a highly confidential letter, you might hire a representative, a proxy, near the addressee and place the addressed envelope into a secure box with a combination lock. Then you would address the secure box for delivery to your proxy, with instructions to deliver it in person to the addressee. And you would provide the combination lock code to the addressee via a phone call, but not to your proxy. When the proxy delivers the secure box to the addressee, this ensures that no other parties except you and your addressee can read the letter and that it has not been altered. For the Internet, you can have

the same assurance for your content by using encryption.

12. To understand how the Internet works, it helps to understand its history. The Internet was designed for the US Department of Defense to enable command and control communications within the military even in the event of a nuclear war that has destroyed the traditional centralized telephone and other communication systems. Thus, at its core the Internet is resilient in the face of damage. The Internet is designed to be highly adaptable. This makes the Internet resistant to traditional censorship and regulation. "[A]s Internet pioneer John Gilmore puts it, 'The Net [Internet] interprets censorship as damage and routes around it.'" *See* Exhibit C: the Time magazine article "First Nation in Cyberspace," Dec. 6, 1993.

V INTERNET AGE VERIFICATION

13. Internet age verification is a set of techniques to determine the age or likely age of a consumer interacting with a commercial website. The website could be selling products or services that require a minimum age, like tobacco products or online gambling; or the website could provide adult content, e.g., sexual material. Chelsea Jarvie and Karen Renaud presented an excellent summary of the current state of Internet age verification at the Dewald Roode Information Security Research Workshop, San Antonio, Texas in 2021, in their presentation and paper titled "Are you over 18? A Snapshot of Current Age Verification Mechanisms." *See* Exhibit D. Jarvie and Renaud examined 1119 papers from academic databases and the Internet to find 35 papers that were relevant to the Internet age verification between the years 2011 and 2021. Jarvie and Renaud determined

from their review of the Internet age verification literature that such techniques should meet the following objectives: 1) Effective & Inclusive, 2) Affordable, 3) Privacy Preserving.

14. They further found Internet age verification techniques that require a copy of a government issued ID to be "highly privacy invasive." They also found assumptions that minors will not have access to credit cards or "their parents' identity documents" to be incorrect.

15. Jarvie and Renaud compiled a table of available commercial Internet age verification techniques:

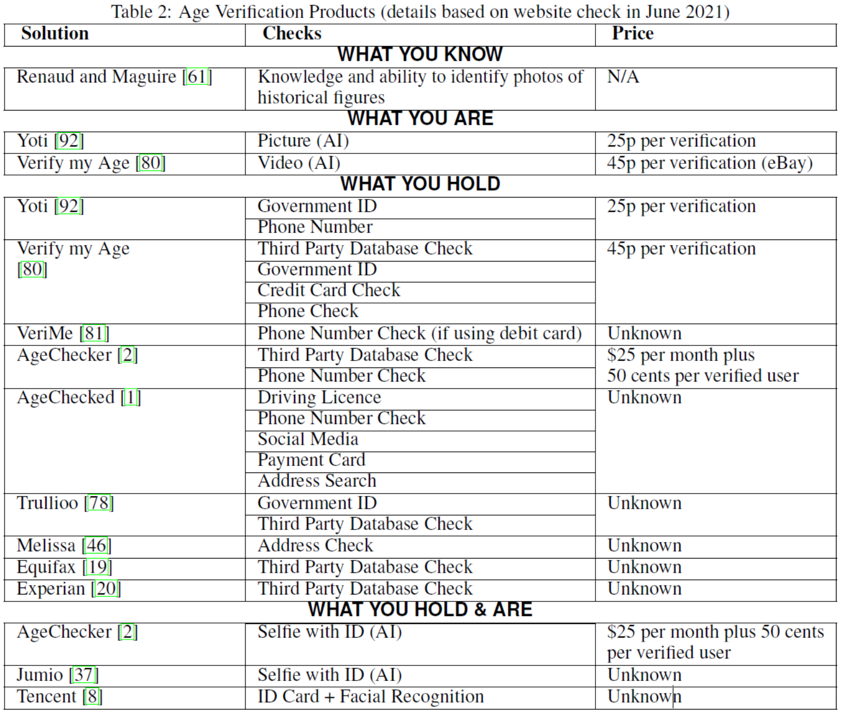


Table 2: Age Verification Products (details based on website check in June 2021)

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

16. Regarding the three objectives of Internet age verification vis-à-vis the available techniques, Jarvie and Renaud concluded:

> 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.

17. In my opinion, it makes sense that Jarvie and Renaud found that Internet age verification fails the key objectives. Due to the nature of current Internet technologies, Internet age verification is trying to solve the problem of limiting access to age restricted websites in the wrong place and with the wrong toolset.

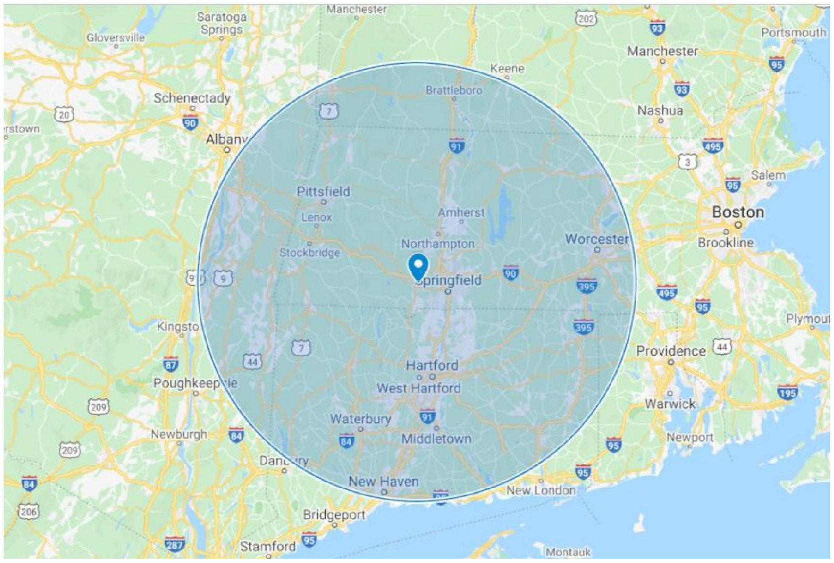
VI ISSUES WITH INTERNET AGE VERIFICATION

18. The nature of the Internet (as discussed above) suggests that current Internet age verification technology will not work, and this is in fact the case. First,

an Internet website cannot accurately and consistently determine the geographical location of its user. To apply the age restrictions for a particular state, a website must determine if the user is in that state. However, there is no mechanism to reliably do that. What is sometimes called the "geolocation" of the user is nothing of the sort; instead, it is the last known geolocation of the computer connecting to the website based on that computer's Internet address. Various service providers of geolocation information compile large databases of Internet addresses and their approximate or best guess geolocation in the world. In large part, these geolocation service providers rely on information reported by Internet Service Providers, registries of Internet addresses, as well as big data methods. MaxMind, Inc., one the major geolocation service providers, describes it this way:

> All of our IP geolocation data comes with an accuracy radius field. The actual geolocation of the IP address is likely within the circle with its center at the geolocation coordinates and a radius equal to the accuracy radius field. While the pin on the map might lead us to think that the IP address is close to the center of this circle, in reality we're defining a region in which the IP address is very likely to be.

Thus, the first step in applying the correct state age verification law rests on a guess of where the user "is very likely to be." MaxMind provides this example of an accuracy radius field:



So, an Internet website receives a connection from an IP address and asks MaxMind for its geolocation; and the website gets this circle from MaxMind with the assurance that the user's IP address is "very likely" in this circle. However, that circle includes parts of Connecticut, Vermont, Rhode Island, New Hampshire, Massachusetts, and New York. The website cannot apply the applicable state age verification law, if any, because it does not know in which state the user is located.

19. IP Location provides an Internet website that allows you to lookup the geolocation of an IP address in multiple services at the same time. For example, I disconnected my Verizon cell phone from my office Wi-Fi and then looked-up the IP address that Verizon assigned to my phone on the IP Location website. My cell phone's IP address was 174.203.0.3 and IP Location returned the following possible locations from the various geolocation providers: Beaumont, Texas; Houston, Texas; New York, New York; Baton

Rouge, Louisiana; Ashburn, Virginia; Houston, Texas; Ashburn, Virginia; and Houston, Texas. At the time, my cell phone was in the zip code 77018 in which encompasses Houston, Texas. Thus, three of the eight geolocation services identified the correct city and state and one more identified the correct state but was off by approximately 78 miles. However, the other four services failed to identify the correct city or state, with one missing my cell phone's location by approximately 1420 miles IP Location explains that the accuracy of geolocation from IP addresses is the result of many factors.[2] IP Location cites a rough measure of geolocation accuracy based on the claims of the providers: the country of the IP address is accurate between 95% and 99%, the accuracy of the region or state of the IP address is between 55% and 80%, and the accuracy of the city of the IP address is between 50% and 75%. However, IP Location warns "the actual result may vary from provider to provider," and that the geolocations of cell phones may be less accurate than those for home computers. IP Location's estimate of accuracy matches with my test results where the city was accurate for 38% of the providers, the state was accurate for 50% of the providers, and the country was accurate for 100% of the providers.

20. The accuracy of the geolocation of IP addresses is limited by the nature of the Internet. A block of IP addresses is assigned to the Internet Service Provider (ISP) and that ISP has flexibility to assign each address to a user's device. Depending on the network technology of the ISP and the implementation choices they make, that block of addresses could be assigned to user's devices over a small geographic area or a very

[2] https://www.iplocation.net/geolocation-accuracy

large one. Within those areas, any address can be dynamically assigned to many different user's devices over time. The IP address can easily, and often does, change each day. The geolocation providers compile the address blocks assigned to each ISP and then make determinations of likely geographic service area for that block. They then report the geolocation as the center of that service area and provide a confidence window for the entire area.

21. In the context of cell phones and cellular networks, the accuracy of geolocation can degrade quite a bit, because the large national carriers like Verizon have very large IP address blocks, which can be assigned over very large, multistate service areas or even the entire country. For example, I have traveled with a Verizon mobile hot-spot in a car from Virginia through Tennessee, Alabama, Georgia, Mississippi to Louisiana. The IP address assigned to the hot-spot rarely changed, despite my going in and out of the range of numerous cell phone communication towers. During this trip, my geolocation was changing continuously but my IP address was not.

22. Another example of the issues with geolocation was reported by a Verizon cell phone user trying to listen to Philadelphia Phillies games over his cell phone. The user reports that sometimes his listening is blocked because although he is located in Delaware, which is in the designated market area for the Phillies games, his cell phone gets assigned an IP address located in York, PA, which is not. When this happens, the cell phone is blocked from playing the game audio.[3]

[3] https://community.verizon.com/t5/Other-Network-Discussions/How-are-IP-addresses-assigned-for-phones/td-p/1254931

VII YOU CAN BE ANYWHERE YOU WANT TO BE

23. As I noted above, physical-world rules about where an individual is located don't apply to Internet commerce. Since the Internet fundamentally does not know where the user is in the world and, by design, does not care for its proper function, the user can appear to be pretty much anywhere in the world they would like to be. There are numerous mechanisms to achieve this: proxy servers, virtual private networks (VPNs), virtual desktops, remote desktop access, the Orion Router (TOR), and peer to peer networking or decentralized websites. Before going into the specifics of each of these technologies, I should point out they were all created to solve legitimate Internet problems dealing with security, privacy, and efficiency. They were not created to evade state law or facilitate criminal activity. Internet technologies are neutral, but Internet users vary. For example, TOR was created by researchers at the Center for High Assurance Computer Systems, Naval Research Laboratory, Washington; and, disclosed to the public in a January 28, 1999, paper. *See* Exhibit E. Its purpose was private communications over public networks like the Internet. Today, many security professionals consider TOR a security risk, the playground of hackers, and part of or a gateway to the dark web.

24. Going back to the postal email analogy described above, a proxy server is like using a private postal service for your mail. You don't give anyone your real address, instead you provide the private service's postal address, and the private service picks up your outbound mail and delivers any mail it receives for you. To the world, your real location is hidden by the private postal service. Similarly, a proxy server on the Internet will hide your computer's IP address from any

website. Instead, the website will see the IP address of the proxy server. For example, ProxyScrape provides a list of free proxy servers, and faster and safer ones for a small fee. One of the free proxy servers was geolocated by MaxMind as "very likely to be" in Los Angeles, California, so a user in a state with restrictive laws could use it to fall under California law instead. ProxyScrape offers proxy servers in 129 countries around the world, so you can be almost anywhere you want to be.

25. Just like proxy servers, VPNs hide your actual IP address from the Internet website by presenting the IP address from the VPN instead. The major difference is that all the communication between your computer and the VPN is fully encrypted, which may not be true for a proxy server. Another difference is that some Internet activity may not work through a proxy server, whereas VPNs will support any type of Internet activity. Certain proxy servers are free. Similarly, VPNs, which are easy to set up, either come at no charge (such as Proton VPN), or at a minimal cost, such as ExpressVPN, which offers a free trial period of 30-days, charges $12.95 per month, and allows you to "be" in 94 countries. Furthermore, within the USA, you can choose to be in 15 different states. There are many competing VPN services, so if ExpressVPN does not support a chosen location, there is a good chance another service will. For example, if you want to be from Texas and ExpressVPN cannot support you, its competitor VyprVPN will. Another low-cost VPN service is offered by Mozilla Firefox[4] for $5 per month. It is called Mozilla VPN and offers IP addresses in 30

[4] https://www.mozilla.org/en-US/firefox/

countries.[5] Furthermore, VPN services customarily offer free trial options, thus allowing users to switch from one free trial offer to another to avoid incurring charges.

26. Virtual desktops became widely used during the COVID-19 period when most companies had their employees work from home. Virtual desktops are analogous to your private postal service providing you direct access to a computer in their office where you can create and print your mail and they will scan onto that computer any mail you receive. Thus, you can be anywhere, and connect to the private service computer over the Internet. The virtual desktop has a public address that any website you access from the virtual desktop will see. While widely used by businesses, virtual desktops are now offered to individuals and students at very low cost, similarly to VPNs. For example, Shells.com offers virtual desktops for $5 per month and is rated "extremely easy to use" by TechRadar.[6] Shells.com virtual desktops can be accessed from many devices, including PCs, smart phones, and tablets. Shells.com highlights a "Browser in the Cloud" solution that would certainly allow users to view adult content without restrictions.[7] Shells.com offers six locations outside Texas. Alternatively, Amazon WorkSpaces is a virtual desktop with many more features and costs as low as $7.25 per month, plus $0.19 per hour of active use. Amazon offers the service from approximately 15 locations around the world, so your website access would come from one of those locations.

[5] https://www.mozilla.org/en-US/products/vpn/features/

[6] https://www.techradar.com/best/virtual-desktop-services

[7] https://www.shells.com/l/en-US/browser-in-the-cloud

27. Remote desktops are similar to virtual desktops. Both allow the user to securely connect to a remote computer, and the user's website access then appears to come from that remote computer's IP address. The differences are 1) the remote computer is your computer, or a computer controlled by you, 2) you must install the remote desktop access software both your computer and the remote computer, and 3) free versions of the software are available for personal use. For example, suppose you are a 17-year-old student at the University of Texas in Austin, TX, living in the dorms on campus with a laptop; but your home is in Boston, Massachusetts where you have a desktop PC. You can install the remote desktop access software on both computers and then use your laptop in Austin to connect to the desktop in Boston. Now, the you can access a website from the laptop in Texas while appearing to be in Massachusetts. One example of this type of software is TeamViewer, which is free for personal use.

28. TOR is another tool that permits users to conceal their true location. TOR is maintained by a non-profit corporation, the Tor Project, which creates the software, distributes it, and supports it. TOR software is free. The TOR network consists of thousands of relays run by volunteers around the world. TOR will hide your computer's IP address, and the website will see the IP address of the last TOR relay instead. Unlike VPNs, TOR protects from "man in the middle" attacks. With a VPN, the VPN service is the man in the middle. If the VPN service is not trustworthy or is compromised by criminals or some government, then the VPN offers no security at all. TOR protects against this by using at least 3 relays on the path from your computer to the destination website where each relay knows the previous node and the next node in the

path. TOR's objective is to work around censorship and government restrictions so it will allow a user to bypass them, e.g., age verification laws. TOR is like my postal letter analogy using a proxy and secure box, except TOR uses at least three proxies together with an equal number of secure boxes nested inside one another. TOR can even circumvent the Great Firewall: part of China's much stricter laws on Internet usage. For TOR to be effective, it needs to be easy to use. As Autumn Skerritt, a Software Engineer at Cisco/Duo, puts it:

> Tor needs a lot of users to create anonymity, if Tor was hard to use new users wouldn't adopt it so quickly. Because new users won't adopt it, Tor becomes less anonymous. By this reasoning, it is easy to see that usability isn't just a design choice of Tor but a security requirement to make Tor more secure.

To that end, the Tor Project makes it easy to use TOR by providing a custom web browser pre-configured to use it as a simple download. Once installed, you can browse via TOR. To be a TOR relay is also simple if you have a suitable server and Internet bandwidth. For example, on a Linux server, it takes just 7 steps.[8]

29. These Internet technologies can be combined to avoid age verification. For example, VPNs can be used in combination with all the others.

VIII PEER-TO-PEER NETWORKS

30. Peer-to-peer networking avoids age verification law in an entirely different way. With peer-to-peer networking, there is no website delivering adult content. At most, there is an indexing website that

[8] https://community.torproject.org/relay/setup/guard/centos-rhel/

provides a list of the content available via the peer-to-peer network. The network is a collection of computers that have some portion of the content. It is a form of file sharing that is decentralized. There is not one website server sharing the content, but rather an army of ordinary user computers providing portions of it. Thus, there is no website landing page on which required notices can be displayed or where age verification can be enforced. Instead, the website just provides peer-to-peer networking instructions to access the content on that network with a network client application, not a web browser. For example, a very popular peer-to-peer network is Torrents, which uses the BitTorrent protocol. The software is free, with faster and enhanced versions available for a fee.

31. In my opinion, if Internet age verification laws become more common, workarounds like peer-to-peer networking will become much more prevalent.[9]

VIII INTERNET CONTENT FILTERING

32. Internet content filtering is a superior alternative to Internet age verification. In fact, controlling access to adult content has been a high priority for Internet content filtering from the beginning, and remains in high demand by large enterprises. Thus, despite the rapid evolution of the Internet, Internet content filtering has kept up with the changes. Internet content filtering is a critical component of cyber security for any computer or device with Internet access, and has long included filtering of adult content. Therefore, it is not surprising that Internet content filtering works better than Internet age verification for restricting access to adult content by minors.

[9] https://adultblog.io/best-porn-torrent-sites/

33. Internet content filtering can be implemented at many levels such as at the ISP, at the home router, or at the user device, to provide an in-depth defense against malicious or unwanted Internet content. There are thus many avenues to use to block adult content from reaching minors. Further, Internet content filtering is tunable. For example, many of my corporate clients block gambling and firearm websites, along with adult content, while many families allow gambling and firearm websites and block adult content only.

34. Internet content filtering is widely available at no additional cost with an Internet connection, in the Internet router or firewall, and built-in to the software of many computers and devices. More advanced content filtering can be purchased at various price points. Thus, Interne content filtering is available that fits most user needs and budgets.

35. Some of the latest Internet technologies, such as Domain Name System (DNS) filtering and artificial intelligence (AI), are being applied to Internet content filtering, thus improving accuracy. DNS is the phonebook of the Internet, where you can look up the address of any website or other Internet service. By examining the content of each website in DNS and then categorizing it, DNS filtering allows the user to block or allow websites based on their categories. This filtering is dynamic in that once the user blocks a category like adult content, the DNS filtering services constantly scans the Internet and updates that category with the latest websites. Uncategorized websites can be blocked as well, to address the fact that newly registered websites are the most common source of malware, viruses, and other malicious content. For example, DNSFilter, one commercial provider of DNS filtering, will upon receiving a request

to access an uncategorized website from a user initiate a real-time scan of that website's content through its AI engine to classify and determine if it is in one of the allowed categories for the user.[10] Because of its large infrastructure and investment in technology, this can be done without disrupting the user's work, e.g. with very little time delay from the user's perspective. For families, Cisco Systems, one of the largest companies for Internet technologies, provides DNS filtering free of charge via its OpenDNS FamilyShield service.[11]

36. Internet content filtering is embedded in many Internet access routers. A recent list of them is available with reviews from Lifewire, a well-known website promoting easy to us technology.[12] The best overall router was the Synology RT2600ac Dual-Band Gigabit Wi-Fi Router, available from Amazon for $150. The Lifewire reviewers found the parental controls on this device to be easy to adjust, such that parents with multiple children can tune the filtering to age appropriate levels for each minor in the household as well as configure default filtering for the entire home network, including guests.

37. Microsoft provides parental controls in its products and offers the Microsoft Family Safety service in both free and paid versions.[13] The free version includes "Web and search filters" as well as

[10] https://help.dnsfilter.com/hc/en-us/articles/1500008108542-uncategorized-sites

[11] https://signup.opendns.com/familyshield/

[12] https://www.lifewire.com/best-parental-control-routers-4160776

[13] https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344

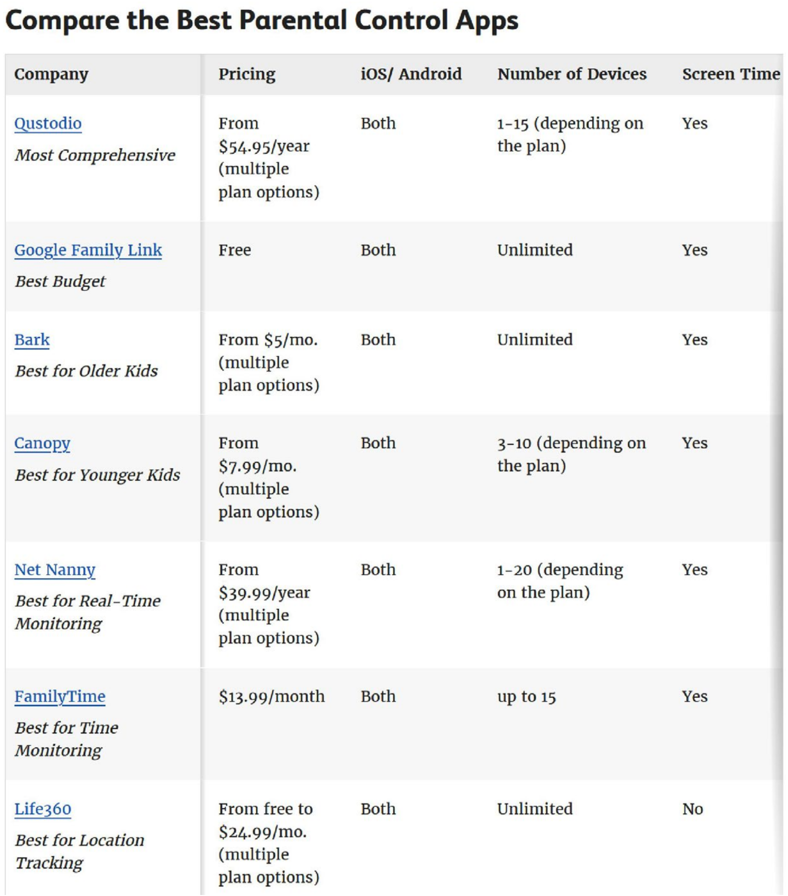
"App and game filters."[14] Apps and games can be another avenue to adult content on the Internet that can be controlled through these parental control tools. Similarly, Apple offers parental controls with its products such as the iPad or iPhone that include the option: "Limit Adult Websites."[15]

38. There also are technical solutions to make Internet content filtering easy for busy parents or those who are not technology savvy, including to manage the filtering on different devices that may have different parental control capabilities. The industry has developed a solution for this in the form of combo applications often called "Parental Control Apps," which provide the user with a single interface to manage Internet content filtering. Here is one list of such applications by Verywell Family[16]:

[14] https://www.microsoft.com/en-us/microsoft-365/family-safety?ocid=cmmy4tuo5qp

[15] https://support.apple.com/en-us/HT201304

[16] https://www.verywellfamily.com/best-parental-control-apps-4779963#toc-compare-the-best-parental-control-apps



Compare the Best Parental Control Apps

Company	Pricing	iOS/ Android	Number of Devices	Screen Time
Qustodio *Most Comprehensive*	From $54.95/year (multiple plan options)	Both	1-15 (depending on the plan)	Yes
Google Family Link *Best Budget*	Free	Both	Unlimited	Yes
Bark *Best for Older Kids*	From $5/mo. (multiple plan options)	Both	Unlimited	Yes
Canopy *Best for Younger Kids*	From $7.99/mo. (multiple plan options)	Both	3-10 (depending on the plan)	Yes
Net Nanny *Best for Real-Time Monitoring*	From $39.99/year (multiple plan options)	Both	1-20 (depending on the plan)	Yes
FamilyTime *Best for Time Monitoring*	$13.99/month	Both	up to 15	Yes
Life360 *Best for Location Tracking*	From free to $24.99/mo. (multiple plan options)	Both	Unlimited	No

One aspect of parental control applications is that they monitor the Internet content access and keep a history of websites visited, often including snapshots for parental review. Monitoring allows the parents or guardians who supervise the minor's activities to calibrate their preferences for protecting the minors, making a family-by-family, case-by-case determination according to the items of risk or that are concerning to them. One-size-fits-all-restrictions may not meet the needs within or across households.

39. Most of the Internet content filtering provided by these parental control applications is dynamic, in that parents select specific categories of websites to block. These applications will analyze each website and then the software will apply the category rules the parents have selected. For example, Qustodio says "Qustodio analyzes the content of each page each time it is visited. It then decides if the content is unsafe or suspicious, according to the rules you have set, and applies a category to that page. This process is continuously tested and improved."[17] Another example, Canopy, says "Our patented SafeSmart Internet Filter uses artificial intelligence to scan, detect, and eliminate explicit content on web browsers and many popular apps in milliseconds, before it reaches their screen" and specifies that it "makes real-time decisions about content, doesn't rely on an incomplete or outdated list of inappropriate sites."[18] Thus, these applications operate dynamically similar to DNSFilter as explained above. Additionally, Canopy works on all children's devices, including phones, tablets and computers, as does Qustodio.[19]

X INTERNET SEARCH ENGINES

40. Search engines, such as Bing.com, scan most Internet content so that users can search for it. Since search engines scan adult content and most users don't want such content in their results, search engines developed mechanisms to identify adult content and filter it out of their search results, depending on the level of "safe search" options a user

[17] https://help.qustodio.com/hc/en-us/articles/360005216237-Qustodio-is-not-correctly-classifying-a-website

[18] https://canopy.us/parental-control-app-technology/

[19] https://www.qustodio.com/en/

selects. There are many types of content that need to be identified and filtered out like malware, viruses, scams, frauds, and other malicious Internet content.

41. Many Internet search engines allow users to specifically search for images and videos and to easily change their level of "search safety." Thus, by simply turning off all "safe search" filters and performing a video search with the search terms "hot sex," the result I got is that Bing.com displays sexual material, i.e., adult content videos. Absent content filtering software, which typically forces the "safe search" filters of search engines into their most protective settings, any minor users would get adult content by simply running a search.

XII LACK OF BATTLE TESTED INTERNET AGE VERIFICATION CONSIDERING THE RISKS

42. Given that Internet age verification requires or at least recommends as a first or an enumerate choice the capturing of a government-issued ID, like a state driver's license or US passport, and that such documents are high value targets for many criminals, the risks to users of such age verification is very high. Internet age verification should be subjected to the same sort of extensive process as, for example, national encryption standards. There should be complete transparency of the algorithms, techniques and operating procedures including reference implementations suitable for testing by security researchers.

43. Considering the history of the SSL/TLS encryption network, the most widely used security on the Internet, shows 1) it takes the time to get security right, 2) major vulnerabilities are essentially inevitable, 3) it is a costly endeavor to maintain effective security. SSL 2.0 was widely deployed in 1995 to address the

security needs of the Internet, only to be revised a year later as SSL 3.0 to address vulnerabilities in SSL 2.0. Then in 2014, a major security vulnerability, POODLE, was found in SSL 3.0, forcing an Internet-wide migration effort to TLS that was very costly to both providers and users. Millions and millions of devices had to be upgraded. Older devices require manual effort by technicians to upgrade firmware or software and manually disable the badly broken SSL 3.0; in some cases, the devices could not be fixed and had to be replaced entirely.

XIV CONCLUSIONS

44. I conclude, as explained above, current Internet age verification technologies have little to no efficacy, including because they are easily circumvented by minors and carry significant risks to the privacy of personal information.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 1st day of August 2023 in Huston, Texas.

/s/ Richard L Sonnier III
RICHARD L SONNIER III

EXHIBIT A

Curriculum Vitae

Richard L Sonnier III

Houston, TX

PH: 281-445-4800

Email: rsonnier@nimbleservices.com

SUMMARY OF QUALIFICATIONS

I bring over 35 years of experience and skill to Nimble Services' customers who need cost effective computer systems and networks. I create solutions across a multitude of computer platforms and network technologies and focus on solutions with longevity based on industry standard technology.

Analyze and Design

- High performance computer infrastructures integrated with legacy systems
- High speed LANs/WANs/SANs and client/server architectures using Ethernet (10/100/1000) Switches, Routers, TCP/IP, Frame Relay, T1/T3, FDDI, Fibre Channel, TCP/IP, and the Internet
- Complex software systems including software architecture, performance tuning, source code analysis and migration from old to new platforms

Secure

- Computer security including audit preparation, audit remediation, penetration testing, policies and procedures

Integrate

- UNIX, NT, Solaris, HP-UX, AIX, IRIX, SCO, Digital UNIX, UNICOS, MPE/iX, MVS, Linux, and Windows networks into coherent company information system
- Standard and custom solutions with BMC ASA software: Patrol, BEST/1, SQL*Backtrack

Implement

- Computer systems management including policies, procedures, knowledge transfer, and products
- Network services: distributed backup, network printing, E-mail, security, universal file and data access, ORACLE, SQL Server, AFS, NFS, DFS, Samba, www, ftp, and high availability servers

Troubleshoot

- All aspects of complex networked systems focusing on increased performance and seamless ease of use

Develop

- Complex software systems including software architecture and design
- Custom system services and applications to provide complete computing environment in C, C++, C#, FORTRAN, Visual BASIC, Pascal, LISP, Korn, Perl, TCL/TK, SQL, NT Batch, Java, JavaScript, PowerShell, Python, Zig and Go.

Manage

- Complex software systems design and development projects

- Complex systems integration and management projects

BIOGRAPHY

I am the co-owner of the Nimble Services, Inc. based in Houston, Texas. I graduated from Louisiana State University in 1985 with a B.S. in Physics and second B.S. in Computer Science, and I have over 30 years experience designing technical computing solutions.

I began my professional career at Litton Industries supporting a US Navy contract creating a large database of warship design and support data. I was responsible for all aspect of the system: database, data storage, high-speed networking, imaging and scanning, and data visualization. I developed and implemented operational support systems and data converters. In my last assignment with Litton, I was the DB2 Database Administrator for a large business unit.

After leaving Litton, I moved to Houston, TX and took a contract position with Exxon Corporation. Over the next ten years, I worked on numerous data storage and migration projects including a custom HSM system that migrated data from Apollo and Sun workstations to a large IBM mainframe attached to a very large tape storage facility and a large AFS implementation that scaled from a few hundred Gigabytes to 4 Terabytes during my tenure. I designed, developed and implemented the backup system for Exxon's AFS site using up to 8 DLT tape jukeboxes. Additionally, I served on the evaluation team that extensively tested all the major enterprise RAID storage products of that time. Ultimately, Data General Clarrion systems were selected and I was instrumental in rolling out the new system to a capacity of 25 Terabytes. Also, I connected the Netscape web server to Exxon's AFS data via a custom security plug-in and implemented one of the first web search engines deployed in Exxon.

While contracting at Exxon, I joined a start-up company, Paranet, as its first employee. At Paranet I was a technology leader and advised many project teams. I managed the development of two commercial software products. One was a geophysical map data converter that was very successful. The other was a data backup system that was one of the first systems to support the new 8mm and 4mm tape stackers and jukeboxes. This backup system was sold to Exxon and used in production for several years. Additionally, I developed a custom driver for EPOCH Systems' InfiniteStorage Architecture to allow data backup and archive of Apollo workstation data to EPOCH systems.

After leaving Paranet, I co-founded Net Partners, Inc. where I continued to work on data converters for geophysical data and worked on many other types of information technology projects. My last project at Net Partners was leading a team to develop a seismic data processing collaboration platform for a seismic processing vendor. The project allowed seismic data to be processed and interpreted remotely over the Internet with a web browser. I designed and implemented the entire data management subsystem including the relational database. Also, while at Net Partners, I specialized in computer system performance analysis and capacity planning. I completed many performance-troubleshooting projects often involving large ORACLE databases, and I trained BMC Software's class instructors on BEST/1, BMC's well-known performance and capacity planning tool.

After leaving Net Partners, I founded Nimble Services, Inc. where I continued to develop and lead cutting edge information technology projects including:

- Converting a Microsoft Access application into a web-based solution serving a community of global users for a major chemical company.
- Developing many web-based interfaces to legacy computer applications and databases running on mainframe or minicomputers.
- Scaling up web application infrastructure to support thousands of users using clusters of application and database servers with secure, redundant firewall front-end systems.
- Designing high performance computer networks.
- Migrating legacy IT applications and systems to modern web-based solutions.
- Redeveloping risk management software for insurance claims to use latest Windows technologies.

EXPERIENCE

IT Security: Access Control Systems and Methodology

- Designed and implemented numerous security schemes to meet client needs using user IDs, security groups and ACLs available in most operating systems.
- Audited access control systems and security at many sites.
- Implemented custom password complexity programs at several clients.
- Analyzed password strength using cryptographic analysis and brute force attacks.
- Engineered solutions to eliminate clear text passwords in applications and databases using

security standards and custom programs to encrypt passwords.

- Extended applications like web servers to use advanced system security features like Kerberos Authentication and ACLs.
- Unified access control across the network by integrating Windows, UNIX and other computer security.

IT Security: Telecommunications and Network Security

- Performed security penetration test including Internet WAN and LAN
- Developed custom firewall solutions based on the Linux operation system.
- Secured Internet access with firewalls: FWTK, MS Proxy Server, Cisco PIX/ASA, CheckPoint, NetScreen, NetMax, SonicWall, Linksys, routers and other network security devices.
- Evaluated firewall effectiveness and reported on the results.
- Performed TCP/IP network performance tests.
- Analyzed security incidents at many companies including ExxonMobil, Global Marine and Universal Weather.

Business Continuity Planning and Disaster Recovery Planning

- Developed business continuity plan for UNIX systems at several clients
- Implemented failover solutions including clusters and data replication.

- Designed hot and cold backup sites for several clients including network, hardware, software and security aspects.

Security Management Practices

- Presented security best practices to CIO level executives and IT staff at several clients.
- Trained IT staff on security management and maintenance.
- Presented on computer security at conferences like Houston Business Expo and GHRUG.

Security Architecture and Models

- Created security audit scripts to maintain compliance.
- Implemented audit remediation to comply with corporate policies.
- Developed SOX audit policies and procedures.
- Developed tax compliance system to track corporate tax filings and compliance.
- Conducted numerous Technical Control Analysis Processes (TCAPs) on many IT products and services for ExxonMobil. TCAP is ExxonMobil's security evaluation and audit process to ensure all IT products and services comply with corporate standards and policies.
- Designed ExxonMobil's B2 level security environment for its exploration company covering systems, software, networks and security training.
- Audited security practices against business policies at several clients including ExxonMobil, Global Marine, and Challenger Mineral.

Legal Analysis

- Performed forensic analysis of many systems and provided expert reports for 8 or more legal cases dealing with theft of intellectual property, serving as expert witness in several cases.
- Provided expert analysis and reports for a software patent case. This expert witness analysis was cited by the Circuit Court of Appeals in a successful appeal of the case and instrumental in the favourable outcome for the client: http://www.cafc.uscourts.gov/opinions/06-1440.pdf

Application and Systems Development

- Developed application level network security solutions where remote systems were granted access to mainframe resources based on their physical IP address and two factor user authentication.
- Developed web-based application requiring SSL security.
- Converted a low security commercial web server farm to higher security farm located in a physically secure co-location facility and designed remediation solutions to fix 90% of the risk exposures.
- Developed a security framework to improve security of the web-based applications.
- Integrated, programmed and managed IBM Series/1 computers that linked the IBM mainframe with machine tools on the manufacturing floor.
- Integrated several manufacturing floor systems with HP 3000 mainframe and later HP-UX

server including shop scheduling system, labor data collection system, and DNC machine tools.

- Designed and developed the operating system based on Linux for custom manufacturing floor terminals.
- Developed custom data communication protocols for communication between the HP 3000 mainframe and the manufacturing servers running over both Ethernet and RS-232 serial links with full redundancy, failover and failback.
- Developed support software for testing of Blue Sky's custom TDC for high end physics experiments (STAR TOF experiment of the Relativistic Heavy Ion Collider at Brookhaven National Laboratory) in LabWindows/CVI.
- Managed the development team for Blue Sky's follow-up software to support their TDC including recruiting the team, designing the software, and debugging it.
- Developed the device driver for Blue Sky's line of high performance waveform digitizers as well as some parts of the firmware and VHDL for the PCI-E interface.
- Analyzed patents on embedded systems in vehicles and how those systems form a distributed multiprocessor system via an open communication system.
- Analyzed the source code for numerous electronic control units (ECU's) found in Ford vehicles especially how they communicate over the CANbus to form a loosely connected distributed multiprocessor system.

- Analyzed the specification and schematics of the electronic components installed in Ford vehicles known commercially as Ford SYNC; and how those components are linked to other systems including Ford SYNC services.
- Inspected and tested various combination of Ford ECU's on vehicle bucks.
- Developed embedded system software for custom electronics.
- Developed Windows device drives for custom hardware.

IT Infrastructure

- Managed technical tools for support personnel.
- Enhanced sales with technical support and technical information.
- Improved customer service levels by increasing site efficiency.
- Developed Help Desk and Network Inventory service offerings.
- Developed an AFS backup system.
- Configured Internet mail gateway and MS Exchange to support SMTP mail for 400 Exchange users.
- Managed the corporate network of Suns, HPs, Macs and PCs.
- Implemented a command line interface to TCP/IP sockets for UNIX systems.
- Implemented a UNIX and PC integration project using PC/TCP.

- Developed a UNIX file archival system using TCP/IP.
- Designed LAN and WAN networks with 100's of nodes using TCP/IP, IPX, and SNA protocols.
- Configured NFS for Suns tied to Apollo networks.
- Administered an IBM DB2 relational database system on a 4381.
- Created relational databases in ORACLE on a VAX VMS system.
- Administered a 50 node Apollo network with over 100 users.
- Administered an Empress relational database system.
- Tested new CAD software.
- Supported Versatec and HP plotters.
- Supported Optigraphics system and scanner.
- Supported the Symix/Syteline ERP, engineering design systems, and the manufacturing floor electronic test equipment and the integration between them.
- Developed custom applications interfacing with the Laserfiche document management system.

Business Systems Development

- Implemented Compiere ERP on ORACLE 9 and 10.
- Developed an engineering drawing control system.

- Developed a multi-media web application providing audio, video and application windows to remote Internet users.
- Setup UltraSeek Internet search engine to index and search corporate information.
- Administrated SQL Server and Net Dynamics server for database oriented Web applications.
- Improved a backup product with 8mm tape support on DOMAIN/OS and AFS support for Suns.
- Managed a geophysical map converter development team and developed the core application framework for the product.
- Developed a user interface for a GeoShare converter product.
- Developed a converter for 3D manufacturing data between Computer Vision and Calma CAD/CAM systems.
- Managed a CAD installation project that installed 3 division networks.
- Designed and implemented GUIs in DOMAIN/ Dialog, Open Dialogue, X11, and OSF/Motif.
- Implemented TCP/IP to SNA gateways.
- Developed an IOS type manager for backing up Apollo networks to an IBM mainframe.
- Developed a color raster formatter for a Versatec 3444 plotter.
- Developed a user support/problem tracking system.

- Introduced software engineering techniques into CAD project.
- Developed a custom IBM/RJE server.
- Developed a plot control/management system.
- Developed a generic mailbox communications package.

Performance and Monitoring

- Developed a network monitoring application that used audio recording and playback for messaging.
- Fixed ORACLE SQL*Net operations and performance.
- Analyzed X11 performance over Frame Relay network.
- Developed a UNIX system performance tool.
- Created and taught computer performance classes features BMC's BEST/1 product.
- Analyzed the performance of databases, networks, clients and applications providing recommendations to increase performance and resolve bottlenecks.

Conversions

- Converted UNIX web server to NT 4.0 and IIS.
- Ported an application from DOMAIN/OS to HP-UX.
- Converted data from numerous different systems to new formats.
- Developed an HP 3000 MPE emulation layer to port an entire suite of business applications from MPE to HP-UX.

EXPERT WITNESS CASES

Testifying

- ASCENSION DATA & ANALYTICS, LLC v. PAIRPREP, INC. d/b/a OPTICSML, SEAN M. LANNING, AND JOHN MICHAEL BROZENA
- UNITED STATES OF AMERICA v. RAMESH "SUNNY" BALWANI (Theranos COO)
- AllVoice Computing PLC v. Nuance Communications, Inc.
- AirGas, Aeriform v. IWS Gas and Supply
- JOHN C. MITCHELL, ALAN J. HEARD, STEVEN N. CORBETT, and NICHOLAS J. DANIEL v. DOUGLAS HOLT, MICHAEL K. DAVIS, and JOSEPH H. MIGLIETTA
- ALLVOICE DEVELOPMENTS US, LLC v. MICROSOFT CORPORATION

Consulting

- EAGLE HARBOR HOLDINGS, LLC, and MEDIUSTECH, LLC v. FORD MOTOR COMPANY
- WCS v. TMI
- OmmiLabs v. Core Lab
- POLYDYNE SOFTWARE INC. v. CELESTICA INTERNATIONAL, INC.

Forensics

- James Roll vs GCA Services Group
- Jacintoport vs former employees
- AET vs C5 Communications, Eric Smith, et al.

- US Quality Furniture of Services Inc. vs Furniture Works Inc.
- Sanitors Services Inc. vs Nathaniel B. Shaw
- BASEOPS INTERNATIONAL, INC. VS. EDUARDO HERNANDEZ, INTERNATIONAL TRIP PLANNING SERVICES LLC, INTERNATIONAL TRIP PLANNING, LLC and MGAS GLOBAL AVIATION SERVICES LLC
- Brad Randell
- Conix
- GAO
- Massage Envy Imperial Oaks
- Boulevard Reality/Sudhoff
- Beacon Medical v. Steve Sullivan
- PointServe (Mobi) v. IPX
- All Star Outdoors v. Mahindra (USA)
- Pipeline Trenchers LLC
- Trading Technologies International, Inc. Patent cases
- T & T Engineering Services, Inc. v. Axel Michael Sigmar, et al

EMPLOYMENT

- Nimble Services Inc., Founder, President & Senior Systems Analyst 2001-Present
- Net Partners, Inc., Co-founder, Senior Partner 1993-2001
- Paranet, Inc., Senior Systems Consultant 1991-1993

- Prime Computer, Inc., Systems Integration Consultant 1990-1991
- Exxon Company, USA Systems Analyst (contract) 1988-1990
- Litton Industries, Inc., Systems Programmer/ Analyst 1986-1988

EDUCATION

- Louisiana State University, B.S. Computer Science 1985
- Louisiana State University, B.S. Physics 1985
- University of Southern Mississippi, Graduate courses: Relational Database Systems and Software Engineering 1987
- Tulane University A. B. Freeman School of Business, Master Certificate in Business Management 2005

CONTINUING EDUCATION

- BMC Patrol Administration/Implementation
- Microsoft Windows NT Programming
- Developing File Systems for Windows NT
- BEST/1 for UNIX
- BEST/1 for Distributed Systems SureStart Engagement Process
- FileNET Panagon Sys Admin on UNIX
- OSF DME Workshop
- OSF DCE Internals
- Tivoli Management Environment Advanced Developer
- Advanced Perl Programming

- Mach 3.0 MIG Programming
- Porting the Mach 3.0 OS
- OSF/1 Introduction
- Project Management
- Parallel Algorithms and Architectures for 3D Image Generation
- X-Windows and Open Dialogue Programming
- Network Computing System (NCS) Programming
- MVS/XA Introduction
- IBM Series/I CF Support
- IBM Series/I EDL Programming
- Calma Apollo DDM System Support
- Introduction to Hypertext and Hypermedia
- Architecting on AWS

PUBLICATIONS

- UNIX Review, “Spotlight on FDDI” October, 1992
- LISA IV, “TCL and Tk: Tools for the System Administrator” October, 1992

Houston Business Review, Cost Effective IT series of articles, 2004-2005

- Cost Effective IT
- Cost-Effective IT 100 Megabit Wireless
- Cost-Effective IT Are PCs Getting Easier To Use
- Cost-Effective IT Auditing
- Cost-Effective IT Cell Phone 2005

- Cost-Effective IT Cell Phone Applications
- Cost-Effective IT Compiere
- Cost-Effective IT Cost Savings
- Cost-Effective IT EBusiness
- Cost-Effective IT Easy To Use Software
- Cost-Effective IT For Marketing Your Business
- Cost-Effective IT Future Technology
- Cost-Effective IT Hardware Failures
- Cost-Effective IT Hardware Trends
- Cost-Effective IT High Speed Wireless
- Cost-Effective IT In Emergencies
- Cost-Effective IT Internet Future
- Cost-Effective IT Internet Security
- Cost-Effective IT Linux And Open Source 2005
- Cost-Effective IT Mozilla Thunderbird
- Cost-Effective IT Netscape Reborn
- Cost-Effective IT Network Storage
- Cost-Effective IT New Developments March 2004
- Cost-Effective IT New Sales Software
- Cost-Effective IT Nvu
- Cost-Effective IT Offshoring
- Cost-Effective IT Open Source Compiere
- Cost-Effective IT Photo No No
- Cost-Effective IT Planning
- Cost-Effective IT Planning For New Year

- Cost-Effective IT Policies Procedures
- Cost-Effective IT Security Part One
- Cost-Effective IT Security Part Three
- Cost-Effective IT Security Part Two
- Cost-Effective IT Service Oriented
- Cost-Effective IT Software Failures
- Cost-Effective IT Stopping SPAM
- Cost-Effective IT Successful Ventures
- Cost-Effective IT The Business Process
- Cost-Effective IT The Compiere Difference
- Cost-Effective IT The Compiere Difference NEXT
- Cost-Effective IT The Dark Side
- Cost-Effective IT Tough Decisions
- Cost-Effective IT User Failures
- Cost-Effective IT Web Applications
- Cost-Effective IT Web Based Training
- Cost-Effective IT Web Development and Dreamweaver
- Cost-Effective IT Web Forms
- Cost-Effective IT Wireless Networking
- Cost-Effective IT Wireless Inventory

OTHER SKILLS

- Houston Business Show on CNN 650 Radio, Periodic Appearances and Guest Host, 2004-2005

REFERENCES: Available upon request.

EXHIBIT B

List of Materials Considered

URLs

https://adultblog.io/best-porn-torrent-sites/

https://arstechnica.com/tech-policy/2023/01/no-porn-without-id-louisiana-law-forces-porn-sitesto-verify-users-ages/

https://avpassociation.com/standards-for-age-verification/

https://aws.amazon.com/workspaces/pricing/

https://blog.maxmind.com/2021/07/how-accurate-is-ip-geolocation/

https://btcpeers.com/top-5-adult-crypto-projects-an-overview/

https://canopy.us/2023/07/04/how-to-block-inappropriate-websites-adult-content/

https://canopy.us/parental-control-app-technology/

https://community.torproject.org/relay/relays-requirements/

https://community.torproject.org/relay/setup/guard/centos-rhel/

https://community.verizon.com/t5/Other-Network-Discussions/How-are-IP-addresses-assignedfor-phones/td-p/1254931

https://db.dcp.utah.gov/edu/filtering.html

https://developers.google.com/search/docs/crawling-indexing/safesearch

https://developers.yoti.com/digital-id/mobile-integration https://developers.yoti.com/digital-id/security---data-protection

https://forum.dfinity.org/t/censorship-and-ip-liability-expectations/2953

https://forum.dfinity.org/t/lets-get-the-decentralized-porn-sites-up-and-going/13937

https://forum.dfinity.org/t/parler-on-the-ic/1811

https://geekflare.com/dns-content-filtering-software/

https://help.dnsfilter.com/hc/en-us/articles/1500008108542-uncategorized-sites

https://k9-web-protection.en.softonic.com/

https://lawallet.com/commercial-verification/

https://learnsafe.com/the-limitations-of-content-filtering/

https://proxyscrape.com/blog/does-tor-hide-your-ip

https://signup.opendns.com/familyshield/

https://skerritt.blog/how-does-tor-really-work/

https://suip.biz/?act=all-country-ip&province=Texas

https://support.apple.com/en-us/HT201304

https://support.microsoft.com/en-us/account-billing/filter-websites-and-searches-in-microsoftedge-3034d91e-5efa-9fbe-1384-46009f087ccf

https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344

https://support.microsoft.com/en-us/microsoft-edge/learn-more-about-kids-mode-in-microsoftedge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd

https://support.torproject.org/about/

https://support.torproject.org/https/

https://tools.zvelo.com/

https://us.norton.com/blog/privacy/tor-vs-vpn

https://vpnoverview.com/internet-safety/secure-browsing/keep-your-children-safe-online/

https://www.accscheme.com/

https://www.agechecked.com/content/

https://www.agechecked.com/gambling/

https://www.allpasstrust.com/en

https://www.asacp.org/index.html?content=parental_guidelines

https://www.bark.us/learn/bark-home/

https://www.bittorrent.com/

https://www.digicert.com/blog/evolution-of-ssl

https://www.digitaltrends.com/computing/teens-top-tech-savvy-chart-adults-lag-behind/

https://www.expressvpn.com/?msclkid=3a857574b4e417c8912811b7f0460b68

https://www.google.com/safesearch

https://www.iplocation.net/geolocation-accuracy

https://www.iwf.org.uk/our-technology/our-services/url-list/

https://www.lifewire.com/best-parental-control-routers-4160776

https://www.lifewire.com/torrent-file-2622839

https://www.linkedin.com/in/brandonls/?ref=skerritt.blog&original_referer=https%3A%2F%2Fskerritt.blog%2Fstart-here%2F

https://www.microsoft.com/en-us/microsoft-365/family-safety?ocid=cmmy4tuo5qp

https://www.microsoft.com/en-us/photodna

https://www.mozilla.org/en-US/firefox/

https://www.mozilla.org/en-US/products/vpn/features/

https://www.opendns.com/home-internet-security/

https://www.pcmag.com/opinions/louisianas-new-porn-law-is-a-privacy-time-bomb

https://www.quora.com/Is-Tor-basically-the-same-as-software-that-hides-the-users-ip-address

https://www.rtalabel.org/

https://www.shells.com/l/en-US/

https://www.shells.com/l/en-US/browser-in-the-cloud

https://www.shells.com/l/en-US/network

https://www.shells.com/l/en-US/whyshells

https://www.spiceworks.com/it-security/network-security/articles/top-10-content-filtering-software-solutions/

https://www.star-telegram.com/news/local/article277034458.html https://www.teamviewer.com/en/info/free-for-personal-use/

https://www.teamviewer.com/en-us/

https://www.techradar.com/best/virtual-desktop-services

https://www.techradar.com/reviews/shellscom

https://www.tomsguide.com/us/pictures-story/450-bittorrent-clients-list.html

https://www.torproject.org/about/history/

https://www.verywellfamily.com/best-parental-control-apps-4779963#toc-compare-the-bestparental-control-apps

https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/

https://www.webroot.com/us/en/resources/tips-articles/safety-pornography

https://www.webtitan.com/https-content-filtering-solution/

https://www.webtitan.com/internet-content-filtering-solution/

https://www.wm.edu/offices/it/services/network/virtualdesktop/faqs/index.php

https://www.yoti.com/blog/our-approach-to-security-and-privacy/

https://www.yoti.com/privacy/

https://www.yoti.com/security/

https://yoti.my.site.com/yotisupport/s/article/What-information-does-Yoti-store-about-me

https://zvelo.com/harnessing-the-power-of-website-categorization/

https://ro.ecu.edu.au/theses/2409/

https://datatracker.ietf.org/doc/html/rfc8674

https://5rightsfoundation.com/static/2089-2021-with-disclaimer.pdf?_cchid=5de613a54088e9532e49ae45cca908b8

https://help.qustodio.com/hc/en-us/articles/360005216237-Qustodio-is-not-correctly-classifying-a-website

https://www.qustodio.com/en/

https://support.mozilla.org/en-US/kb/block-and-unblock-websites-parental-controlsfiref?redirectslug=Parental+controls&redirectlocale=en-US#

Documents

- Declaration of Tony Allen, Case 2:23-cv-02123-SM-DPC Document 18-15 Filed 07/17/23 in the Eastern District of Louisiana.(18-15.pdf)
- Act of June 12, 2023, Ch. 676, ¶ 2 (H.B. 1181) Tex. Sess. Law Serv. (HB01181F.pdf)
- WHO LACKED PHOTO ID IN 2020?: An Exploration of the American National Election Studies (CDCE_VoteRiders_ANES2020Report_Spring2023.pdf)
- Internet Filtering and Adolescent Exposure to Online Sexual Material (Filtering tech article.pdf)
- Are you over 18? A Snapshot of Current Age Verification Mechanisms (AgeVerification.pdf)
- An investigation into the effifficacy of URL content fifiltering systems, Brett Ronald Turner, Edith Cowan University (https://ro.ecu.edu.au/theses/ 2409/)

- A Concise Study of Web Filtering (A Concise Study of Web Filtering.pdf)
- Yoti Facial Age Estimation White Paper Full version March 2023 (Yoti-Age-Estimatio White-Paper-March-2023.pdf)
- Onion Routing for Anonymous and Private Internet Connections (Onion Routing for Anonymous and Private (CACM-1999).pdf)
- The internet treats censorship as a malfunction and routes around it? A new media approach to the study of state internet censorship (Rogers_in_Parikka_Spam_book_optimized.pdf)
- First Nation in Cyberspace (First Nation in Cyberspace -- Printout -- TIME.pdf)
- The Security Impact of HTTPS Interception (interception-ndss17.pdf)
- Encryption, Privacy, & Data Protection: A Balancing Act (encryption-privacy-dataprotection.pdf)
- Tor: The Second-Generation Onion Router (tor-design.pdf)
- Cryptopolitik and the Darknet (Cryptopolitik and the Darknet.pdf)
- ICRAfail A Lesson For the Future (ICRAfail.pdf)
- Reimagining Digital ID INSIGHT REPORT JUNE 2023 (WEF_Reimagining_Digital_ID_2023.pdf)
- IEEE Std 2089-2021 (https://5rightsfoundation.com/static/2089-2021-withdisclaimer.pdf?_cchid=5de613a54088e9532e49ae45cca908b8)

EXHIBIT C

TIME

Monday, Dec. 06, 1993

First Nation in Cyberspace

By Philip Elmer-Dewitt

Back in the mid-1960s, at the height of the cold war, the Department of Defense faced a tough question: How could orders be issued to the armed forces if the U.S. were ravaged by a nuclear assault? The communication hubs in place at the time -- the telephone switching offices and the radio and TV broadcast stations -- were not only vulnerable to attack, they would also probably be the first to go. The Pentagon needed a military command-and-control system that would continue to operate even if most of the phone lines were in tatters and the switches had melted down.

In 1964 a researcher at the Rand Corp. named Paul Baran came up with a bizarre solution to this Strangelovian puzzle. He designed a computer-communications network that had no hub, no central switching station, no governing authority, and that assumed that the links connecting any city to any other were totally unreliable. Baran's system was the antithesis of the orderly, efficient phone network; it was more like an electronic post office designed by a madman. In Baran's scheme, each message was cut into tiny strips and stuffed into electronic envelopes, called packets, each marked with the address of the sender and the intended receiver. The packets were then released like so much confetti into the web of interconnected computers, where they were tossed back and forth over high-speed wires in the general direction of their destination and reassembled when they finally got there. If any packets were missing or mangled (and it was assumed that some would be), it was no big deal; they were simply re-sent.

Baran's packet-switching network, as it came to be called, might have been a minor footnote in cold war history were it not for one contingency: it took root in the computers that began showing up in universities and government ^ research laboratories in the late 1960s and early 1970s and became, by a path as circuitous as one taken by those wayward packets, the technological underpinning of the Internet.

The Internet, for those who haven't been hanging out in cyberspace, reading the business pages or following Doonesbury, is the mother of all computer networks -- an anarchistic electronic freeway that has spread uncontrollably and now circles the globe. It is at once the shining archetype and the nightmare vision of the information highway that the Clinton Administration has been touting and that the telephone and cable-TV companies are racing to build. Much of what Bell Atlantic and Time Warner are planning to sell -- interactivity, two-way communications, multimedia info on demand -- the Internet already provides for free. And because of its cold war roots, the Internet has one quality that makes it a formidable competitor: you couldn't destroy it if you tried.

Nobody owns the Internet, and no single organization controls its use. In the mid-1980s the National Science Foundation built the high-speed, long- distance data lines that form Internet's U.S. backbone. But the major costs of running the network are shared in a cooperative arrangement by its primary users: universities, national labs, high-tech corporations and foreign governments. Two years ago, the NSF lifted restrictions against commercial use of the Internet, and in September the White House announced a plan to make it the starting point for an even grander concept called the National Information Infrastructure.

Suddenly the Internet is the place to be. College students are queuing up outside computing centers to get online. Executives are ordering new business cards that show off their Internet addresses. Millions of people around the world are logging on to tap into libraries, call up satellite weather photos, download free computer programs and participate in discussion groups with everyone from lawyers to physicists to sadomasochists. Even the President and Vice President have their own Internet accounts (although they aren't very good at answering their mail). "It's the Internet boom," says network activist Mitch Kapor, who thinks the true sign that popular interest has reached critical mass came this summer when the New Yorker printed a cartoon showing two computer-savvy canines with the caption, "On the Internet, nobody knows you're a dog."

But the Internet is not ready for prime time. There are no TV Guides to sort % through the 5,000 discussion groups or the 2,500 electronic newsletters or the tens of thousands of computers with files to share. Instead of feeling surrounded by information, first-timers ("newbies" in the jargon of the Net) are likely to find themselves adrift in a borderless sea. Old-timers say the first wave of dizziness doesn't last long. "It's like driving a car with a clutch," says Thomas Lunzer, a network designer at SRI International, a California consulting firm. "Once you figure it out, you can drive all over the place."

But you must learn new languages (like UNIX), new forms of address (like president whitehouse.gov and new ways of expressing feeling (like those ubiquitous sideways smiley faces), and you must master a whole set of rules for how to behave, called netiquette. Rule No. 1: Don't ask dumb questions. In fact, don't ask any questions at all before you've read the FAQ (frequently asked questions) files. Otherwise you risk annoying a few hundred thousand people who may either yell at you (IN ALL CAPS!) or, worse still, ignore you.

All that is starting to change, however, as successive waves of netters demand, and eventually get, more user-friendly tools for navigating the Internet. In fact, anyone with a desktop computer and a modem connecting it to a phone line can now find ways into and around the network. "The Internet isn't just computer scientists talking to one another anymore," says Glee Willis, the engineering librarian at the University of Nevada at Reno and one of nearly 20,000 (mostly female) academic librarians who have joined the Internet in the past five years. "It's a family place. It's a place for perverts. It's everything rolled into one."

As traffic swells, the Internet is beginning to suffer the problems of any heavily traveled highway, including vandalism, break-ins and traffic jams. "It's like an amusement park that's so successful that there are long waits for the most popular rides," says David Farber, a professor of information science at the University of Pennsylvania and one of the network's original architects. And while most users wait patiently for the access and information they need, rogue hackers use stolen passwords to roam the network, exploring forbidden computers and reading other people's mail.

How big is the Internet? Part of its mystique is that nobody knows for sure. The only fact that can be measured precisely is the number of computers directly connected to it by high-speed links -- a figure that is updated! periodically by sending a computer program crawling around like a Roto-Rooter, tallying the number of connections (last count: roughly 2 million). But that figure does not include military computers that for security reasons are invisible to other users, or the hundreds of people who may share a single Internet host. Nor does it include millions more who dial into the Internet through the growing number of commercial gateways, such as Panix and Netcom, which offer indirect telephone access for $10 to $20 a month. When all these users are taken into account, the total number of people around the world who can get into the Internet one way or another may be 20 million. "It's a large country," says Farber of the Internet population. "We ought to apply to the U.N. as the first nation in cyberspace."

That nation is about to get even bigger as the major commercial computer networks -- Prodigy, CompuServe, America Online, GEnie and Delphi Internet Service -- begin to dismantle the walls that have separated their private operations from the public Internet. The success of the Internet is a matter of frustration to the owners of the commercial networks, who have tried all sorts of marketing tricks and still count fewer than 5 million subscribers among them. Most commercial networks now allow electronic mail to pass between their services and the Internet. Delphi, which was purchased by Rupert Murdoch's News Corp. in September, began providing its customers full Internet access last summer. America Online (which publishes an electronic version of Time) is scheduled to begin offering limited Internet services later this month.

People who use these new entry points into the Net may be in for a shock. Unlike the family-oriented commercial services, which censor messages they find offensive, the Internet imposes no restrictions. Anybody can start a discussion on any topic and say anything. There have been sporadic attempts by local network managers to crack down on the raunchier discussion groups, but as Internet pioneer John Gilmore puts it, "The Net interprets censorship as damage and routes around it."

The casual visitor to the newsgroups on the Usenet (a bulletin-board system that began as a competitor to the Internet but has been largely subsumed by it) will discover discussion groups labeled, according to the Net's idiosyncratic cataloging system, alt.sex.masturbation, alt.sex.bondage and alt.sex.fetish.feet. On Internet Relay Chat, a global 24-hour-a-day message board, one can stumble upon imaginary orgies played out with one-line typed commands ("Now I'm taking off your shirt . . ."). In alt.binaries.pictures.erotica, a user can peek at snapshots that would make a sailor blush.

But those who focus on the Internet's sexual content risk missing the point. For every sexually oriented discussion group there are hundreds on tamer and often more substantial topics ranging from bungee jumping to particle physics. Last week Virginia college student Chris Glover responded to a distressed message from a suicidal undergraduate in Denver. After two hours of messages back and forth, Glover was able to pinpoint the woman's location and call for help.

With all this variety, Internet users are unimpressed by television's promise of a 500-channel future. The Internet already delivers 10,000 channels, and the only obstacle that prevents it from carrying live TV pictures is the bandwidth (or carrying capacity) of the data lines. Some video clips -- and at least one full-length video movie -- are already available on the network. And last spring, writer Carl Malamud began using the Internet to distribute a weekly “radio” interview show called Geek of the Week. Malamud is undeterred by the fact that it takes a computer about an hour over a high- speed modem to capture the 30 minutes of sound that a $10 radio can pick up instantly for free. But bandwidth capacity has nowhere to go but up, says Malamud, and its cost will only go down.

The Internet, however, will have to go through some radical changes before it can join the world of commerce. Subsidized for so long by the Federal Government, its culture is not geared to normal business activities. It does not take kindly to unsolicited advertisements; use electronic mail to promote your product and you are likely to be inundated with hate mail directed not only at you personally but also at your supervisor, your suppliers and your customers as well. “It’s a perfect Marxist state, where almost nobody does any business,” says Farber. “But at some point that will have to change.”

The change has already begun. NSF’s contribution now represents about 10% of the total cost of the network, and the agency is scheduled to start phasing out its support next April, removing at the same time what few restrictions still remain against commercial activity. According to Tim O’Reilly, president of O’Reilly & Associates, a publisher experimenting with advertiser-supported ^ Internet magazines, the system could evolve in one of two ways: either entrepreneurs will manage to set up shop on a free-market version of the Internet, or some consortium will take the whole thing over and turn it into a giant CompuServe. “That’s an outcome,” O’Reilly says, “that would effectively destroy the Internet as we know it.”

As the traffic builds and the billboards go up, some Internet veterans are mourning the old electronic freeway. “I feel kind of sad about it,” says Denise Caruso, editorial director of Friday Holdings, a publisher specializing in new media. “It was such a dynamic, pulsing thing. I wonder whether we shouldn’t have left it alone.” Others see the period of uncertainty ahead as a rare opportunity for citizens to shape their own technological destiny. “We need . . . a firm idea of the kind of media environment we would like to see in the future,” warns Howard Rheingold in his new book, The Virtual Community. While it may be difficult for communities as diverse as those on the Internet to set their own agenda, it seems increasingly likely that if they don’t, someone else will do it for them.

Find this article at:

https://content.time.com/time/magazine/article/0,9171,979768,00.html

EXHIBIT D

Are you over 18?

A Snapshot of Current Age Verification

Mechanisms

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

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

Proceedings of 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, 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)

[1] University of Strathclyde, Glasgow, UK

[2] Rhodes University, Grahamstown, South Africa

[3] University of South Africa, Pretoria, South Africa

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.

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.

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

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

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.

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 solution 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 standar [36], which aims at "*making products, systems, services, environments and facilities more accessible to more people i 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, 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].

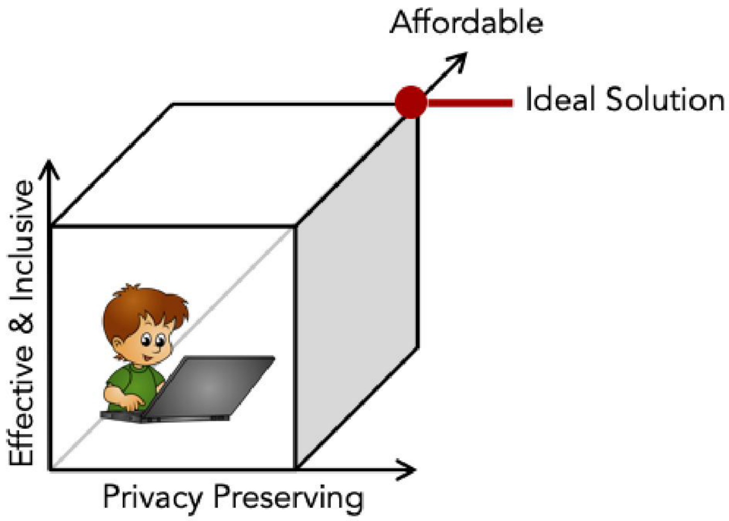


Figure 1: Age Verification Mechanism Dimensions

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.

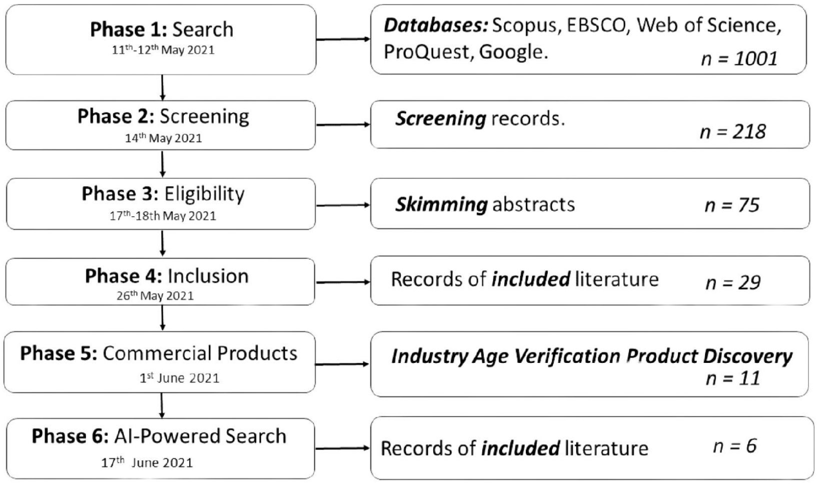


Figure 2: PRISMA of Systematic Literature Review [40]

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

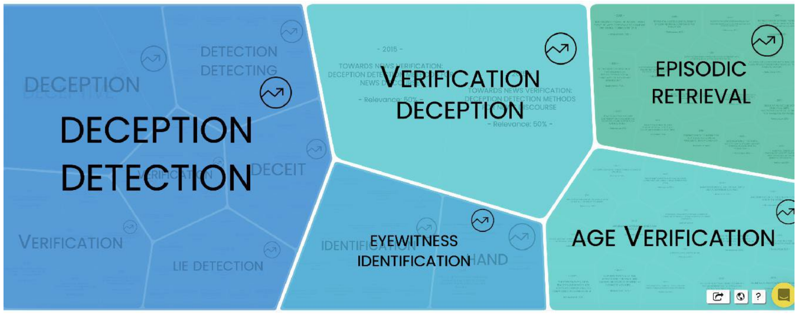


Figure 3: Result of AI-Powered Search

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.

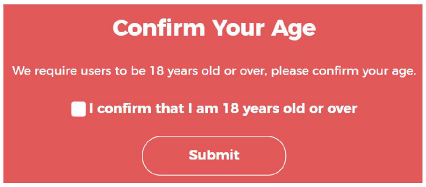
In summary, the most common age verification process demonstrated in these studies is the tick box, which cannot possibly be effective in preventing youths buying or accessing adult products and services. This method is essentially "verification theatre" (Figure 4). The only consideration recommending 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 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].

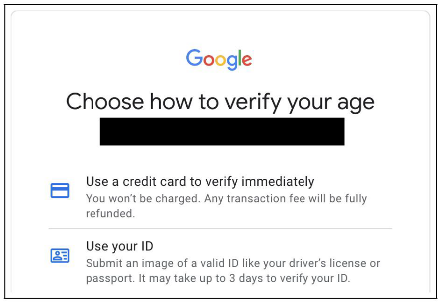


Confirm Your Age

We require users to be 18 years old or over, please confirm your age.

□ I confirm that I am 18 years old or over

Figure 4: "Verification Theatre" Tick Box



Choose how to verify your age

[redacted]

Use a credit card to verify immediately
You won't be charged. Any transaction fee will be fully refunded.

Use your ID
Submit an image of a valid ID like your driver's license or passport. It may take up to 3 days to verify your ID.

Figure 5: Google's Age Verification

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:

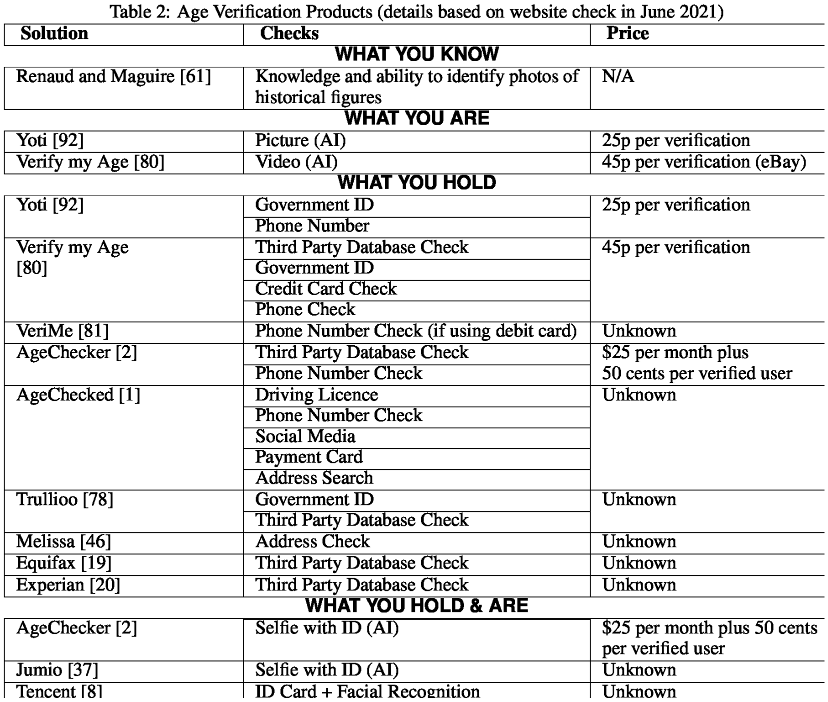


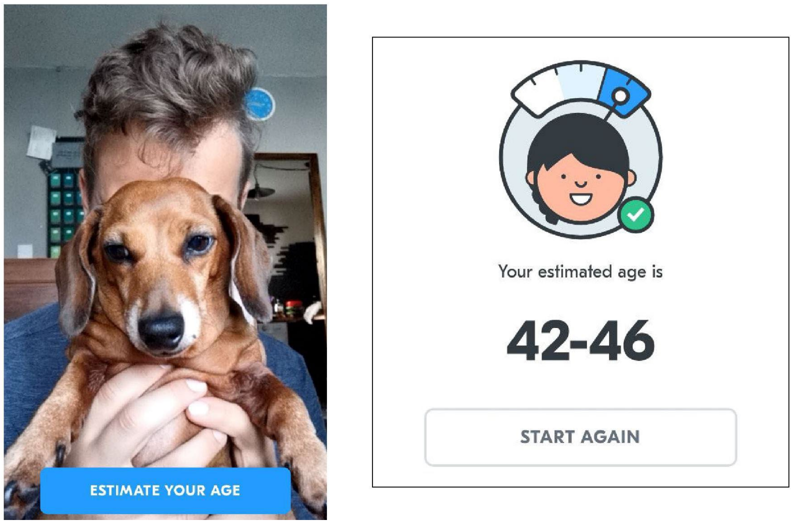
Table 2: Age Verification Products (details based on website check in June 2021)

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.



Your estimated age is

42-46

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-fair

weather-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 cyber safety 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.

EXHIBIT E

Onion Routing for Anonymous and Private Internet Connections

David Goldschlag[*]

Michael Reed[†]

Paul Syverson[†]

January 28, 1999

1 Introduction

Preserving privacy means not only hiding the content of messages, but also hiding who is talking to whom (traffic analysis). Much like a physical envelope, the simple application of cryptography within a packet-switched network hides the messages being sent, but can reveal who is talking to whom, and how often. Onion Routing is a general purpose infrastructure for private communication over a public network [8, 9, 4]. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. The connections are bidirectional, near real-time, and can be used for both connection-based and connectionless traffic. Onion Routing interfaces with off the shelf software and systems through specialized proxies, making it easy to integrate into existing systems. Prototypes have been running since July 1997. As of this article's publication, the prototype network is processing more than 1 million Web connections per month from more than six thousand IP addresses in twenty countries and in all six main top level domains. [7]

[*] Divx, Herndon, VA USA, david.goldschlag@divx.com

[†] Center for High Assurance Computer Systems, Naval Research Laboratory, Washington, DC USA, Breed, syversonl@itd.nrl.navy.mil

Onion Routing operates by dynamically building anonymous connections within a network of real-time Chaum Mixes [3]. A Mix is a store and forward device that accepts a number of fixed-length messages from numerous sources, performs cryptographic transformations on the messages, and then forwards the messages to the next destination in a random order. A single Mix makes tracking of a particular message either by specific bit-pattern, size, or ordering with respect to other messages difficult. By routing through numerous Mixes in the network, determining who is talking to whom becomes even more difficult. Onion Routing's network of core onion-routers (Mixes) is distributed, fault-tolerant, and under the control of multiple administrative domains, so no single onion-router can bring down the network or compromise a user's privacy, and cooperation between compromised onion-routers is thereby confounded.

2 Application Support via Proxies

Onion Routing can be used with applications that are proxy-aware, as well as several non-proxy-aware applications, without modification to the applications. Currently supported protocols include HTTP, FTP, SMTP, rlogin, telnet, NNTP, finger, whois, and raw sockets. Proxies are under development for Socks5, DNS, NFS, IRC, HTTPS, SSH, and Virtual Private Networks (VPNs). A proxy has three logical layers: an optional application specific privacy filter that sanitizes the data streams; an application specific proxy that translates the data streams into an application independent format accepted by the Onion Routing network; and lastly, an onion proxy that builds and manages the anonymous connections. Because it builds and manages the anonymous connections, the onion proxy is the most trusted component in the system. Likewise, to build onions and hence define routes the onion proxy must know enough of the topology and link state of the network, the public certificates of nodes in the network, and the exit policies of nodes in the network. This information is distributed securely within the network automatically as new nodes come on-line or as the information changes.

3 Moving Data through the Network

Onion Routing's anonymous connections are protocol independent and exist in three phases: connection setup, data movement, and connection tear-down. Setup begins when the initiator creates an onion, which defines the path of the connection through the network. An onion is a (recursively) layered data structure that specifies properties of the connection at each point along the route, e.g. cryptographic control information such as the different symmetric cryptographic algorithms and keys used during the data movement phase. Each onion router along the route uses its public key to decrypt the entire onion that it receives. This operation exposes the cryptographic control information, the identity of the next onion router, and the embedded onion. The onion router pads the embedded onion to maintain a fixed size, and sends it to the next onion router. After the connection is established, data can be sent in both directions. Data from the initiator is repeatedly pre-encrypted using the algorithms and keys that were specified in the onion. As data moves through the anonymous connection, each onion-router removes one layer of encryption as defined by the cryptographic control information in the onion defining the route, so the data arrives as plaintext at the recipient. This layering occurs in the reverse order (using different algorithms and keys) for data moving backward. Connection tear-down can be initiated by either end, or in the middle if needed.

All information (onions, data, and network control) are sent through the Onion Routing network in uniform-sized cells. All cells arriving at an onion-router within a fixed time interval are mixed together to reduce correlation by network insiders. Likewise, the long-standing connections between onion-routers can be padded and bandwidth-limited to foil external observers. An Onion looks different to each onion-router along a connection because of the layered public-key cryptography. Similarly, the layering of symmetric cryptography over the data phase cells makes them appear different to each onion-router. This design resists traffic analysis more effectively than any other deployed mechanisms for Internet communication.

4 Overhead

Onion Routing's overhead is relatively small. Connection setup overhead is typically much less than one second and appears to be no more noticeable than other delays associated with normal web connection setup on the Internet. Computationally expensive public-key cryptography is used only during this connection setup phase. Also, because public key decryption is much more expensive than encryption, the public key burden is mainly placed upon the onion routers themselves, where dedicated hardware acceleration can be justified. The data movement phase uses only secret-key (symmetric) cryptography, which is much faster. Furthermore, since the symmetric encryption can be pipelined, data throughput can be made as fast as ordinary link or end-to-end encryption. Data latency is affected by the number of onion-routers along the connection and can vary with route length and the duration of the Mix cycles.

5 Network Architectures that Shift Trust

Proxies, onion-routers, and other components can be run in a variety of distributed configurations. This allows Onion Routing to mesh well with a wide variety of operational and policy environments. At one extreme, proxies can run remotely. If a user makes a secure connection (e.g., encrytped or withing a firewall) to a trusted remote proxy, Onion Routing's protection can be utilized without installing any software or inducing local computational overhead. At the other extreme, all trusted components can run locally, providing maximum protection of anonymity and privacy against non-local components, even those participating in a connection. In between these two extremes are multiple configurations of proxies and onion routers, running on enclave firewalls or at ISPs.

By shifting trust in this way, Onion Routing can also complement other services like the Anonymizer [1] and LPWA [6]. The Anonymizer uses a central, trusted intermediary to provide sender anonymity (i.e., hide the identity of the sender from the receiver). If Onion Routing is used for privacy, an Anonymizer can run as a filtering proxy on the user's desktop (or the enclave firewall, or the user's ISP) to add sender anonymity. Security is improved because the filtering executes on a machine the user trusts, and communication leaving that machine will resist traffic analysis. Such security in depth removes the central point of failure for network traffic anonymity. LPWA provides various psuedonymybased services (described elsewhere in this issue). Like Onion Routing it is designed to handle email in addition to HTTP. And, like Onion Routing, it can be configured so that trusted functions are performed at various locations [2]. However, communication between and from these points is not itself anonymous or resistant to traffic analysis. This makes LPWA and Onion Routing especially natural complements.

6 Extensions

A natural extension to Onion Routing is the introduction of reply onions. Reply onions allow connections to be made back to an anonymous sender through the Onion Routing network long after the original connection existed. Reply Onions could be used to send anonymous replies in response to a previously received anonymous email. They could also enable novel applications such as anonymous publishing (anonymous URLs) similar to the Rewebber project [5].

7 Conclusion

In summary, Onion Routing is a traffic analysis resistant infrastructure that is easily accessible, has low overhead, can protect a wide variety of applications, and is flexible enough to adapt to various network environments and security needs. The system is highly extensible, allowing for additional symmetric cryptographic algorithms, proxies, or routing algorithms with only minor modifications to the existing code base. Instructions for accessing the Onion Routing network can be found on our web page along with additional background, pointers to publications, and contact information [7].

References

[1] The Anonymizer. http://www.anonymizer.com/

[2] D. Bleichenbacher, E. Gabber, P. Gibbons, Y. Matias, and A. Mayer. “On Secure and Pseudonymous Client-

Relationships with Multiple Servers", to appear in Proc. 3rd USENIX Electronic Commerce Workshop , August 1998.

[3] D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, v. 24, n. 2, Feb. 1981, pp. 84-88.

[4] D. Goldschlag, M. Reed, P. Syverson. "Hiding Routing Information", in Information Hiding, R. Anderson, ed., LNCS vol. 1174, Springer-Verlag, 1996, pp. 137{150.

[5] I. Goldberg and D. Wagner. "TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the World Wide Web", First Monday,

[6] The Lucent Personalized Web Assistant. http://lpwa.com/

[7] The Onion Routing Home Page. http://www.onion-router.net/ Conference:

[8] M. Reed, P. Syverson, and D. Goldschlag. "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, vol. 16 no. 4, May 1998, pp. 482{494.

[9] P. Syverson, M. Reed, and D. Goldschlag. "Private Web Browsing", Journal of Computer Security, vol. 5 no. 3, 1997, pp. 237{248.

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No.: 1:23-cv-917

FREE SPEECH COALITION, INC., MG PREMIUM LTD, MG FREESITES LTD, WEBGROUP CZECH REPUBLIC, A.S., NKL ASSOCIATES, S.R.O., SONESTA TECHNOLOGIES, S.R.O., SONESTA MEDIA, S.R.O., YELLOW PRODUCTION S.R.O., PAPER STREET MEDIA, LLC, NEPTUNE MEDIA, LLC, JANE DOE, MEDIAME SRL, MIDUS HOLDINGS, INC.,

Plaintiffs,

vs.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,

Defendant.

DECLARATION OF ALISON BODEN IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Alison Boden, declare as follows:

1. I provide this declaration in support of the Motion for Expedited Preliminary Injunction against enforcement of Act of June 12, 2023, Ch. 676, § 2 (H.B. 1181) Tex. Sess. Law Serv. ("the Act"). I am over eighteen years of age, and I have personal knowledge of the matters set forth in this Declaration; if called as a witness I could and would testify competently to these matters.

2. I am the Executive Director of the Free Speech Coalition ("FSC"), a plaintiff in this action. Before joining FSC, I was professionally involved in the adult entertainment industry for 20 years in various capacities, including as a small business owner, marketer, product manager, software developer, manager, and chief executive officer.

3. FSC is a not-for-profit trade association that assists filmmakers, producers, distributors, wholesalers, manufacturers, retailers, internet platforms, performers, writers, educators, and other creative artists located throughout North America in the exercise of their First Amendment rights and in the vigorous defense of those rights against censorship.

4. Founded in 1991, FSC currently represents hundreds of businesses and individuals involved in the production, distribution, sale, and presentation of constitutionally-protected and non-obscene materials that are disseminated to consenting adults via the internet.

5. In this action, FSC acts especially on behalf of its many members who are individual adult performers gravely concerned about the consequences of the Act, but who fear for their safety should they come forward publicly to challenge the Act in court.

6. As someone who has worked in adult entertainment industry for many years, I am aware that privacy is of paramount importance to individuals working within the industry. Most models or actors, and many individuals working behind the camera or in administrative positions, use pseudonyms to protect themselves against harassment, doxing, and general animosity targeted towards those who work within the adult industry. I have personally witnessed individuals

whose lives have been nearly destroyed after being publicly connected to adult businesses. The same animosity and judgement is targeted towards those who watch, read, or listed to adult content. Thus, although many people access adult material, few would want their friends, neighbors, or family to know.

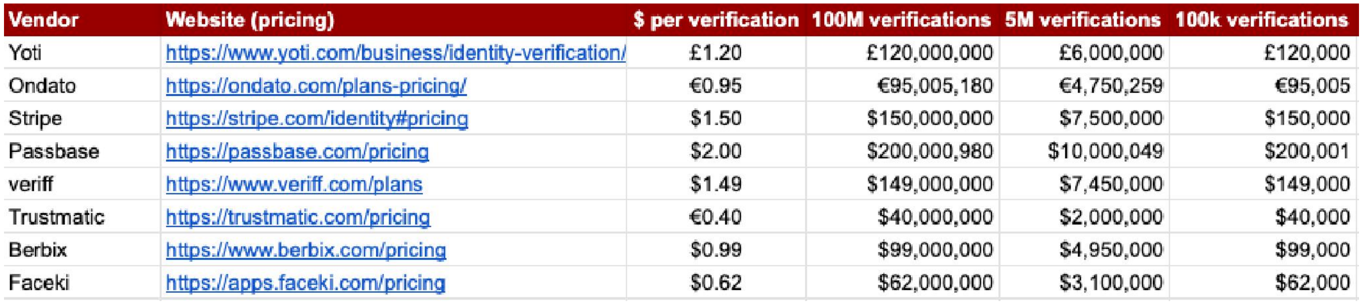
7. The rights of FSC members and viewers of their material will be seriously infringed if the Court does not enjoin the Act. FSC members are currently responding to similar Acts recently enacted in other states in one of three ways: by (1) declining to abide by the statutory terms, thus risking lawsuits or civil penalties so long as the Act remains in effect; (2) diverting web traffic from IP addresses within the state passing such Acts, thus precluding online visitors from those States (to the extent possible); or (3) contracting (at great expense) the services of age-verification platforms to age-verify visitors to their site. When the Act goes into effect on September 1, 2023, they will have those same three options.

8. Option (1) outlined above puts FSC members at grave risk of lawsuits and civil penalties, including costs and attorney's fees. For many—including performers who operate as corporations, single-member LLCs, or sole proprietorships likely qualifying as "commercial entities" governed by the Act—even a single adverse judgment or statutory penalty could prove ruinous for the business.

9. Option (2) prevents FSC members from reaching Texas customers and prevents those customers from accessing non-obscene, constitutionally protected material. It also impedes the rights of residents living in border towns of neighboring states from receiving such material where their IP addresses mistakenly reflect presence in Texas.

10. Option (3) is unworkable for most FSC members. Because of the Act's vagueness, members are unsure what protocols constitute "a digital network that may be accessed by a commercial entity and that serves as proof of the identity of an individual" or a "commercially reasonable method [relying] on public or private transactional data to verify the age of an individual" sufficient to provide safe harbor under the Acts. Nor is it clear what it means under the Act to, "require an individual to present a government-issued identification." To the best of my knowledge, Texas does not provide access to any government identity databases to third-party vendors, and FSC members do not wish to rely on the provision of services from such third-party vendors to distribute constitutionally-protected materials to Texas adults. Likewise, verification via "any commercially reasonable method" is also unworkable and unclear where that method must rely on "public or private transactional data" to verify the user's age. FSC members do not know what "commercially reasonable" means and do not know of third-party vendors using such transactional data to age-verify users.

11. Although there *are* providers of age-verification services in operation, the specifics of those services vary. What they share in common is an exorbitant price placed on the age-verifying entity. I used similarweb.com to research estimates for the number of US-based users that FSC members' websites received in April 2023. The average is nearly 80,000,000 and the median is about 5,000,000. Then, I created the following table to identify the providers of which I am aware that verify a user's identity via government identification documents and make their pricing public (most do not). I used my calculations to create an estimated cost for websites of various sizes.



Vendor	Website (pricing)	$ per verification	100M verifications	5M verifications	100k verifications
Yoti	https://www.yoti.com/business/identity-verification/	£1.20	£120,000,000	£6,000,000	£120,000
Ondato	https://ondato.com/plans-pricing/	€0.95	€95,005,180	€4,750,259	€95,005
Stripe	https://stripe.com/identity#pricing	$1.50	$150,000,000	$7,500,000	$150,000
Passbase	https://passbase.com/pricing	$2.00	$200,000,980	$10,000,049	$200,001
veriff	https://www.veriff.com/plans	$1.49	$149,000,000	$7,450,000	$149,000
Trustmatic	https://trustmatic.com/pricing	€0.40	$40,000,000	$2,000,000	$40,000
Berbix	https://www.berbix.com/pricing	$0.99	$99,000,000	$4,950,000	$99,000
Faceki	https://apps.faceki.com/pricing	$0.62	$62,000,000	$3,100,000	$62,000

12. Instead of website-based age verification, FSC fully supports the use of parental filtering on children's devices. That's why we use the "Restricted to Adults" (RTA) label on our sites and platforms. It was created by the nonprofit Association of Sites Advocating Child Protection (ASACP) to standardize a single, consistent, universally recognizable tag for adult material that triggers an automatic block by device-level parental control and filtering software.

13. Separately from the issue of age verification, the Act mandates that websites display what the Act calls "Sexual Materials Health Warnings." The content of these warnings is antithetical to the beliefs of FSC and its members, who have pledged to advocate for the constitutional rights of adults to freely express themselves and to make their own decisions regarding personal sexual behavior, and treat every member of the adult entertainment industry with respect and professionalism both on and off the set. FSC vigorously disputes the accuracy of the "Health Warnings" and finds them counterproductive and harmful to those who chose to exercise their First Amendment right to read, watch, or listen to erotic material, including consumers of FSC members' erotic content.

14. I read and shared with FSC members the Jun. 16, 2023 article written by Carlie Kollath Wells for Axios New Orleans, titled *Millions of Louisiana resident targeted in massive cyberattack*, available at https://www.axios.com/local/new-orleans/2023/06/16/louisiana-cyberattack-dmv-moveit, which reports "[e]veryone with a Louisiana driver's license or state ID likely had their personal information exposed in a massive cyberattack that's punctured agencies across the country." This hack is particularly alarming to FSC, as Louisiana recently passed an age-verification statute

that works in conjunction with Louisiana's digital driver's license and age verification service LA Wallet. Given the risks of identity theft that come even with purportedly "more secure" ways to verify age like LA Wallet, FSC members are 1) concerned that unnecessarily requiring the entry of personal data to access legal erotic content on the internet increases the risk that adults' sensitive personal data will be hacked, and 2) that knowing of this risk, potential customers will decline to access such material through any website that follows the age-verification mandates of the Act.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on August 1, 2023 in San Francisco, California.

Dated: August 1, 2023

/s/ *Alison Boden*
Alison Boden

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA

Civil Action No. 23-02123

FREE SPEECH COALITION, INC., et al.,

Plaintiffs,

v.

JAMES M. LEBLANC, in his official capacity as Secretary of the Louisiana Department of Public Safety and Corrections, et al.,

Defendants.

Judge Susie Morgan

Magistrate Judge Donna Phillips Curraul

Section "E" (2)

DECLARATION OF DR. GAIL DINES

I, Gail Dines, Ph.D., under 28 U.S.C. § 1746, declare as follows:

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

2. I am President and CEO of Culture Reframed, a nonprofit organization dedicated to building resilience and resistance in youth to hypersexualized media and porn.

3. I am also a Professor Emerita of Sociology and Women's Studies at Wheelock College in Boston,

Massachusetts. (Wheelock College merged with Boston University in 2018)

4. I have been researching and writing about the porn industry and sexual violence for over 30 years. For my work, I received the Myers Center Award for the Study of Human Rights in North America. I was also named as one of the top 10 most influential women sociologists in the last 10 years by Academic Influence.[1]

5. I have devoted my professional life to studying the effects of pornography on children and adults. I have written numerous articles and my latest book, *Pornland: How Porn Has Hijacked our Sexuality*,[2] has been translated into 5 languages. Given my professional expertise I am well-positioned to speak to the harms of pornography on young people from a social-scientific stance.

Age of Children First Viewing Pornography

6. Pornography has now become the major form of sex education for children.[3] Studies show that a majority of adolescents (90+% of boys and 60+% of girls) are exposed to pornography at some point in their teenage years,[4] with 11 being the average age of first exposure, usually on a digital device accessible within the home.[5] Exposure is often accidental or unwanted[6] as a result of advertisements, misspelled searches, and "redirections."[7] According to a 2019 study by the British Board of Film Classification, "Children see pornography as young as seven."[8]

7. The majority of the most popular porn website are called Tube Sites, and much like YouTube, the vast amount of content is free, and requires no Age Verification. Any child with a mobile device can access

the mainstream hardcore pornography in a matter of seconds.

Content of Mainstream Pornography

8. It is a mistake to think of Playboy, Penthouse, or even Hustler when discussing the contemporary porn online porn industry. Dominated by Mindgeek,[9] a company located in Quebec, with offices all over the world, this huge enterprise owns most of the popular porn sites, including its flagship porn site, Pornhub (see section below on the porn industry for further discussion). Rather than the images of yesterday, which showcased pinup pornography, today's mainstream pornography is violent, body-punishing, and cruel.[10]

9. The obvious next question is what are children seeing when they are exposed to pornography. Spanking, gagging, slapping, hair pulling, and choking are the five most common forms of physical aggression shown in pornography. Women are the target of the aggression in 97% of the scenes, and their response to aggression was either neutral or positive and rarely negative.[11]

10. The industry has seen a dramatic increase in what is commonly called "choking" but is in reality defined by medical science as "nonfatal strangulation" which poses grave neurological harms to victims, including unconsciousness, brain injury, seizure, motor and speech disorders, memory loss, and post-traumatic stress disorder (PTSD).[12]

11. Some Pornhub videos also show scenes of rape. Although Pornhub claims that all the videos they upload feature consensual sex, there are tags that intentionally misspell the word consensual as "consesual," to avoid legal action. In July 2023, there were over 200,000 videos in the "Un Consesual"

category, and 198,000 videos in the "Non Consesual Porn Porn videos."[13] The theme of the videos, as the name suggests, is forcing sex on an unwilling woman. This normalizes rape for the consumers, especially children, who are more likely to believe that the violence being played out is real, rather than staged[14].

12. In its latest "Year in Review," Pornhub (2022)[15] announced that the most popular search term on the site was "hentai." In January 2023 Pornhub hosted more than 109,000 hentai videos, some with more than five million views. The term is an English loanword from a Japanese phrase that in the early 20th century came to mean 'sexual perversion.'

13. In the West today, hentai refers to pornified renditions of anime, the distinctive, colorful, action-packed style of Japanese animation much beloved by kids everywhere. In fact, the characters in hentai typically *look* like kids, except for their enlarged breasts and genitals. They are typically entangled in brutal, often monstrous sex. The latter is literally true, since a common theme in hentai is a grotesque creature penetrating a girl with an enormous phallus or tentacle. The sexual violence in hentai is so extreme that in real life it would result in the bloody harm and death of the women and children so victimized.[16]

14. A study by the British Board of Film Classification or BBFC (2022)[17], an independent regulatory agency, examined online computer-generated or drawn images – cartoons and animation - depicting the sexual abuse of children and child-like characters. A key finding of the report was that "children aged 6-12 are," compared to adults, "disproportionately exposed to pornography sites specializing in non-photographic content". That content mainly consists of hentai - the very content prominently featured on Pornhub.

15. Hentai, as the BBFC report stated, promotes "an interest in abusive relationships." Much of the hentai available on free porn sites consists of characters from movies, television, games, and the internet "likely to be familiar or appealing to children." In fact, Pornhub features cartoons, animation, and costumed skits drawn from a wide range of children's entertainment and games.

16. Another popular theme in hentai is incest, which almost always involves depictions of children. I googled "hentai incest" in January 2023 and received 5.4 million results.The latter was hosted by Hentai.tv, which displayed advertisements for Brazzers, another MindGeek company that also has its own Pornhub channel.

Research exploring the Social, Emotional, Cognitive and Sexual Harms of Pornography on Young People

17. Peer-reviewed research continues to deepen and validate our knowledge of the harms of pornography. The habitual viewing of pornography remains linked to a host of mental health afflictions, such as depression, dissociation ("become increasingly detached from both their own feelings and reality"), and behavioral problems such as sexual impulsivity.[18] Studies show that many young people are so obsessed with porn that they continue to watch it even though they know that what they are seeing is unreal, wrong in the offline world, and goes against their own values. Porn is not only violence against women. But it is violence against the self. And against others, of course, since adolescent users of porn are at a higher risk of perpetrating intimate partner cyberstalking.[19] They also "have lower degrees of social integration...and decreased emotional bonding with caregivers."[20]

18. Studies also show that both young men and young women emulate in their own lives what they see in pornography. This is especially true for sexual strangulation,[21] verbal or physical sexual coercion,[22] and dating violence.[23] In a study from the UK, 42% of 15-16 year olds expressed the desire to mirror pornography – and more than half of all boys believe that online porn depicts realistic sexuality.[24]

19. The latter point is especially troubling since, as a recent study concluded, "far from being represented as aberrant, sexual practices involving coercion, deception, non-consent and criminal activity are described in mainstream online pornography in ways that position them as permissible."[25] One study cautioned that "*any* pornography use resulted in a significantly greater likelihood of physically coercive behavior."[26]

20. Recent study after recent study has shown that viewing pornography leads young people, especially boys, to engage in sexual aggression.[27]

21. Research also shows that minors who view porn are at a higher risk of adult perpetration of child sexual abuse and seeking out illegal child porn.[28] They are more likely to display hypersexualization and to develop paraphilias (e.g., exhibitionism, voyeurism).[29]

22. For girls, early internet exposure to porn is a risk factor for later suffering sexual abuse, sexual coercion, and sexual aggression.[30] Frequent use of pornography is linked to young people perpetrating face-to-face bullying and online cyberbullying.[31]

23. Adolescents and teens who view porn are more likely to use illegal drugs, alcohol, and tobacco as well as rule-break more generally, such as skipping school.[32]

24. Higher porn use predicts adolescent and teen sexting (texting nude and semi-nude photos), including the non-consensual sharing of intimate photos ("revenge porn").[33] In many countries, including the US, it is illegal for minors to possess or share naked photos of other minors. The rise of teen sexting is directly tied to the ongoing prevalence of pornography.[34]

25. Adolescent porn users often lack the social-emotional skills to say no to unhealthy relationships and unwanted sex. They rate themselves poorly at choosing trustworthy partners, communicating how they want to be treated, setting limits and realistic expectations, and making decisions rather than letting things happen.[35]

26. Regular adolescent porn consumers are more likely to use the internet continuously and compulsively, to the detriment of everyday life. Symptoms of this addiction can include irritability, poor social functioning, impulsiveness, and social anxiety.[36]

27. Advances in brain science are also increasing our awareness of the harms of pornography. The under-developed adolescent brain is particularly susceptible to the content of porn,[37] which can lead to dysfunctional stress responses and poor executive function, including impairments to judgment, memory, and emotional regulation.[38]

28. Early use of porn may trigger adolescent depression and psychosomatic symptoms (e.g., headache, irritability, trouble sleeping). Unhappy adolescents may turn to porn for "mood management," leading to further dysfunction and negative effects on their mental health.[39]

29. Porn continues to teach young people that sexism and misogyny are acceptable. Adolescent boys

who consume porn are more likely to value girls and women only for their appearance and willingness to satisfy men's desires, to believe that it is more important for women to be pretty than smart, and that women should learn to obey men.[40]

30. Both boys and girls who view porn are more accepting of sexual violence against women and rape myths (e.g., the victim asked for it, or wanted it). They are also more likely to trivialize sexual aggression.[41]

31. Girls who view porn may develop distorted and unrealistic expectations about the appearance of a normal woman's body, thus impairing the healthy development of their self-esteem.[42] Girls who view porn, too, may internalize the message that women are supposed to play only a "supporting role" in sex, thus compromising their own agency.[43]

32. In addition, there is considerable research showing that pornography users, especially young people, say that over time they need to view more extreme and violent porn in order to reach the same sexual satisfaction.[44]

Conclusion

33. The evidence presented in this declaration demonstrates the urgent need for an age verification law in Louisiana to address the pervasive harms of pornography on young people. The research findings, supported by a large body of peer-reviewed scientific studies from multiple disciplines, clearly highlight the detrimental effects of pornography on the social, emotional, and cognitive well-being of children and adolescents.

34. One of the most alarming revelations is that pornography has become the major form of sex

education for children, with the average age of first exposure being as young as 11. The easy accessibility of pornographic content through digital devices, coupled with the violent and non-consensual nature of mainstream pornography, creates a toxic environment for young minds.

35. Children are being exposed to explicit acts of violence, coercion, and sexual aggression, which normalizes and perpetuates harmful behaviors against them, and increasingly, by them (especially boys) as perpetrators.

36. The research unequivocally demonstrates that pornography consumption is associated with a range of negative outcomes for young people. These include promoting coercive behavior, sexual violence, depression, drug and alcohol abuse, cyberbullying and cyberstalking. The addictive nature of pornography leads to poor social integration, poor academic and work performance, and impaired social functioning.

37. Furthermore, the findings reveal that pornography viewers, especially boys, are more likely to emulate what they see in pornography, including sexual strangulation, verbal or physical coercion, and dating violence. The normalization of abusive and non-consensual sexual practices in mainstream pornography contributes to a distorted perception of healthy relationships and consent among young people.

38. Importantly, the research highlights the alarming connection between pornography consumption and the perpetration of child sexual abuse. Minors who view pornography are at a higher risk of engaging in illegal activities such as seeking out child pornography and developing paraphilias. For girls, early exposure

to pornography increases the likelihood of suffering sexual abuse, coercion, and aggression.

39. The porn industry is highly concentrated and lightly regulated, and dominated by the company MindGeek, which owns Porhhub and many other sites that offer vast amounts of free images and videos. The company has been associated with cases of child exploitation, non-consensual images, and sex trafficking. The industry facilitates individual and societal harms through its dominance in the online pornography market and its cynical efforts to masquerade as a bastion of free speech.

40. The findings presented in this declaration are supported by a wealth of scientific research, demonstrating the harmful impact of pornography on young people. It is essential to prioritize public health and safeguarding the well-being of our youth by implementing age verification laws that restrict minors' access to harmful pornographic content, thereby mitigating the negative impacts on their mental, emotional, and social development.

41. The age verification laws will help to protect the development and healthy growth of future generations, empowering them to form healthy relationships, promote consent, and foster a society free from the damaging effects of pornography

Executed on this16th day of July, 2023, in the United States, Massachusetts.

/s/ Gail Dines
Gail Dines PhD.

[1] https://academicinfluence.com/rankings/people/women-scholars/sociology

[2] http://www.beacon.org/Pornland-P891.aspx

[3] E.g., Rothman, E. F., & Adhia, A. (2015). Adolescent pornography use and dating violence among a sample of primarily black and Hispanic, urban-residing, underage youth. *Behavioral sciences*, *6*(1), 1,

[4] Chen, A. S., Leung, M., Chen, C. H., & Yang, S. C. (2013). Exposure to internet pornography among Taiwanese adolescents. *Social behavior and personality: An international journal*, *41*(1), 157-164.

[5] Allen, K. R., & Lavender-Stott, E. S. (2015). Family contexts of informal sex education: Young men's perceptions of first sexual images. *Family Relations*, *64*(3), 393-406.

[6] https://www.apa.org/news/press/releases/2017/08/pornography-exposure

[7] Bloom, Z. D., & Hagedorn, W. B. (2015). Male adolescents and contemporary pornography: Implications for marriage and family counselors. *The Family Journal*, *23*(1), 82-89.

[8] Children see pornography as young as seven, new report finds, BBFChttps://www.bbfc.co.uk/about-us/news/children-see-pornography-as-young-as-seven-new-report-finds.

[9] https://www.newyorker.com/magazine/2016/09/26/making-sense-of-modern-pornography

[10] Bridges, A. J., Wosnitzer, R., Scharrer, E., Sun, C., & Liberman, R. (2010). Aggression and sexual behavior in best-selling pornography videos: A content analysis update. *Violence against women*, *16* (10), 1065-1085.

[11] Fritz, N., Malic, V., Paul, B., & Zhou, Y. (2020). A descriptive analysis of the types, targets, and relative frequency of aggression in mainstream pornography. *Archives of Sexual Behavior*, 1-13. doi:10.1007/s10508-020-01773-0

[12] Bichard, H., Byrne, C., Saville, C. W., & Coetzer, R. (2020). The neuropsychological outcomes of non-fatal strangulation in domestic and sexual violence: A systematic review. *Neuropsychological rehabilitation* 32.6 1164-1192

[13] My research conducted July 15th, 2023

[14] https://openparliament.ca/committees/health/42-1/50/dr-sharon-cooper-1/

[15] https://www.pornhub.com/insights/2022-year-in-review

[16] Dines, G., & Sanchez, M. (2023). Hentai and the Pornification of Childhood: How the Porn Industry Just Made the Case for Regulation. *Dignity: A Journal of Analysis of Exploitation and Violence*, *8*(1), 3.

[17] British Board of Film Classification. (2022, December 6). New BBFC research reveals children are more exposed to sites specialising in non-photographic pornography, compared to adults. https//www.bbfc.co.uk/about-us/news/new-bbfc-research-reveals-children-are-more-exposed-to-sites-specialising-in-non-photographic-pornography-compared-to-adults

[18] See, e.g., Bernstein, S., Warburton, W., Bussey, K., & Sweller, N. (2023). Mind the Gap: Internet Pornography Exposure, Influence and Problematic Viewing Amongst Emerging Adults. *Sexuality Research and Social Policy*, *20*(2), 599-613; Castro-Calvo, J., Cervigón-Carrasco, V., Ballester-Arnal, R., & Giménez-García, C. (2021). Cognitive processes related to problematic

pornography use (PPU): A systematic review of experimental studies. *Addictive Behaviors Reports*, *13*, 100345; Alexandraki, K., Stavropoulos, V., Anderson, E., Latifi, M. Q., & Gomez, R. (2018). Adolescent pornography use: A systematic literature review of research trends 2000-2017. *Current Psychiatry Reviews*, *14*(1), 47-58.

[19] Rodríguez-Castro, Y., Martínez-Román, R., Alonso-Ruido, P., Adá-Lameiras, A., & Carrera-Fernández, M. V. (2021). Intimate partner cyberstalking, sexism, pornography, and sexting in adolescents: new challenges for sex education. *International journal of environmental research and public health*, *18*(4), 2181.

[20] George, M., Maheshwari, S., Chandran, S., & Rao, T. S. (2019). Psychosocial aspects of pornography. *Journal of Psychosexual Health*, *1*(1), 44-47.

[21] Herbenick, D., Fu, T. C., Eastman-Mueller, H., Thomas, S., Svetina Valdivia, D., Rosenberg, M., ... & Feiner, J. R. (2022). Frequency, method, intensity, and health sequelae of sexual choking among US undergraduate and graduate students. *Archives of sexual behavior*, *51*(6), 3121-3139.

[22] Bernstein, S., Warburton, W., Bussey, K., & Sweller, N. (2022). Pressure, preoccupation, and porn: The relationship between internet pornography, gendered attitudes, and sexual coercion in young adults. *Psychology of Popular Media***.**

Pornography, Gendered Attitudes, and Sexual Coercion in Young Adults," Psychology of Popular Media 12(2), 2023, 159-172, https://doi.org/10.1037/ppm0000393; see also Dillard, Rebecca, et al. "Abuse disclosures of youth with problem sexualized behaviors and trauma symptomology." Child abuse & neglect 88 (2019): 201-211; Emily A. Waterman, et al., Prospective

Associations Between Pornography Viewing and Sexual Aggression Among Adolescents, Journal of Research on Adolescence 32, 4, 2022, 1612-1625, DOI: 10.1111/jora.12745

[23] Kara Anne E. Rodenhizer and Katie M. (2019). The Impacts of Sexual Media Exposure on Adolescent and Emerging Adults' Dating and Sexual Violence Attitudes and Behaviors: A Critical Review of the Literature. Trauma, Violence, & Abuse, 20(4), 439–452. https://doi.org/10.1177/1524838017717745

[24] Martellozzo, E., Monaghan, A., Adler, J. R., Davidson, J., Leyva, R., & Horvath, M. A. H. (2016). "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. Middlesex University, NSPCC, OCC. https://doi.org/10.6084/m9.figshare.3382393

[25] Fiona Vera-Gray and others, Sexual violence as a sexual script in mainstream online pornography, The British Journal of Criminology, Volume 61, Issue 5, September 2021, Pages 1243–1260, https://doi.org/10.1093/bjc/azab035

[26] Ethan A. Marshall, Holly A Miller, and Jeff A Bouffard, "Crossing the Threshold From Porn Use to Porn Problem: Frequency and Modality of Porn Use as Predictors of Sexually Coercive Behaviors." Journal of interpersonal violence vol. 36,3-4 (2021): 1472-1497. doi:10.1177/0886260517743549). See also Nicky Stanley, et al., Pornography, Sexual Coercion and Abuse and Sexting in Young People's Intimate Relationships: A European Study, Journal of Interpersonal Violence 33, 19, 2018, 2919-2944, https://doi.org/10.1177/0886260516633204

[27] Paul J. Wright, Bryant Paul & Debby Herbenick (2021) Preliminary Insights from a U.S. Probability Sample on Adolescents' Pornography Exposure, Media Psychology, and Sexual Aggression, Journal of Health Communication, 26:1, 39-46, DOI:10.1080/10810730.2021.1887980; Rostad, W.L., Gittins-Stone, D., Huntington, C. et al. The Association Between Exposure to Violent Pornography and Teen Dating Violence in Grade 10 High School Students. Arch Sex Behav 48, 2137–2147 (2019). https://doi.org/10.1007/ s10508-019-1435-4; Jochen Peter & Patti M. Valkenburg (2016) Adolescents and Pornography: A Review of 20 Years of Research, The Journal of Sex Research, 53:4-5, 509-531, DOI: 10.1080/00224499.2016.1143441

[28] Tegan Insoll, et al., "Risk Factors for Child Sexual Abuse Material Users Contacting Children Online: Results of an Anonymous Multilingual Survey on the Dark Web," Journal of Online Trust and Safety 1 (2), 2022, https://doi.org/10.54501/jots.v1i2.29

[29] Aina M. Gassó and Anna Bruch-Granados, Psychological and Forensic Challenges Regarding Youth Consumption of Pornography: A Narrative Review, Adolescents 1, 2021, 108-122, https://doi.org/10.3390/adolescents1020009

[30] Sarah J. Harsey, et al., "Women's Age of First Exposure to Internet Pornography Predicts Sexual Victimization," *Dignity: A Journal of Analysis of Exploitation and Violence* 6 (5), 2021, Article 1, https://doi.org/10.23860/dignity.2021.06.05.01

[31] Sandra Feijóo, "Cyberbullies, the Cyberbullied, and Problematic Internet Use: Some Reasonable Similarities," *Psicothema* 33 (2), 2021, pp. 198-205, doi: 10.7334/psicothema2020.209; Meghan N. Long and Elizabeth B. Dowdell, "Online and Health Risk

Behaviors In High School Students: An Examination of Bullying," *Pediatric Nursing* 44 (5), 2018, pp. 223-228

[32] Meghan Donevan, et al., "Adolescents' Use of Pornography: Trends over a Ten-year Period in Sweden," Archives of Sexual Behavior 51, 2022, pp. 1125–1140, https://doi.org/10.1007/s10508-021-02084-8

[33] Sarah Boer, et al., "Prevalence and Correlates of Sext-Sharing Among a Representative Sample of Youth in the Netherlands," Frontiers in Psychology 12, 2021, Article 655796, doi: 10.3389/fpsyg.2021.655796; Karen M. Holt, et al., "Assessing the role of self-control and technology access on adolescent sexting and sext dissemination," Computers in Human Behavior 125, 2021, Article 106952, https://doi.org/10.1016/j.chb.2021.106952

[34] Eric Silverman, The Harms of Sexting: Scholarly Literature Review, 2022, https://www.culturereframed.org/wp-content/uploads/2022/01/culture-reframed_harms-of-sexting.pdf

[35] Charlie Huntington, Brian Willoughby, and Galena Rhoades, "Associations of Adolescents' Pornography Viewing with their Romantic Relationship Skills and Behaviors," The Journal of Sex Research, 2022, DOI: 10.1080/00224499.2022.2096844. See also Yaniv Efrati and Yair Amichai-Hamburger, "Are adolescents who consume pornography different from those who engaged in online sexual activities?," Children and Youth Services Review 111, 2020, 104843, https://doi.org/10.1016/j.childyouth.2020.104843.

[36] Kyriaki Alexandraki, et al., "Internet pornography viewing preference as a risk factor for adolescent Internet addiction: The moderating role of classroom personality," *Journal of Behavioral Addictions* 7(2), 2018, pp. 423–32, DOI: 10.1556/2006.7.2018.34; Kyoung

Min Kim, et al., "What Types of Internet Services Make Adolescents Addicted? Correlates of Problematic Internet Use," *Neuropsychiatric Disease and Treatment* 16, 2020, pp. 1031-1041, doi:10. 2147/NDT. S247292

[37] Jennifer A. Brown and Jonathan J. Wisco, "The components of the adolescent brain and its unique sensitivity to sexually explicit material," *Journal of Adolescence* 72, 2019, pp. 10-13, https://doi.org/10.1016/j.adolescence.2019.01.006

[38] Carolina Valdez-Montero, et al., "Coercive and problematic use of online sexual material and sexual behavior among university students in northern Mexico," *Sexual Addiction & Compulsivity* 25 (4), 2018, pp. 367-379, https://doi.org/10.1080/10720162.2019.1565847; Pukovisa Prawiroharjo, et al., "Impaired Recent Verbal Memory in Pornography-Addicted Juvenile Subjects," *Neurology Research International* 2019, Article 2351638, https://doi.org/10.1155/2019/2351638

[39] Ann Rousseau, Beáta Bőthe, and Aleksandar Štulhofer, "Theoretical Antecedents of Male Adolescents' Problematic Pornography Use: A Longitudinal Assessment," *Journal of sex research* 58 (3), 2021, pp. 331-341, doi:10.1080/00224499.2020.1815637; Magdalena Mattebo, et al., "Pornography consumption and psychosomatic and depressive symptoms among Swedish adolescents: a longitudinal study," *Upsala Journal of Medical Sciences* 123 (4), 2018, pp. 237-246, https://doi.org./10.1080/03009734.2018.1534907

[40] Niccolò Principi, et al., Consumption of sexually explicit internet material and its effects on minors' health: latest evidence from the literature," *Minerva Pediatrics* 74 (3), 2022, pp. 332-339, DOI: 10.23736/S2724-5276.19.05367-2; Yolanda Rodríguez-Castro, "Intimate Partner Cyberstalking, Sexism, Pornography,

and Sexting in Adolescents: New Challenges for Sex Education," *International Journal of Environmental Research and Public Health* 18, 2021, Article 2181, https://doi.org/10.3390/ijerph18042181

[41] Megan K. Maas and Shannamar Dewey, "Internet Pornography Use Among Collegiate Women: Gender Attitudes, Body Monitoring, and Sexual Behavior," SAGE Open 8(2), 2018, https://doi.org/10.1177/2158244018786640; Kara Anne E. Rodenhizer and Katie M. Edwards, "The Impacts of Sexual Media Exposure on Adolescent and Emerging Adults' Dating and Sexual Violence Attitudes and Behaviors: A Critical Review of the Literature," Trauma, Violence, & Abuse 20 (4), 2019, pp. 439–452, https://doi.org/10.1177/1524838017717745

[42] Richard Joseph Behun and Eric W. Owens, *Youth and Internet Pornography: The Impact and Influence on Adolescent Development* (Taylor & Francis Group, 2019).

[43] Michael Tholander, "Traces of Pornography: Shame, Scripted Action, and Agency in Narratives of Young Swedish Women," Sexuality & Culture 26, 2022, pp. 1819-1839, https://doi.org/10.1007/s12119-022-09973-7

[44] Dwulit, Aleksandra Diana, and Piotr Rzymski. 2019. "Prevalence, Patterns and Self-Perceived Effects of Pornography Consumption in Polish University Students: A Cross-Sectional Study" International Journal of Environmental Research and Public Health 16, no. 10: 1861. https://doi.org/10.3390/ijerph16101861; Blinka L, Ševčíková A, Dreier M, Škařupová K and Wölfling K (2022) Online Sex Addiction: A Qualitative Analysis of Symptoms in Treatment-Seeking Men. Front. Psychiatry 13:907549. doi: 10.3389/fpsyt.2022.907549

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Civil Action No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC, et. al.,

Plaintiffs,

v.

ANGELA COLMENERO, in her official capacity as
Interim Attorney General for the State of Texas,

Defendant.

DECLARATION OF ERIK CABRERA

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

2. I am a Sergeant in the Child Exploitation Unit of the Criminal Investigations Division in the Office of the Texas Attorney General where I have been employed for 9 years. Prior to that, I spent 6 years as a law enforcement officer with Uvalde County Sheriff's Department.

3. As part of my job with the Texas OAG, I conduct investigations involving the online sexual exploitation of children. I have to visit porn websites on a daily basis.

4. After reading paragraph 41 of the declaration of Richard L. Sonnier, I recreated the scenario he presents there. I went to Bing.com. I turned off safe search filters and searched "hot sex." The first page of results was exclusively links to Pornhub.com and

XNXX.com. Images were blurred even though I had turned off "safe search."

5. When I clicked on the "videos" tab, the vast majority of results—almost all—were for Pornhub.com, XNXX.com, xhamster.com, and xvideos.com.

6. On the main tab for all results, I clicked the first link, which directed me to XNXX.com.

7. Among other things the landing page of XNXX.com shows still shots of porn videos, 6 images across the screen and about 6 rows down. In total, about 36 still shots of porn videos. When I moved my mouse over an image, scenes from the video begin to play even if I did not click on the image.

8. Below each of the images was a title for the video. Titles on the landing page of XNXX.com included, "18yo chubby teen Alba gets her first cock up her tight ass," "Ebony Little Step Sister Cums On Step Brother's Cock," and "White Whore Fucks Biggest Black Cocks Ever."

9. XNXX.com links to various categories of videos called "Tags" on their site. There are thousands of tags available. They include "balls deep anal" (200,311 results), "family porn" (196,887), "gaping asshole" (44,380), "perfect girl porn" (306,230), "teen hardcore" (579,497), and "young petite porn" (328,273).

10. I also searched the word "bondage" in the search bar and the search bar indicated that 49,461 videos matched that tag. But it also showed that 257,987 videos matched "teen bondage." Other apparently popular categories of bondage videos include "bondage anal" (199,003), "anal bondage" (198,984), "Asian bondage" (88,713), "Japanese Bondage" (67,340), and "ebony bondage" (91,203).

11. I typed in “teen bondage” in the search bar and the site provided the top auto-fill option as “teen bondage gangbang.” I initiated that search and it returned 304,523 free videos in response with additional 18,346 available through XNXX.com Gold

12. I clicked to watch a video titled, “Using and a. the whore.” In that 36-minute video, 5 men tie up a woman with electrical tape and rope. Throughout the video, they take turns penetrating her orally, vaginally, and anally, sometimes simultaneously. At one point, a man puts his hands around her neck. The men also slap her repeatedly. While she is still tied up, the men later strap a device around her head called a “mouth spreader” or “spider mouth gag” that forces her mouth to remain open. They then take turns ejaculating into her mouth. This video had approximately 671,000 views and a 98 percent rating. During my time on XNXX.com, I came across other videos that I would prefer not to describe in this declaration.

13. I also clicked on a link to XNXX “Gold.” This portal within the website offers access to “Exclusive Content.” When I clicked the link to sign up, it took me to xxnx.gold/account/create which advertised “XNXX GOLD originals.” It also showed a picture of a man dressed in all black, with black gloves, a black handkerchief over his face, covering the mouth of a naked woman whom he appeared to be taking by surprise. The website Porndoe.com had a similar scheme where I could click to get original content.

14. I also visited the website Pornhub.com. It has the same general layout as xnxx.com, which is a common layout for porn sites, where the landing pages show photos that you can click on to view videos. Or, you can scroll over the pictures to see a preview without clicking. Among the many channels on

Pornhub.com, is a channel for Pornhub Originals which indicates Pornhub itself produces content for the site and has been doing so for about 6 years. Pornhub also has a blog.

15. Pornhub provides a "Year In Review" where it analyzes the data Pornhub collects about its visitors. One chart shows how much time each state's residents spent on Pornhub per visit, down to the second. Pornhub also identifies the most popular search terms per state.

16. On their site, Pornhub also represents that in 2019 it had 42 billion visitors, 115 million visitors per day, and 6.83 million new video uploads that constituted 1.36 million hours of new content, which, Pornhub calculates as 169 years. And the site states, "If you started watching 2019's new videos in 1850, you would still be watching them today."

17. I also visited the websites Letsdoeit.com, Superbe.com, MYLF.com, and TeamSkeet.com. The landing pages of those websites likewise show pictures of videos that you can click on to view. However, you can only view short previews, and if you click on the videos, you are taken immediately to a screen that requests payment.

18. Even for the non-subscription websites, the videos posted on the channel often act as advertisements for other porn channels. Sometimes those content creators provide free full-length videos that provide a link to the channel or content creator that posted the video. Other times the videos will include a watermark that advertises the content creator. And when you click on a video, an ad usually plays first.

19. The sites' pages are also filled with advertisements along the top banner and/or sidebars. Those ads

sometimes promote other porn sites by showing a porn video that leads to another porn site. The ads may also show male or female genitalia being stimulated by an advertised sex toy. The product or purpose of the ads varies, but they are always, or almost always, themselves pornographic.

DECLARATION UNDER PENALTY OF PERJURY

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.

/s/ *Sgt. Erik Cabrera*
Sgt. Erik Cabrera

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Civil Action No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC, et. al.,

Plaintiffs,

v.

ANGELA COLMENERO, in her official capacity as
Interim Attorney General for the State of Texas,

Defendant.

DECLARATION OF TONY ALLEN

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 global age assurance industry. I am also an audit member of the Age Verification Providers Association (AVPA) – the 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 H.B. 1811, the Complaint, and Plaintiffs' Motion for Preliminary Injunction 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 and consumers in verifying age is minimal, and reducing as technology evolves ever more.

9. Based on my knowledge and experience, software filters on devices, when properly installed, can be a useful parental tool in protecting children from online pornography, but in practice only provide a partial solution. They are less effective than, and not a substitute for, website-based age assurance which delivers a substantively different policy intent.

The availability of age verification services and how they work

10. Age Verification in the context of H.B. 1811 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.

11. 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 pornography. I am aware that age verification is already actively deployed by many adult content service providers including Dorcel, Only Fans, Jacqui & Michel, StripChat, PornHub, MyDirty Hobby, Clips4Sale, MYM, Skokka, Live Jasmin, FanCentro, Loyal Fans, Viva Street and xHamster, who are all subscribers to at least one Age Verification Provider, a company mentioned by the Plaintiffs called, Yoti[1]. These companies have applied age verification to one extent or another to their services elsewhere in the US, but also in the UK, France, Germany, Italy and in some cases, globally. PornHub have issued public information about their existing approaches to age verification[2].

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

13. 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.

[1] https://www.yoti.com

[2] https://www.pornhub.com/press/show?id=2172

14. With the explosion of pornography 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 places on the internet, while simultaneously protecting rights of speech and privacy. The goal is to create safer places online where children can enjoy and benefit from the opportunities created by the worldwide web[3].

Privacy and the security of data

15. At the same time, Europe was implementing the General Data Protection Regulations ("GDPR"), a strict data protection regime requiring application of the principles of privacy-by-design and data minimization. This reinforced the need to devise a way to prove a user's age without disclosing their identity. In the United States, Consumer Privacy Protection Laws containing similar provisions, such as the CCPA (or California Consumer Privacy Act) are also now in place. In Texas, the Texas Data Privacy and Security Act (TDPSA) contains objectives to limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purpose of processing as disclosed to the consumer[4]. Consistent with these objectives, H.B. 1811 includes a requirement not to store personal data used for the purpose of age verification. See Texas H.B. 1811 § 29B.002(b)[5].

[3] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appld=PPGMS

[4] See, Tex. H.B. 4, 88th Leg., 1st C.S. (2023)

[5] "(b) A commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) may not retain any identifying information of the individual" TEXAS H.B. 1811 § 29B.002(B).

16. In light of the foregoing, the most straightforward solution was 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. The various data protection laws globally, including in Texas, insist that providers only collect, process, and retain the data required for the specified purpose. So, generally where an Age Verification Provider 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. This approach, therefore, does not require that all visitors to an adult website transmit to it their personal information and pre-empt any data breach similar to the example of Ashley Madison.[6]

17. Age Assurance Providers who are members of the AVPA and, thus sign up to its code of conduct[7], do not create new central databases when conducting age checks for the adult industry. There are, of course, sectors such as online gambling where regulators require audit trails, but H.B. 1811 requires, and indeed the industry's general practice is, not to retain any personal 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.

[6] See, e.g., Kim Zetter, Hackers Finally Post Stolen Ashley Madison Data, Wired, Aug. 18, 2015, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data

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

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

19. 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.

20. 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 of the 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. Adult websites serving users in Texas may choose to use commercially available Age Verification providers certified by these regulatory bodies, not only to consolidate their defense against potential legal claims, but also to build consumer trust and confidence.

21. In 2017, the UK government passed the Digital Economy Act which included a provision that sought to ensure that minors could not normally access pornography without age verification. Both consumers and the adult websites themselves expressed concerns about privacy — particularly the risk that a treasure trove database of users' identities connected to the adult websites they chose to visit would be exposed by hackers. So, from the outset, privacy was a primary objective for those designing technical solutions for the age verification. Indeed, the Ashley Madison leak in 2015, cited by the Plaintiffs, was front of mind for the

adult industry after seeing the user base of that site decimated by news of the breach.

22. Any question about whether an adult site 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 are needed.

23. Although Content Providers may perform Age Verification themselves, as set forth further below, Content Providers may, and often do, contract with third-party companies ("Age Verification Providers") to perform the service for a fee. These fees, discussed in paragraphs 56 to 63 of my declaration, are considerably lower than claimed in the Plaintiffs complaint. H.B. 1811 specifically allows for third-party verification. See (ibid) Texas H.B. 1811 § 29B.002(b).

24. When using an Age Verification Provider, a Content Provider directs the consumer to provide personal information directly to the Age Verification Provider 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. This is usually in response to a binary question (is this user over 18?) to which the answer can only be 'Yes' or 'No'. It is sometimes accompanied by a statement from the Age Verification Provider about how sure they are that their answer is correct (say 99% or 99.9%). It should be noted that whilst this statement can be a very high percentage, it will never be 100%.

25. The Age Verification Provider does not generally retain a consumer's personal Information other than the date of birth, which can be used to respond to subsequent enquiries about that user's age.

26. 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 Content Providers and other websites, thereby minimizing the need for multiple age verification checks of the same individual.

27. Users may be asked to authenticate when they wish to re-use a previously completed age check. This is the process of confirming the same user who completed the check is the current user. It can be achieved simply with a password or Personal Identification Number (PIN) or for a higher level of assurance, a biometric interaction such as how users currently open their cell phone.

Methods of available age verification

28. 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.

29. Previous implementations of Age Verification solutions, such as in 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 age verification.

30. A choice of methods also addresses issues that arise from inclusivity, should any one method not be suitable for an individual.

Definitions of age verification

31. To assist the court with some terminology, I set out here the definitions and terms that are being included in international standards, including ISO/IEC 27566 — Age Assurance Systems — Framework (of

which I am the Technical Editor). 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.

b. There are three categories of Age Assurance:

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 an 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.

iii. "Age Inference" is age determination based on the possession of something or access to something from which it can be inferred that only a person over 18 could have that.

32. Age Verification may be achieved by reference to drivers' licenses, passports, electoral rolls, credit reports, cell phone network records, banking, and credit card records. Users may also choose to create a digital identity, and selectively release just their age attributes.

33. Age Estimation, on the other hand, can be achieved by analyzing facial images, voiceprints or game play. The most advanced of these, facial estimation, is 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 certification team has independently verified and validated the results of this testing by Yoti.

34. The value of Age Estimation, as described more fully below, for both Content Providers and consumers is that it does not require consumers to submit any personal information other than suppling a live facial image or saying a short phrase to create a voiceprint.

35. There are a wide range of non-exclusive reasonable age verification methods that Content Providers and Third-Party Services can adopt to assure the ages of their users to varying degrees of certainty. These methods are used across the full range of situations where online age checks are required and have been certified by the Age Check Certification Scheme, which I manage.

36. Those which would be appropriate for implementing H.B. 1811 include the following;

a. Review of Government Issued Documents

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 a "liveness" check. 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 data on the chip compared to the image on the document, and a fresh photo or video of the user.

b. Review of Credit reports and other private sector databases

In this method, users typically enter their name, address, and date of birth (Either specifically for the purposes of age verification or as part of their account opening or 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.

c. Review of digital identity apps

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. Based on information and belief, I understand that Texas does not yet have a state issued digital identification card or app.

d. Submission of Credit Card number

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

e. Review of bank records

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 them 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 the Age Verification Provider.

f. Age estimation via facial, voice, or behavioral analysis

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.

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 still or video image, or an existing profile picture can be used, 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, so is not deemed to be sensitive personal information by law and regulation, but in any event can and should be instantly deleted. In addition, this form of technology is not trained with associated names or addresses.

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 image matching takes place for the purpose of estimating age.

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.

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.

This method is inclusive of people of all ages, who do not own or have access to a government issued document. Age Estimation by facial or voice technology is one tool in a toolbelt. For example, for a law that requires a user to be aged 18 or older, such technology may be useful for assuring that individuals are, say, 21 years or older even if the Content Provider and Ag Verification Provider 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 user.

37. Other methods of reasonable age verification, but which have not been subject to independent testing and certification, may include physical checks and vouching.

a. Physical Check

This is where a user is enrolled into an age assurance program in person. 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 certified the user to be over 21.

b. Vouching

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.

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

1. you have an existing relationship with the user;
2. you are sure the user is who they say they are;
3. you are in a position of authority in their community; and
4. you have proved your own identity

38. H.B. 1811 allows for a wide range of the reasonable 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.

39. There are other methods of age assurance that are less reliable than those previously discussed and, subject to the facts of any specific subsequent case, may not amount to reasonable age verification methods for the purpose of H.B. 1811.

40. An example is known as Attestation or Self-Declaration. This is not considered a method that provides any assurance about the user's 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, then it may not be a problem to assume they are and protect them from harmful material on the internet. 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.

41. 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. 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.

42. 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 and the international standards the industry has developed.

Accuracy of methods, geolocation and circumvention

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

44. Regulators, or a regulated business, can determine this "level of assurance." For example, regulators or regulated businesses might use different processes for alcohol sales, gambling, pornography access, and knife, gun or ammunitions purchases.

45. The plaintiffs express a concern that "minors can use virtual private networks (VPNs), proxy servers, the "Tor" browser, and numerous other circumventions to bypass the Act's verification requirements with ease." Many online services already block traffic from well-known VPNs. For example, UK television channels the BBC and ITV[8] actively prevent users from pretending to be in a different geographical location in order to access content they would otherwise be unable to view from their real location. The most common way to achieve this is to look out for a single internet protocol (IP) address which is generating significantly more traffic than other IP addresses, which is a characteristic of most VPN traffic. There are specialist services that allow businesses to check if a user's IP address is associated with a VPN or TOR[9], as

[8] "Potentially blocked up to 1M pirate viewers in the historic England v. Denmark Euro 2020 match" https://www.geocomply.com/resources/case-study/itv-tackles-streaming-piracy-with-geoguard/

[9] https://focsec.com

well as open-source lists[10] to assist sites which wish to prevent the use of VPNs. Generally, only more expensive, premium VPN services offer each user a new and unique IP address which is harder to identify and block. These are considerably more expensive than the most widely used VPNs, making it harder for most minors to take advantage of their services.

46. The online gaming industry already makes extensive use of compliance services which require gaming operators to validate a customer's location to prove that the customer is located in a state or jurisdiction which permits online betting and gaming. One of the leading geolocation compliance providers is GeoComply. The company is licensed by state gaming regulators and its technology is tested for accuracy and adherence to regulatory standards. GeoComply conducts up to 1 billion geolocation transactions monthly from apps installed on 400m devices worldwide which allow a user to prove where they really are located. The company "Collects geolocation signals from multiple sources, including: GPS, WiFi, GSM, browser/HTML5 and IP address" to verify location accuracy. Further, GeoComply technology detects the use of location "spoofing" software or other methods of location obfuscation as is required under various state laws and regulations[11].

47. Age verification providers have invested heavily in anti-spoofing technology. This includes a number of techniques intended to reduce circumvention or 'spoofing' of age verification systems, including:

[10] https://github.com/X4BNet/lists_vpn/blob/main/ipv4.txt

[11] https://cdn.geocomply.com/wp/app/uploads/20230528242903/GeoComply-Core_Brochure_Gaming.pdf

a. Liveness detection is generally deployed to ensure that where a facial image is used for facial age estimation, or is required for comparison with the photograph supplied as part of a government-issued ID, it is of a live human being who is presently using the device through which the age check is being completed.

b. Fake or altered documents are detected using a wide range of techniques. For example, AU10TIX employs a dual-layered defense against fake or altered documents. The aim is to combat not just visible fraud but also professional, organized-crime level of manipulations that employ advanced tools and possibly insider-expertise. AU10TIX case-level detection goes forensic in detecting altered as well as "manufactured" fakes, while AU10TIX traffic-level detection is detecting professional attack behavior, even when document manipulations are well hidden.

c. The combination of case-level forensics and traffic-level detection has shown that the currently known fraud statistics do not reflect the actual magnitude of fraud activity, with more sophisticated fraud (such as one utilizing generative AI Deepfake) technology actually showing constant increase "thanks" to the increasing availability of off-the-shelf tools.

d. Stolen documents can be detected by checking against published lists of compromised identity documents.

48. In general, the objective of most legislation in this field has been to ensure that sexually explicit content is not normally accessible by minors. In other words, most children should be prevented from seeing most adult content most of the time. Neither age verification nor age estimation techniques can guaran-

tee 100 per cent accuracy, any more than staff in an adult bookstore are infallible when they check the age of their customers. But the technology is more than capable of preventing an adult website from knowingly giving access to children, as is the standard required in H.B. 1811[12].

Re-usability

49. 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.

50. This approach means the technology exists now to ensure that H.B. 1811 does not threaten the principle of navigating seamlessly between many websites 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.

51. Historically, the Age Verification 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 sites they are just

[12] "CIVIL PENALTY; INJUNCTION. (a) If the attorney general believes that an entity is knowingly violating or has knowingly violated this chapter..." Texas H.B. 1811 § Sec.129B.006.

visiting temporarily, this could quickly become inconvenient and expensive. 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.

52. A project was developed in six member states of the European Union, but has since opened up worldwide and includes major US companies to further develop the concept. 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 in the United States, as many states, including Texas, move to require age verification.

53. 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. As these are held locally on the device, there is no centralized 'honeypot of data that could be the target of a hack (this is sometimes referred to as decentralized identity attributes). This significantly reduces the risk of data compromise at scale and, in any event, it only indicates that a user is over 18 and nothing about the reasons why they may have needed to prove that (it could be buying tobacco, gambling, gaming, car hire, accessing pornography or anything with an age-related eligibility criteria).

54. 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 the internet, as their clients do not wish to drive any users away.

55. 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.

The Cost of Age Verification

56. 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.

57. 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.

58. The Plaintiff has set out a table of costs in their complaint (at paragraph 46). In my opinion, the Plaintiffs are quoting costs for identity verification

here (sometimes referred to as 'Know-your-customer' (KYC) checks). These are of an order more expensive than age verification checks (which are merely verifying one attribute (your age) and not all aspects of your identity (like full legal name, address, previous addresses, marital status, credit, etc).

59. As a leader of an independent conformity assessment body, I cannot speak to the specific pricing offered by every individual provider, but the UK Government recently published an Impact Assessment for the Online Safety Bill 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. I am aware of some providers who offer age verification at no cost to certain sectors as part of a wider digital identity service and others have shared with me further details of their pricing which they are content to be shared in public.

60. Trustmatic, one of the providers quoted by the Plaintiff, have been willing to confirm that the plaintiff has incorrectly interpreted its pricing. Face biometric based age verification, according to their public pricing on our website, starts at EUR 0.39 per verification (for 100 monthly verifications) and goes to EUR 0.14 per verification (for 30,000 monthly verifications). While this provider does not publicly publish pricing for volumes above 30,000 monthly, it has confirmed that it would charge EUR €18,000 for 100,000 verifications, not USD $40,000 as stated by the plaintiff. The claim that Trustmatic's pricing for 1M and 100M transactions is EUR 0.40 per TRX is therefore also incorrect. Their batch pricing for a batch of 1M transactions is EUR €50,000, or EUR 5 cents each; for a batch of 100M, they would charge €1 million, which is just

1 EUR cent each. To give a specific example, in order to help MindGeek fulfil legal obligations under the Bill, and to help address the issue of minors accessing restricted online content, Trustmatic would consider pricing of not more than EUR 3 cents per user to carry out selfie-based age checking on their users based in the State of Texas (subject to scoping — obviously this does not constitute a legally binding offer).

61. Yoti, another provider quoted by the Plaintiff, have confirmed to me that the pricing of £l.20 is quoted incorrectly, out of context and not relevant for this use case. The sterling £1.20 refers to list price i.e. for low volumes of document based identity verification checks (following the one-off upload of a government issued identity document and including identity document authenticity check, liveness detection, data extraction, face match). List pricing is where an organisation is not accessing any volume discounts - i.e. that would not be the case of a global adult site. Yoti state that their Age Verification Service (AVS) pricing ranges between $0.03 (for large volumes eg circa 100 M, $0.10 for circa 5M checks and $0.31 for lower volumes, one time account based checks e.g. under 100,000). They also offer free, $0.0 shares of 18 plus attributes from the reusable Yoti digital identity app, as explained below. The pricing will be dependent upon the age method, monthly volumes and whether the relying party is performing a one-time account based age check or an anonymized returning guest age check.

62. It is also important to highlight that adult content websites can be configured to recognize age attributes from certain age verification app wallets or data stores. These can sometimes be shared free of charge, including the Yoti app which is free for anyone sharing Over Age (eg Over 18). This is a one-time setup, taking

3-5 minutes, which can be created any time and thereafter reused to share age or identity details, privately, with relying parties across multiple industries.

63. The plaintiffs refer to a 700-word blog[13] by Jason Kelley, Activism Director at the Electronic Frontier Foundation, and its Senior Staff Attorney, Adam Schwartz, which argues that "there is no current method that does not carry inherent, unacceptable disadvantages and harms."

a. They claim that "This scheme [age verification] would lead us further towards an internet where our private data is collected and sold by default." This is unequivocally prevented by Age Verification providers not retaining centrally, in any new databases, personally identifiable information about the users, or any record of their online behavior. And where facial or voiceprint estimation methods are operated on a user's own device, personal data need not be shared even temporarily, and when it is, it is not retained by certified Age Verification providers.

b. The authors further state that "The tens of millions of Americans who do not have government-issued identification may lose access to much of the internet." which ignores the methods of facial and voiceprint age estimation and vouching, that can both enable undocumented people to verify their age online.

c. And they are concerned that "anonymous access to the web could cease to exist." The existing age verification industry has as its founding principle that the essence of age verification is proving your age

[13] See, e.g., Jason Kelley and Adam Schwartz, Age Verification Mandates Would Undermine Anonymity Online, Electronic Frontier Foundation, March 10, 2023, https://www.eff.org/deeplinks/2023/03/age-verification-mandates-wound-undermine-anonymityonline

without disclosing your identity. The only information given to the sites a user wishes to access is "Pass" or "Fail" in answer to a question about their age qualification.

64. Furthermore, there is no "accessible ledger of adults who view adult content" created by the Age Verification industry, as the plaintiffs fear, because personally identifiable data is not retained. But even if the anonymized records of users who had proven their age online were somehow deciphered, it would offer only a list of adults who had variously purchased alcohol on the internet, placed a bet online, or any US parent or guardian of a child under the age of thirteen, to whom they had given consent to share their personal data under the Childrens Online Privacy Protection Act (COPPA)[14]. It would be a very long list and give no indication which subset of users had proven their age to access adult content.

65. While it is true that, as the complaint argues, "Hackers are targeting information shared on the internet at exponentially high rates," they are aware there is nothing of interest to be found by targeting certified Age Verification providers who store no personal data. The example given from Louisiana is of an attack on "MOVEIt" software which allows large amounts of data to be transferred, not of the LA Wallet.[15] Indeed, LA Wallet has confirmed to me that

[14] See 15 U.S.C. §§ 6501-6506 and 16 C.F.R. §§ 312.1-312.13

[15] This attack, reportedly carried out by the Clop ransomware group, did not specifically target mobile driver's licenses in the state or anywhere else, but the nuances of data thievery, such as they are, might get lost on residents, many of whom are skeptical of things like mDLs [mobile Drivers Licenses]." https://www.biometricupdate.com/202306/theft-of-drivers-license-data-in-louisiana-could-be-a-big-test-for-digital-id

it was not affected by the recent MOVEit data breach[16].

Adding the latest encryption techniques

66. 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://bitly/3EB1ISN [hereinafter CNIL Report].

67. The CNIL Report states:

a. "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."

b. "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."

Age Verification around the world

68. The EU Better Internet for Kids Strategy mirrors the same desire as H.B. 1811: "Our vision is for age-appropriate digital services, with every child in

[16] https://nextsteps.la.gov/substitute-notice/

Europe protected, empowered, and respected online, and no one left behind."

69. The UK Parliament expects to pass the Online Safety Bill in September 2023. 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 latest Bill is focused on children whose personal data is particularly sensitive. Maintaining the anonymity of children is a core design principle for the age verification sector.

70. 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.

71. There are many examples of increasing requirements for age verification for access to adult content online which are all aligned with Texas H.B. 1811.

Effectiveness of other methods

72. Other methods exist to advance the goal of protecting children from harmful material on the internet, including content filtering at the browser

and/or the device level. These are parental controls. They can be device or browser 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.

73. We know from repeated research by the UK's telecom's regulator, OFCOM, that many parents are unaware of this technology[17]. 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. "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." Children can be very persuasive, and parents might release the controls to allow them to play a game designed for 18+, unaware the game itself may be a portal to pornographic or other unsuitable content.

74. I do agree with the Plaintiffs that filtering technology includes not only Domain Name System (DNS) filtering, but also artificial intelligence (AI). However, it should be noted that DNS filtering fails when "DNS over HTTPS" is used to cloak a user's usage. This is easily adopted and has been standard

[17] (https://www.ofcom.org.uk/__datalassets/pdf_file/0024,234609/ehildrens-media-use-and-attitudes-report-2022.pdf)

for US users since 2019 if they use a Firefox/Mozilla browser, so this control is easily circumvented.[18]

75. The ability of AI, particularly if it only operates locally on the device, browser or router, to detect adult content is also limited. The most widely used approach is digital fingerprinting of known illegal content, for example using PhotoDNA, but this is limited to detecting known CSAM, Terrorist and other illegal content so cannot be considered to be AI based.

76. Filtering has proven an ineffective mechanism, as the level of exposure to adult content by minors clearly demonstrates. A survey of US parents by Kapersky in 2021 found that 48% used parental controls.[19] However, research from the Oxford Internet Institute, University of Oxford has found that Internet filtering tools are ineffective and in most cases, were an insignificant factor in whether young people had seen explicit sexual content[20].

77. Internet service providers are thus exploring many other methods for reducing the exposure of explicit material to general browsers. Google, as an example, has recently announced that it will blur by default search results containing sexually explicit

[18] https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[19] (https://usa.kaspersky.com/about/press-releases/2021_study-finds-50-of-parents-use-parental-control-apps)

[20] Andrew K. Przybylski, Victoria Nash. Internet Filtering and Adolescent Exposure to Online Sexual Material. Cyberpsychology, Behavior, and Social Networking, 2018; 21 (7): 405 DOI: 10.1089/cyber.2017.0466

content for all users, not only those who register as minors or turn on their "safe-search" facility[21].

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

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

79. The user need only complete the age-assurance process once before they can reach their subsequent objectives. For websites and apps where users create accounts, the users may only have to complete the age-assurance process one time. After that, the website or app 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. Websites and apps that do not have user accounts need not force their users to repeat the 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.

80. 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 AVPA members, Privately and Yoti.[22] There is already

[21] https//techcrunch.com/2023/02/07/google-will-soon-blur-explicit-imagery-in-search-results-by-default/

[22] *See* https://www.yoti.com/blog/safety-tech-challenge-fund-2021 and https://www.privately.eu/age-estimation/

technology in use to detect injection attacks (where a fake computer-generated image replaces that from a webcam) and prevent spoofing.

81. 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.

82. 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.

83. 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 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.

84. 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, 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.

85. And, of course, users may choose any of many other methods to prove their age, including facial age estimation where neither credit card numbers nor any personal data is required. Also, Age Verification 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.

86. H.B. 1811'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

87. H.B. 1811 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. Age checks online can, in fact, be completed in a more privacy-preserving manner than offline, because other personal data visible on a drivers' license is not shown in the process. 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.

88. H.B. 1811 does not jeopardize First Amendment 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. Many of the Plaintiff's members are already embracing age verification technologies both elsewhere in the United States, but also globally.

DECLARATION UNDER PENALTY OF PERJURY

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.

/s/ Tony Allen
Tony Allen, Subject Matter Expert

/s/ Tony Allen
Tony Allen (Aug 18, 2023 15:32 GMT+1)

Aug 18, 2023

Texas – Adult – Declaration of Tony Allen FINAL

Final Audit Report 2023-08-18

Created: 2023-08-18

By: Tony Allen (tony.allen@accscheme.org.uk)

Status: Signed

Transaction ID: CBJCHBCAABAA78Qo5Ehzt0cXggZRijZ_6aaemYRoxrLK

“Texas - Adult Declaration of Tony Allen FINAL” History

Document created by Tony Allen (tony.allen@accscheme.org.uk)
2023-08-18 - 2:29:45 PM GMT- IP address: 150.220.172.34

Document emailed to tony.allen@accscheme.com for signature
2023-08-18 - 2:31:11 PM GMT

Email viewed by tony.allen@accscheme.com
2023-08-18 - 2:31:50 PM GMT- IP address: 150.220.172.34

Signer tony.allen@accscheme.com entered name at signing as Tony Allen
2023-08-18 - 2:32:09 PM GMT- IP address: 150.220.172.34

Document e-signed by Tony Allen (tony.allen@accscheme.com)
Signature Date: 2023-08-18 - 2:32:11 PM GMT - Time Source: server- IP address: 150.220.172.34

Agreement completed.
2023-08-18 - 2:32:11 PM GMT

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC., *et al.*,
Plaintiffs,
v.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,
Defendant.

REBUTTAL DECLARATION OF RICHARD L. SONNIER III IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Richard L Sonnier III, declare as follows:

1. I have been retained by Plaintiffs in the above captioned matter to provide technical expertise in the areas of Internet technologies and operations including age verification of users, content filtering, parental controls, family safe usage, the cost of implementing Internet technologies, the cost of operating Internet technologies, Internet privacy, Internet standards, cybersecurity, and Internet regulations.

2. I have reviewed Defendant's Opposition, as well as the Declarations of Erik Cabrera and Tony Allen.

3. Mr. Cabrera states that he had trouble reproducing my results with the Bing search engine. Cabrera Decl. at ¶ 4. On a second computer, I performed the procedure described in my previous declaration with

the Bing search engine and confirmed my results. I cannot speculate about why Mr. Cabrera observed blurred images in his search results, but I am happy to assist Mr. Cabrera in replicating my results.

4. Also, Mr. Cabrera states "the vast majority of results – almost – all were for Pornhub.com, XNXX.com, xhamster.com, and xvideos.com." I ran a search on Bing for "sucks cock," and the resulting images were from primarily eporner.com, xbabe.com, and mylust.com. The video results included videos from xhamster.com and spankbang.com.

5. The Opposition brief states (Opp. at p. 12): "According to their declarant, Richard L. Sonnier, a child could search Bing.com for "hot sex" and instantly gain access to porn that way. Dkt. 5-2. But the websites and videos that populate from that search are porn websites that would be subject to HB 1181. Notably, under current conditions, the vast majority—if not all—of the results are Plaintiffs' websites."

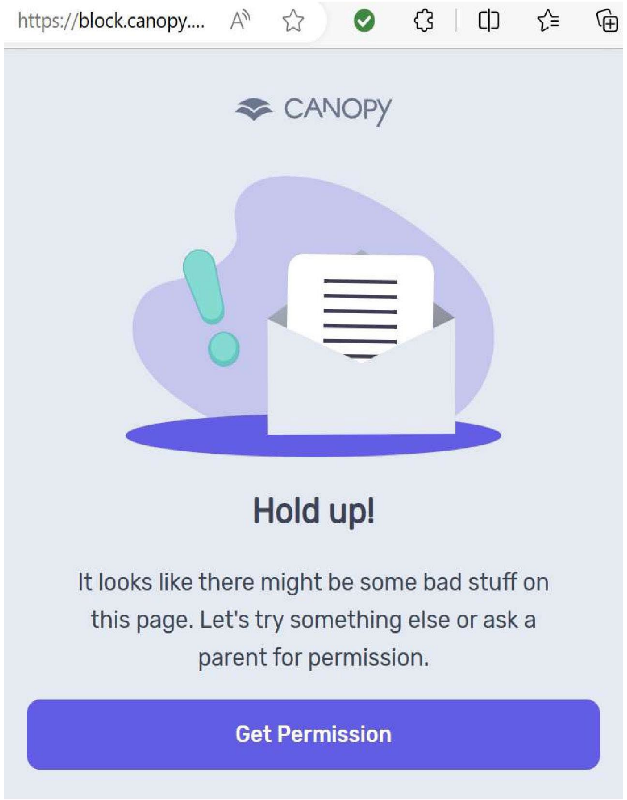
6. If the above-quoted statement implies that age verification protocols would change the search results from search engines so that explicit images and videos from adult websites would no longer appear in the search results, then the Defendant is mistaken due to the way search engines operate. When a search engine scans a website, which is a routine process, it captures the images and videos on that website regardless of any age verification protocols on that website that might prevent a human user from accessing that website. Any website that wants to be in search engine results must be configured to follow search engine procedures. One such procedure is to distinguish between human users and search engine scans when accessing the website. For example, Bing explains how to do this for the Bing search engine. See https://

www.bing.com/webmasters/help/which-crawlers-does-bing-use-8c184ec0. Indeed, search engine scans are automated, userless, machine-run processes without ages so that age verification protocols cannot work. When responding to a search by a user, the search engine sends the previously captured images or videos to the user in the search results without contacting the original website from which the images or videos were captured. As a result, any age verification protocols on the original website do not apply to the search engine results.

7. Mr. Allen refers to survey studies to support his claim that filtering is an "ineffective mechanism." Allen Decl. at ¶ 76. For example, Mr. Allen refers to an Oxford study by Przybylski and Nash. I reviewed that reference; and it does not find that Internet content filtering technology does not work (below I will explain that it absolutely does work), rather it reaches a social science statistical analysis that this known-to-work technology is not being implemented properly within UK and EU society.

8. Content filtering software for parents is actually an implementation of a general technology at work across the Internet. In general, Internet content filtering is simply indexing by category or keyword the context of the Internet, i.e., websites; and then allowing users to use that index to see what they want or to block what they do not want. Internet content filtering is what Bing does, for example. When I and Mr. Cabrera turned Bing's "SafeSearch" function on and off, we were doing Internet content filtering; and both of us have confirmed that it absolutely works. Furthermore, parental control applications that expand upon Internet content filtering work as well. I have personally confirmed the effectiveness of the parental control application called Canopy.

9. To do this, I went to the canopy website (canopy.us) and clicked on the “Start Free Trial” button. I provided an email address and entered my own password exceeding Canopy’s password requirements. Next, I selected one of Canopy’s subscription plans. I chose the mid-level plan. I entered a credit card. As part of the free trial, the first seven days are free. This created my account and placed me directly into a web console where I could start protecting my devices. I added two devices. One was a Windows PC, and the other an Android smart phone. Then I repeated the procedure from my First Declaration on the Bing search engine with the search terms “hot sex.” I received the following instead of my previous results:



Hold up!

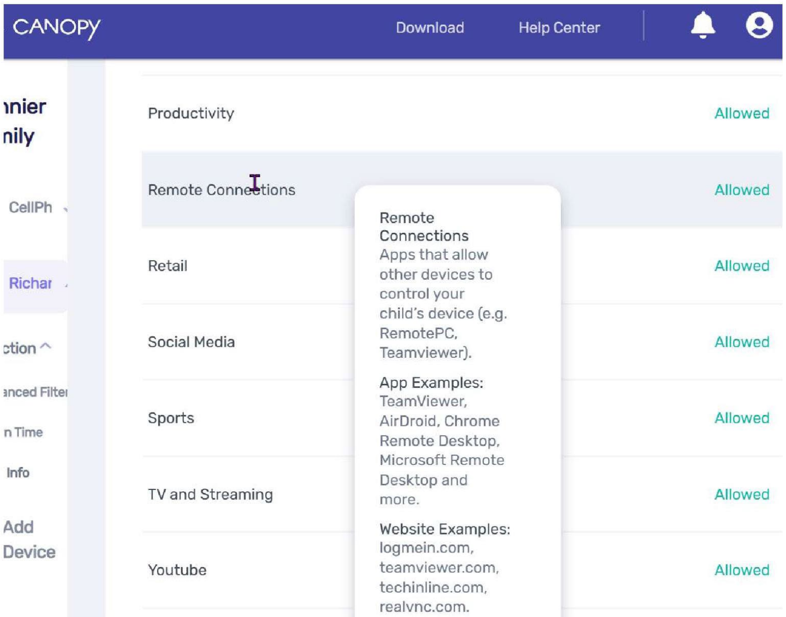
It looks like there might be some bad stuff on this page. Let's try something else or ask a parent for permission.

10. In my previous declaration, I discussed that one advantage of parental control applications is their ability to tune the protection to specific preferences. Here, Canopy automatically forced Bing's "SafeSearch" function to "strict," blocking explicit sexual material. However, for older teenagers, Canopy allows parents to grant permission if desired.

11. Canopy allows parents to permit access to social media sites while still blocking explicit sexual content. For example, I was able to go to the social media site Reddit, https://www.reddit.com/t/nfl/, while Canopy was installed. I then tried to enter a "subreddit" containing sexually explicit material, https://www.reddit.com/r/gonewild/. Although Canopy did not block the Reddit page banner that included a sexually explicit image, it blocked every sexually explicit image within the subreddit thread posted by Reddit users, as I saw when I scrolled down several days' worth of posts.

12. Canopy blocked access to Pornhub.com, xnxx.com, and other sites operated by the Plaintiffs in this action.

13. Also, I found that Canopy blocks the Tor Browser, described in my previous declaration, and prevents it from connecting to the Tor network. Additionally, Canopy blocks alternative web browsers like Brave that can circumvent its protections. While it does not block them by default, Canopy allows parents to block remote desktop applications like TeamViewer:



Productivity Allowed

Remote Connections Allowed

Retail Allowed

Social Media Allowed

Sports Allowed

TV and Streaming Allowed

Youtube Allowed

Remote Connections
Apps that allow other devices to control your child's device (e.g. RemotePC, Teamviewer).

App Examples: TeamViewer, AirDroid, Chrome Remote Desktop, Microsoft Remote Desktop and more.

Website Examples: logmein.com, teamviewer.com, techinline.com, realvnc.com.

14. Canopy's installation procedure recommends as a default to install it so that it cannot be uninstalled by the user unless the parent approves it. The parent can override that configuration during the installation process if they wish or they can turn that configuration on or off at any time in the Canopy's web console.

15. In my opinion, the Canopy setup and installation on devices was simple, and within the skill level of any computer-using adult, and automatically performs many security configurations that would otherwise be confusing to the average computer user.

16. Finally, Mr. Allen states that "DNS filtering fails when 'DNS over HTTPS' is used to cloak a user's usage. This is easily adopted and has been standard for US users since 2019 if they use a Firefox/Mozilla Browser, so this control is easily circumvented." Allen Decl. at ¶74. It is not correct that this feature circumvents parental control software. The same

source that Mr. Allen refers to, https://support.mozilla.org/en-US/kb/firefox-dns-over-https (attached as Exhibit 1), which is consistent with my understanding, explains that Firefox is configured to work with parental control software, so that when Firefox detects such software, it disables the DNS-over-HTTPS feature.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 21st day of August 2023 in Houston, Texas.

/s/ Richard L. Sonnier III
RICHARD L SONNIER III

EXHIBIT 1

Firefox DNS-over-HTTPS

This article describes DNS over HTTPS and how to enable, edit settings, or disable this feature.

Table of Contents

About DNS-over-HTTPS

When you type a web address or domain name into your address bar (example: www.mozilla.org), your browser sends a request over the Internet to look up the IP address for that website. Traditionally, this request is sent to servers over a plain text connection. This connection is not encrypted, making it easy for third-parties to see what website you're about to access.

DNS-over-HTTPS (DoH) works differently. It sends the domain name you typed to a DoH-compatible DNS server using an encrypted HTTPS connection instead of a plain text one. This prevents third-parties from seeing what websites you are trying to access.

Benefits

DoH improves privacy by hiding domain name lookups from someone lurking on public Wi-Fi, your ISP, or anyone else on your local network, DOH, when enabled, ensures that your ISP cannot collect and self personal information related to your browsing behavior.

Risks

- Some individuals and organizations rely on DNS to block malware, enable parental controls, or filter your browser's access to websites. When enabled, DoH bypasses your local DNS resolver and defeats these special policies. When enabling DoH by default for users, Firefox allows users (via settings) and organizations (via enterprise policies and a canary domain lookup) to disable DoH when it interferes with a preferred policy.
- When DoH is enabled, Firefox by default directs DoH queries to DNS servers that are operated by a trusted partner, which has the ability to see users' queries. Mozilla has a strong Trusted Recursive Resolver (TRR) policy in place that forbids our partners from collecting personal identifying information. To mitigate this risk, our partners are contractually bound to adhere to this policy.
- DoH could be shower than traditional DNS queries, but in testing, we found that the impact is minimal and in many cases DoH is faster.

About our rollout of DNS over HTTPS

We completed our rollout of DoH by default to all United States Firefox desktop users in 2019 and to all Canadian Firefox desktop users in 2021. We began our rollout by default to Russia and Ukraine Firefox desktop users in March 2022. We are currently working toward rolling out DoH in more countries. As we do so, DoH is enabled for users in “fallback” mode.

For example, if the domain name lookups that are using DoH fail for some reason, Firefox will fall back and use the default DNS configured by the operating system (OS) instead of displaying an error.

Opt-out

If you're an existing Firefox user in a locale where we've rolled out DoH by default, you'll receive a notification in Firefox if and when DoH is first enabled, allowing you to choose not to use DoH and instead continue using your default OS DNS resolver.

In addition, Firefox will check for certain functions that might be affected if DoH is enabled including:

- Are parental controls enabled?
- Is the default DNS server filtering potentially malicious content?
- Is the device managed by an organization that might have a special DNS configuration?

If any of these tests determine that DoH might interfere with the function, DoH will not be enabled. These tests will run every time the device connects to a different network.

Enabling, disabling and configuring DNS-over-HTTPS

See the Configure DNS over HTTPS protection levels in Firefox article.

Configuring Networks to Disable DoH

- Configuring Networks to Disable DNS over HTTPS
- DNS-over-HTTPS (DoH) FAQs

Share this article: https://mzl.la/3pbH2so

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No.: 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC., *et al.*,

Plaintiffs,

vs.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,

Defendant.

DECLARATION OF PHILIPPE CRAVEIRO-ROMÃO IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Philippe Craveiro-Romão, declare as follows:

1. I provide this declaration in support of the Motion for Expedited Preliminary Injunction against enforcement of the Act of June 12, 2023, Ch. 676 (H.B. 1181) Tex. Sess. Law Serv. ("the Act"). I am over eighteen years of age, and I have personal knowledge of the matters set forth in this Declaration; if called as a witness I could and would testify competently to these matters.

MEDIAME SRL

2. I hold the position of Chief Operating Officer at MediaME SRL, a limited liability company organized under the laws of Romania, that operates the website Porndoe.com ("Porndoe").

3. Porndoe is a website that hosts adult content created by third party studios from around the world. Porndoe is available to the entire world of internet users, setting aside age or country censorship filters, and is available in almost all countries. The content on Porndoe is available to users free of charge. Porndoe makes money through advertising placements on its website and through referral fees generated from certain advertisements placed by third party content creators.

4. The content on Porndoe includes "soft core" content, including nude modeling with no penetration or masturbation.

5. I have reviewed the Declaration of Erik Cabrera, in particular his statement that Porndoe features "original" or "exclusive" content. Cabrera Decl. at ¶ 13. If Mr. Cabrera is interpreting these terms to mean that Porndoe produced or created the content, he is mistaken. These terms mean that the content is available only on Porndoe.

6. Porndoe strongly disagrees with the statements that the Act would require it to make on its website:

> TEXAS HEALTH AND HUMAN SERVICES WARNING: Pornography is potentially biologically addictive, is proven to harm human brain development, desensitizes brain reward circuits, increases conditioned responses, and weakens brain function. TEXAS HEALTH AND HUMAN SERVICES WARNING: Exposure to this content is associated with low self-esteem and body image, eating disorders, impaired brain development, and other emotional and mental illnesses. TEXAS HEALTH AND HUMAN SERVICES WARNING: Por-

> nography increases the demand for prostitution, child exploitation, and child pornography.

7. Porndoe also strongly disagrees with the Act's requirement to post the following message at the bottom of every webpage:

> U.S. SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION HELPLINE: 1-800-662-HELP (4357) THIS HELPLINE IS A FREE, CONFIDENTIAL INFORMATION SERVICE (IN ENGLISH OR SPANISH) OPEN 24 HOURS PER DAY, FOR INDIVIDUALS AND FAMILY MEMBERS FACING MENTAL HEALTH OR SUBSTANCE USE DISORDERS. THE SERVICE PROVIDES REFERRAL TO LOCAL TREATMENT FACILITIES, SUPPORT GROUPS, AND COMMUNITY-BASED ORGANIZATIONS.

8. Porndoe cooperates with parental filtering software by including a meta tag in its coding that designates its content as "RTA" (Restricted to Adults). By including this meta tag, parental control filters can easily identify Porndoe as an adult content site and block access.

9. The Terms and Conditions for Porndoe make clear that individuals under the age of eighteen are not authorized to access the website.

MIDUS HOLDINGS, LLC

10. I hold the position of Chief Operating Officer at Midus Holdings, LLC, a limited liability company organized under the laws of Florida, that operates the

websites Letsdoeit.com ("Letsdoeit") and Superbe.com ("Superbe") within the United States.

11. Letsdoeit is a website that hosts adult content created and owned by RentneR Limited, a content production company organized under the laws of Malta. The content on Letsdoeit includes "soft core" content, including nude modeling with no penetration or masturbation.

12. Superbe is a website that hosts adult content created and owned by RentneR Limited, a content production company organized under the laws of Malta. The content on Superbe is exclusively "soft core," primarily in the form of nude modeling.

13. Letsdoeit and Superbe strongly disagree with the statements that the Act would require them to make on their websites:

> TEXAS HEALTH AND HUMAN SERVICES WARNING: Pornography is potentially biologically addictive, is proven to harm human brain development, desensitizes brain reward circuits, increases conditioned responses, and weakens brain function. TEXAS HEALTH AND HUMAN SERVICES WARNING: Exposure to this content is associated with low self-esteem and body image, eating disorders, impaired brain development, and other emotional and mental illnesses. TEXAS HEALTH AND HUMAN SERVICES WARNING: Pornography increases the demand for prostitution, child exploitation, and child pornography.

14. Letsdoeit and Superbe also strongly disagree with the Act's requirement to post the following message at the bottom of every webpage:

> U.S. SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION HELPLINE: 1-800-662-HELP (4357) THIS HELPLINE IS A FREE, CONFIDENTIAL INFORMATION SERVICE (IN ENGLISH OR SPANISH) OPEN 24 HOURS PER DAY, FOR INDIVIDUALS AND FAMILY MEMBERS FACING MENTAL HEALTH OR SUBSTANCE USE DISORDERS. THE SERVICE PROVIDES REFERRAL TO LOCAL TREATMENT FACILITIES, SUPPORT GROUPS, AND COMMUNITY-BASED ORGANIZATIONS.

15. Letsdoeit and Superbe cooperate with parental filtering software by including a meta tag in their coding that designates their content as "RTA" (Restricted to Adults). By including this meta tag, parental control filters can easily identify Letsdoeit and Superbe as adult content sites and block access.

16. The Terms and Conditions for Letsdoeit and Superbe make clear that individuals under the age of eighteen are not authorized to access the websites.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on August 21, 2023 in Bucharest, Romania.

Dated: August 21, 2023

/s/ *Philippe Craveiro-Romão*
Philippe Craveiro-Romão

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC., et al.,

Plaintiffs,

v.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,

Defendant.

REBUTTAL DECLARATION OF ROBERT SEIFERT IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Robert Seifert, declare as follows:

1. I provide this declaration in support of the Motion for Expedited Preliminary Injunction against enforcement of the Act of June 12, 2023, Ch. 676 (H.B. 1181) Tex. Sess. Law Serv. ("the Act"). I am over eighteen years of age, and I have personal knowledge of the matters set forth in this Declaration; if called as a witness I could and would testify competently to these matters.

2. Xnxx and xvideos both have "soft core" adult content, including scenes and pictures involving clothed models or nudity with no penetration, model pages, and nude and partially clothed modeling galleries.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed on August 21, 2023 in Prague, Czech Republic.

Dated: August 21, 2023

/s/ *Robert Seifert*
Robert Seifert

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC., et al.,

Plaintiffs,

v.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,

Defendant.

REBUTTAL DECLARATION OF ANDREAS ALKIVIADES ANDREOU IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Andreas Alkiviades Andreou, declare as follows:

1. I provide this declaration in support of the Motion for Expedited Preliminary Injunction against enforcement of the Act of June 12, 2023, Ch. 676 (H.B. 1181) Tex. Sess. Law Serv. ("the Act"). I am over eighteen years of age, and I have personal knowledge of the matters set forth in this Declaration; if called as a witness I could and would testify competently to these matters.

2. I am informed that the Attorney General argues that the entirety of MG Premium Ltd's and MG Freesites Ltd's sites and services appeal wholly to the prurient interest, have no artistic value, and are patently offensive. Based on my professional knowledge, as well as my personal knowledge as a member of my

community, this is not correct. The sites contain a significant amount of material—including both videos and images—that are minimally sexually explicit, and no more so in kind and degree than sexually themed scenes and content in "mainstream" current film and television content. For example, Pornhub includes podcasts by creators in the community discussing their work and issues faced by the community, educational content regarding sexual health and wellness (through The Pornhub Sexual Wellness Center), erotic nude photos, and comedic, non-pornographic content playing on industry tropes. SpiceVids, FakeTaxi, and Brazzers also have "soft core" content, including model profiles that have clothed pictures and image galleries of nude modeling.

3. I am also informed that the Attorney General relies on a declaration from Gail Dines stating: "Although Pornhub claims that all the videos they upload feature consensual sex, there are tags that intentionally misspell the word consensual as "consesual," to avoid legal action. In July 2023, there were over 200,000 videos in the "Un Consesual" category, and 198,000 videos in the "Non Consesual Porn Porn videos category."

4. Pornhub does not have categories or tags for "Un Consesual" or "Non Consesual." The term "Consesual" is banned from the site. Rather, searching for two terms with a space between them will return results for both terms. The results Ms. Dines received were thus for the terms "Un" and "Non."

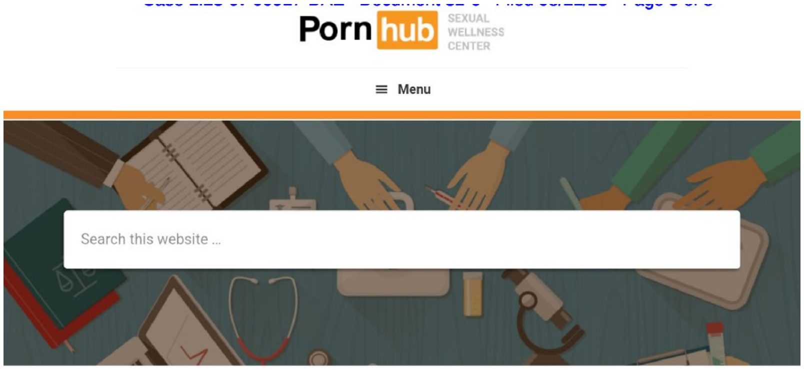
I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on August 21, 2023 in Nicosia, Cyprus.

Dated: August 21, 2023

/s/ *Andreas Alkiviades Andreou*
Andreas Alkiviades Andreou

EXHIBIT 1



What To Expect When Having Sex After a Hysterectomy

By Dr Stacy Friedman

Getting a hysterectomy is a very common medical procedure for people with uteruses. It can be done due to a number of reasons including heavy periods or fibroids, pelvic pain caused by something like endometriosis, prolapse or damage to the uterus, or cancer. A partial hysterectomy is when they just remove your uterus, and a full hysterectomy is a removal of your uterus and cervix. Removal of the ovaries is called an oophorectomy and may or may not be needed, depending on the reason you are having the surgery in the first place.

People who opt for a hysterectomy can be nervous as they may expect their sex drive to change or be gone but if the ovaries are properly functioning and they do not need to be removed, a partial or full hysterectomy should not affect the drive since your ovaries are the organs that supply the hormones. If anything, many people say that their drive may even be better since they had so many issues or pain prior, which is why they needed the hysterectomy in the first place and now post-surgery, those issues and pain are no longer present once healed. As you would imagine, having a major surgery of any kind can take a while to recover and impact your sex life along the way. Here’s how:

1. Recovery. Recovering from major surgery is always going to take time, patience, and rest. Give your body plenty of time to recover before pushing yourself to do or participate in anything strenuous—and that includes sex. It is generally recommended that you do not have sex until you are fully healed and are no longer experiencing discharge. Your doctor will give you instructions, but it is usually 6-8 weeks but can be up to 12 weeks depending on how you heal and the extent of your surgery. It is extremely important to listen to your doctor’s instructions even if you are feeling better before then because you don't want to risk tearing anything inside, especially if you had your cervix removed. If this is the case, you will have a vaginal cuff, which is where they sew the area closed

on the vagina once the cervix is removed, and that needs the time to heal.

2. Expect some dryness. Many people who have had hysterectomies (with or without their ovaries being removed, but especially when removed) experience new or worsened vaginal dryness. Remember that arousal is complicated and you may experience some non-concordance between your mind wanting sex and your body being ready for sex. Be sure to do plenty of foreplay and embrace using lube. Penetration without sufficient lubrication can lead to tears and pain that will not help the situation. Be prepared for dryness and know how to handle it.

3. Expect some changes in libido. At first, you may have a decrease in libido. This is completely normal. But don't worry—once you are fully recovered, most people bounce back just as (or more) horny than ever and even report having a better sex drive and sex life than before the operation. This is especially true for those who keep their ovaries.

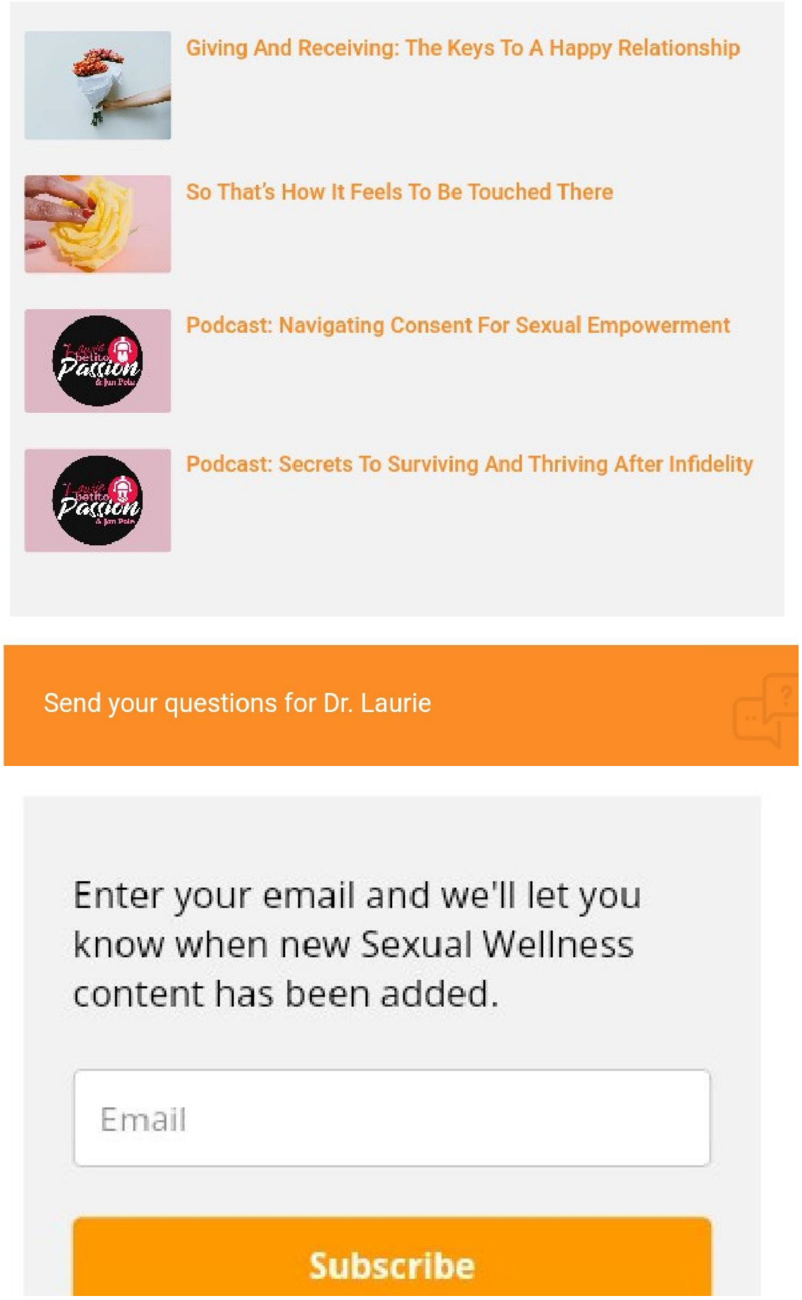
4. Pain is normal, but not forever. If someone cuts you open, you are going to feel pain. Take it easy, follow your doctor's post-op instructions, and listen to your body. Some pain is normal, but it shouldn't stick around too long after the operation and should never be excruciating. If that happens, call your doctor.

5. Don't skip out on the condoms. Just because you don't have a uterus anymore and can no longer have a child, does not mean you are immune to contracting STIs. Be sure to continue to practice safe sex including using protection, getting screened, and being honest with your sex partners.

6. Talk to your partner. Explain what you want, what you need, and what you are experiencing. If you know you are going to have dryness or need more foreplay or that certain positions are more uncomfortable for you, have that conversation ahead of time. If you decide to be intimate with someone without having that conversation first, then be prepared with some efficient ways to communicate your needs quickly in the moment.

Key Takeaway: Take it slow. When you are healed and ready to start having sex again, take it slow. Your body has just been through a major operation and you need time to re-learn how to have sex in ways that feel good and right. Take it slow, listen to your body, and enjoy the fun of figuring it all out. Even your ability to orgasm may be different so you may need to relearn your body in new and exciting ways.

If you or your partner are experiencing sexual concerns of any kind, it may help to talk to a professional. Dr. Stacy Friedman holds a Doctorate degree in Human Sexuality in addition to a Masters in Clinical Sexology and is a Certified Sex Coach. She offers complimentary 15-minute phone consultations and ongoing coaching sessions online or in her Boca Raton, FL office. Call 561-899-7669 or visit https://drstacyfriedman.com/ to schedule a consult today.



Giving And Receiving: The Keys To A Happy Relationship

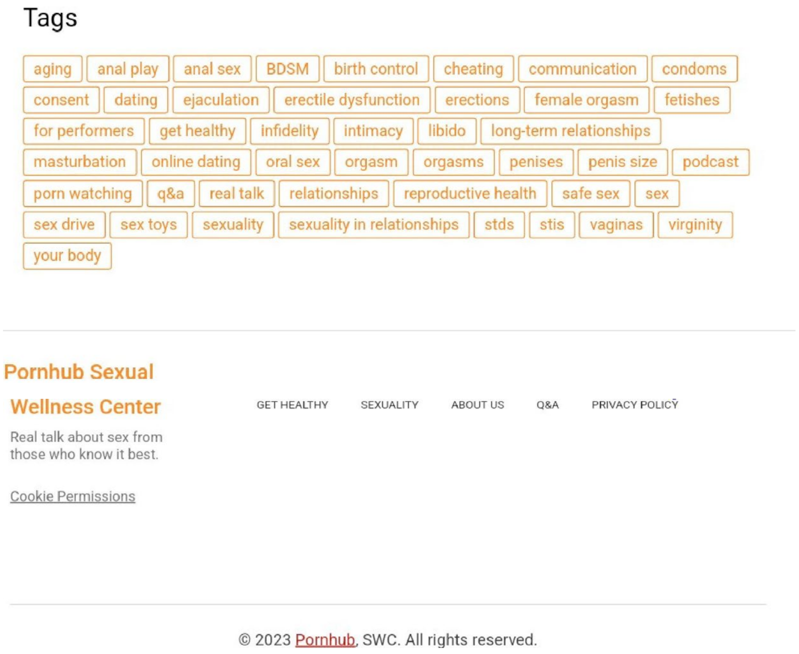
So That's How It Feels To Be Touched There

Podcast: Navigating Consent For Sexual Empowerment

Podcast: Secrets To Surviving And Thriving After Infidelity

Send your questions for Dr. Laurie

Enter your email and we'll let you know when new Sexual Wellness content has been added.



Tags

aging | anal play | anal sex | BDSM | birth control | cheating | communication | condoms | consent | dating | ejaculation | erectile dysfunction | erections | female orgasm | fetishes | for performers | get healthy | infidelity | intimacy | libido | long-term relationships | masturbation | online dating | oral sex | orgasm | orgasms | penises | penis size | podcast | porn watching | q&a | real talk | relationships | reproductive health | safe sex | sex | sex drive | sex toys | sexuality | sexuality in relationships | stds | stis | vaginas | virginity | your body

Pornhub Sexual Wellness Center

Real talk about sex from those who know it best.

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Case No. 1:23-cv-00917-DAE

FREE SPEECH COALITION, INC., et al.,

Plaintiffs,

v.

ANGELA COLMENERO, in her Official Capacity as Interim Attorney General for the State of Texas,

Defendant.

REBUTTAL DECLARATION OF SADIQ MUHAMED IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Sadiq Muhamed, declare as follows:

1. I provide this declaration in support of the Motion for Expedited Preliminary Injunction against enforcement of the Act of June 12, 2023, Ch. 676, § 2 (H.B. 1181) Tex. Sess. Law Serv. ("the Act"). I am over eighteen years of age, and I have personal knowledge of the matters set forth in this Declaration; if called as a witness I could and would testify competently to these matters.

2. I have reviewed Defendant's Opposition to Plaintiffs' Motion, as well as the Declaration of Erik Cabrera.

3. Mr. Cabrera claims that he visited MYLF.com and TeamSkeet.com, and that "[t]he landing pages of those websites likewise show pictures of videos that you can click on to view. However, you can only view short previews, and if you click on the videos, you are taken immediately to a screen that requests payment." Cabrera Decl. at ¶ 17.

4. Mr. Cabrera's description does not fully describe these sites' landing pages. The landing pages for both sites include both pictures and videos, which can be up to three minutes long. In addition, clicking on a video takes you to a preview of that video, under which the option is given to subscribe to the site for full access.

5. Separately, Defendant's Opposition suggests that all the content on MYLF.com and TeamSkeet.com wholly appeals to the prurient interest, lacks artistic value, and is patently offensive under contemporary community standards. Opp. at p. 6. I have not been able to identify evidence for this claim about MYLF.com or TeamSkeet.com in the Opposition or Mr. Cabrera's Declaration. Nevertheless, among the content offered on both sites is content that is minimally sexual, such as image galleries featuring models both fully clothed and in the nude, without penetration, masturbation, or the presence of another model.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on August 21, 2023 in Miami, Florida

Dated: August 21, 2023

/s/ *Sadiq Muhamed*
Sadiq Muhamed

<u>EXHIBIT 1</u>

BILL ANALYSIS

C.S.H.B. 1181
By: Shaheen
Judiciary & Civil Jurisprudence
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Sexual material on websites has become increasingly accessible to a young demographic of users. Exposure to this material can be associated with many negative emotional, psychological, and physical health outcomes for preadolescent users. According to an analysis published in the *Journal of Adolescent Health*, approximately one in five youth experience unwanted online exposure to sexually explicit material. Some studies, such as a 2015 study by Zachary D. Bloom and W. Bryce Hagedorn, have noted several potential negative impacts stemming from certain adolescents' use of sexually explicit material. C.S.H.B. 1181 seeks to hold individuals and entities who publish sexual material harmful to minors on a website accountable by setting out age verification requirements and creating liability for those who violate certain requirements.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 1181 amends the Civil Practice and Remedies Code to require a commercial entity, including a corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized business entity, that knowingly and intentionally publishes or distributes material on a website, including a social media platform, more than one-third of which is sexual material harmful to minors, to use reasonable age verification methods to verify that an individual attempting to access the material is 18 years of age or older. The bill makes liable a commercial entity that knowingly and intentionally publishes or distributes material on a website that is found to have violated the bill's age verification requirement to the parent or guardian of the minor for damages resulting from a minor's access to the material, including court costs and reasonable attorney's fees as ordered by the court.

C.S.H.B. 1181 requires a commercial entity that knowingly and intentionally publishes or distributes material on a website or a third party that performs age verification to require an individual to provide digital identification stored on a digital network that may be accessed by a commercial entity and serves as proof of the identity of an individual or to comply with a commercial age verification system that verifies age using a government-issued identification or a commercially reasonable method that relies on public or private transactional data to verify the age of an individual. The bill prohibits the commercial entity or a third party that performs the age verification from retaining any identifying information of the individual after access has been granted to the material. The bill makes liable a commercial entity that knowingly and intentionally publishes or distributed material on a website or a third party that performs the age verification that is found to have knowingly retained identifying information of an individual after access has been granted to the individual for damages resulting from retaining the identifying information, including court costs and reasonable attorney's fees as ordered by the court.

C.S.H.B. 1181 establishes the bill's provisions do not apply to a bona fide news or public interest broadcast, website video, report, or event and may not be construed to affect the rights of a news-gathering organization. The bill prohibits an Internet service provider, or its affiliates or subsidiaries, a search engine, or a cloud service provider from being held to have violated the bill's provisions solely for providing access or connection to or from a website or other information or content on the Internet or on a facility, system, or network not under that provider's control to the extent the provider or search engine is not responsible for the creation of the content that constitutes sexual material harmful to minors.

C.S.H.B. 1181 establishes that, for purposes of the bill's provisions, sexual material harmful to minors includes any material that:

- the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to or pander to the prurient interest;

- in a manner patently offensive with respect to minors, exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of:
    - a person's pubic hair, anus, or genitals or the nipple of the female breast;
    - touching, caressing, or fondling of nipples, breasts, buttocks, anuses, or genitals; or
    - sexual intercourse, masturbation, sodomy, bestiality, oral copulation, flagellation, excretory functions, exhibitions, or any other sexual act; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

The bill defines the following terms for purposes of the bill's provisions:

- "distribute" as issuing, selling, giving, providing, delivering, transferring, transmuting, circulating, or disseminating by any means;
- "minor" as an individual younger than 18 years of age;
- "publish" as communicating or making information available to another person or entity on a publicly available website; and
- "transactional data" as a sequence of information that documents an exchange, agreement, or transfer between an individual, commercial entity, or third party used for the purpose of satisfying a request or event and include records from mortgage, education, and employment entities.

The bill establishes that, for purposes of the bill's provisions, a news-gathering organization includes:

- an employee of a newspaper, news publication, or news source, printed or on an online or mobile platform, of current news and public interest, who is acting within the course and scope of that employment and can provide documentation of that employment with the newspaper, news publication, or news source; and
- an employee of a radio broadcast station, television broadcast station, cable television operator, or wire service who is acting within the course and scope of that employment and can provide documentation of that employment.

EFFECTIVE DATE

September 1, 2023.

COMPARISON OF INTRODUCED AND SUBSTITUTE

While C.S.H.B. 1181 may differ from the introduced in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute replaces the requirement from the introduced for an organization that owns a website, including an organization that owns a social media website, to include a mechanism that prevents a user from accessing pornographic material unless the user is 13 years of age or older with a requirement for a commercial entity that knowingly and intentionally publishes or distributes material on a website, including a social media platform, more than one-third of which is sexual material harmful to an individual younger than 18 years of age to use reasonable age verification methods to verify that an individual attempting to access the material is 18 years of age or older.

The substitute includes requirements for reasonable age verification methods, whereas the introduced did not include such requirements.

Whereas the requirement for preventing certain users from accessing pornographic material in the introduced applied to a corporation, limited or general partnership, limited liability company, business trust, real estate investment trust, joint venture, joint stock company, cooperative, association, bank, insurance company, credit union, savings and loan association, or other organization, regardless of whether the organization is for-profit, nonprofit, domestic, or foreign, the requirement for age verification in the substitute applies to a corporation, limited liability company, partnership, limited partnership, sole proprietorship, or other legally recognized business entity. Whereas the introduced included the term "pornographic material," defined as an image, video, or other means of visual display depicting actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sadomasochistic abuse, or lewd exhibition of the genitals, the anus, or any portion of the female breast below the top of the areola, the substitute omits this term. The substitute includes the term "sexual material harmful to minors," defined as any material that:

- the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to or pander to the prurient interest;

- in a manner patently offensive with respect to minors, exploits, is devoted to, or principally consists of descriptions of actual, simulated, or animated display or depiction of:
  - a person's pubic hair, anus, or genitals or the nipple of the female breast;
  - touching, caressing, or fondling of nipples, breasts, buttocks, anuses, or genitals; or
  - sexual intercourse, masturbation, sodomy, bestiality, oral copulation, flagellation, excretory functions, exhibitions, or any other sexual act; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

This term does not appear in the introduced.

Whereas the introduced established that an applicable organization may be held liable for damages if the organization does not include the mechanism to prevent certain users from accessing pornographic materials, the substitute makes liable an applicable commercial entity that knowingly and intentionally publishes or distributes material on a website and is found to have violated the age verification requirement to the parent or guardian of the minor for damages resulting from a minor's access to the material, including court costs and reasonable attorney's fees as ordered by the court.

Whereas the introduced included a provision that established that a person who uploads pornographic material to a website may be held liable for damages if an individual younger than 13 years of age accesses the material on the website, the substitute does not include this provision.

The substitute includes the following provisions absent in the introduced:

- a prohibition against a commercial entity or a third party that performs the age verification retaining any identifying information of an individual after access has been granted;
- a provision making liable a commercial entity that knowingly and intentionally publishes material on a website or a third party that performs the age verification that is found to have knowingly retained identifying information to the applicable individual for damages, including court costs and reasonable attorney's fees as ordered by the court;
- a provision establishing that the bill's provisions do not apply to a bona fide news or public interest broadcast, website video, report, or event and may not be construed to affect the rights of a news-gathering organization; and
- a provision prohibiting an Internet service provider, or its affiliates or subsidiaries, a search engine, or a cloud service provider from being held to have violated the bill's provisions under certain conditions.

The substitute includes definitions of the following terms, which were absent in the introduced:

- "commercial entity";
- "digital identification";
- "distribute";
- "minor";
- "news-gathering organization";

- “publish”; and
- “transactional data.”

The substitute omits the definition for “organization,” which appeared in the introduced.

EXHIBIT 2

BILL ANALYSIS

Senate Research Center

H.B. 1181
By: Shaheen et al. (Paxton)
State Affairs
5/13/2023
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Studies show the ease at which minors are able to access pornography is poorly controlled and allows exposure and exploitation of children online. Pornography is potentially biologically addictive, desensitizing brain reward circuits, increasing conditioned responses, and weakening brain function.

This legislation would ban minors under 18 years old from viewing explicit content online by requiring distributors and publishers of explicit content to require 18 years of age to view content. Commercial entities are held liable if they fail to perform age verification.

H.B. 1181 amends current law relating to restricting access to sexual material harmful to minors on an Internet website and provides a civil penalty.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Title 6, Civil Practice and Remedies Code, by adding Chapter 129B, as follows:

CHAPTER 129B. LIABILITY FOR ALLOWING MINORS TO ACCESS PORNOGRAPHIC MATERIAL

Sec. 129B.001. DEFINITIONS. Defines "commercial entity," "distribute," "minor," "news-gathering organization," "publish," "sexual material harmful to minors," and "transactional data."

Sec. 129B.002. PUBLICATION OF MATERIAL HARMFUL TO MINORS. (a) Requires a commercial entity that knowingly and intentionally publishes or distributes material on an Internet website, including a social media platform, more than one-third of which is sexual material harmful to minors, to use reasonable age verification methods as described by Section 129B.003 to verify that an individual attempting to access the material is 18 years of age or older.

(b) Prohibits a commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) from retaining any identifying information of the individual.

Sec. 129B.003. REASONABLE AGE VERIFICATION METHODS. (a) Defines "digital identification."

(b) Requires a commercial entity that knowingly and intentionally publishes or distributes material on an Internet website or a third party that performs age verification under this chapter to require an individual to:

(1) provide digital identification; or

(2) comply with a commercial age verification system that verifies age using:

(A) government-issued identification; or

(B) a commercially reasonable method that relies on public or private transactional data to verify the age of an individual.

Sec. 129B.004. APPLICABILITY OF CHAPTER. (a) Provides that this chapter does not apply to a bona fide news or public interest broadcast, website video, report, or event and is prohibited from being construed to affect the rights of a news-gathering organization.

(b) Prohibits an Internet service provider, or its affiliates or subsidiaries, a search engine, or a cloud service provider from being held to have violated this chapter solely for providing access or connection to or from a website or other information or content on the Internet or on a facility, system, or network not under that provider's control, including transmission, downloading, intermediate storage, access software, or other services to the extent the provider or search engine is not responsible for the creation of the content that constitutes sexual material harmful to minors.

Sec. 129B.005. CIVIL PENALTY; INJUNCTION. (a) Authorizes the attorney general, if the attorney general believes that an entity is knowingly violating or has knowingly violated this chapter and the action is in the public interest, to bring an action in a Travis County district court or the district court in the county in which the principal place of business of the entity is located in this state to enjoin the violation, recover a civil penalty described by Subsection (b), and obtain other relief the court considers appropriate.

(b) Authorizes a civil penalty imposed under this section to be in an amount equal to not more than the total, if applicable, of:

(1) $10,000 per day that the entity operates an Internet website in violation of the age verification requirements of this chapter;

(2) $10,000 per instance when the entity retains identifying information in violation of Section 129B.002(b); and

(3) if, because of the entity's violation of the age verification requirements of this chapter, one or more minors accesses sexual material harmful to minors, an additional amount of not more than $250,000.

(c) Requires that the amount of a civil penalty under this section be based on:

(1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of the violation;

(2) the history of previous violations;

(3) the amount necessary to deter a future violation;

(4) the economic effect of a penalty on the entity on whom the penalty will be imposed;

(5) the entity's knowledge that the act constituted a violation of this chapter; and

(6) any other matter that justice may require.

SECTION 2. Effective date: September 1, 2023.

EXHIBIT 3

BILL ANALYSIS

Senate Research Center
88R30050 JES-D

C.S.H.B. 1181
By: Shaheen et al. (Paxton)
State Affairs
5/15/2023
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

H.B. 1181 passed the House unanimously and, as substituted, includes:

- S.B. 2021. Passed the Senate 31-0
- S.B. 417. Passed the Senate 29-2. This was revised with stakeholder input.

Problem to Solve:

- Protecting children from harm is a primary duty of a parent. Yet in this day and age, the devices they use contain readily available hardcore pornographic content and videos and pictures that harm the minds of children.
- Texas law prohibits exposing a minor to pornography in Section 43.24 of the Texas Penal Code—Relating to the "sale, distribution, or display of harmful material to a minor."
- According to The National Center on Child Exploitation, pornography is proven to be biologically addictive and research shows that adolescents are more susceptible than adults to addictions and there are developmental effects on the brain.

- Exposure to explicit content in childhood is proven to increase the demand for child pornography, child exploitation, human trafficking, and prostitution.
- Children who use pornography are more prone to engage in risky sexual behaviors and are at risk of sexual victimization, which leads to mental health disorders.
- Self-generated imagery now accounts for 1/3 of web pages featuring child pornography. Sexualization through devices is creating more demand, access, and content creation from minors.
- Children's development is harmed when viewing content from mainstream pornography websites that show sexual violence, incest, physical aggression, sexual assault, non-consent, and teens.

Bill Summary:

- This legislation would ban minors under 18 from viewing explicit content online by requiring distributors and publishers of explicit content to require 18+ commercially reasonable age verification in order to view content.
- Publishers and distributors of explicit content are held liable if they fail to perform age verification. Users' data is not retained after verification.

The Committee Substitute:

- The committee substitute adds language from S.B. 417 "Electronic Device Filters" chapter to the Business and Commerce Code. It requires manufacturers to enable an optional filter on electronic devices activated in Texas that blocks minors from accessing explicit material.

- The filter can be bypassed by the parent/ guardian by entering a password or access code but must be reasonably secure.
- Manufacturers violating this chapter can be liable for a civil penalty of up to $10,000 per violation or $50 million total.
- Removes liability of nonparent violator.
- Adds the Miller v. California test to provide a good degree of specificity so that organizations may be put on adequate notice as to what is pornographic and what is not.
- Creates a more specific definition of filter including a good faith clause.
- Removes the private right of action.
- Makes the attorney general the enforcement mechanism.

C.S.H.B. 1181 amends current law relating to access to sexually explicit material on the Internet or electronic devices and provides civil penalties.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subtitle C, Title 5, Business and Commerce Code, by adding Chapter 121, as follows:

CHAPTER 121. ELECTRONIC DEVICE FILTERS

SUBCHAPTER A. ELECTRONIC DEVICE FILTER REQUIREMENTS

Sec. 121.001. DEFINITIONS. Defines "activate," "electronic device," "explicit material," "filter," "manufacturer," "minor," "simulated," and "visual material."

Sec. 121.002. APPLICABILITY. Provides that this chapter does not apply to a telecommunications provider who activates an electronic device on behalf of a user.

Sec. 121.003. ELECTRONIC DEVICE FILTER REQUIRED. (a) Requires a manufacturer to ensure that an electronic device activated in this state will, on activation, automatically enable a filter and notify the user of the device when the filter prevents the device from accessing, downloading, or displaying explicit material.

(b) Requires that an electronic device:

(1) allow the user of the device or a minor user's parent or guardian to circumvent the filter required under Subsection (a) by entering a password or access code; and

(2) reasonably prevent a user of the device from circumventing, modifying, removing, or uninstalling the filter without entering a password or access code.

Sec. 121.004. VIOLATION. (a) Provides that a manufacturer violates this chapter if the manufacturer releases into the market an electronic device that, when activated in this state, does not automatically enable a filter under Section

121.003 because the device lacks the necessary software or is defective.

(b) Provides that a manufacturer, notwithstanding Subsection (a), does not violate this chapter if the manufacturer makes a good faith effort to provide an electronic device that automatically enables a filter under Section 121.003.

SUBCHAPTER B. ENFORCEMENT

Sec. 121.051. CIVIL PENALTY; INJUNCTION. (a) Provides that a manufacturer who violates Section 121.004(a) is liable to this state for a civil penalty in the amount not to exceed the lesser of:

(1) $10,000 for each violation; or

(2) $50 million.

(b) Provides that a manufacturer who negligently violates Section 121.004(a) is liable to this state for a civil penalty in an amount not to exceed the lesser of:

(1) $1,000 for each violation; or

(2) $5 million.

(c) Authorizes the attorney general to bring an action in the name of the state to obtain an injunction preventing further violations of this chapter by a manufacturer or to recover a civil penalty under this section. Requires the prevailing party to recover reasonable and necessary attorney's fees and costs incurred in an action brought under this section.

(d) Authorizes the action to be brought in a district court in:

(1) Travis County; or

(2) the county located in which the defendant's principal place of business is located.

(e) Requires the attorney general to deposit a civil penalty collected under this section in the state treasury to the credit of the general revenue fund.

SECTION 2. Amends Title 6, Civil Practice and Remedies Code, by adding Chapter 129B, as follows:

CHAPTER 129B. LIABILITY FOR ALLOWING MINORS TO ACCESS PORNOGRAPHIC MATERIAL

Sec. 129B.001. DEFINITIONS. Defines "commercial entity," "distribute," "minor," "news-gathering organization," "publish," "sexual material harmful to minors," and "transactional data."

Sec. 129B.002. PUBLICATION OF MATERIAL HARMFUL TO MINORS. (a) Requires a commercial entity that knowingly and intentionally publishes or distributes material on an Internet website, including a social media platform, more than one-third of which is sexual material harmful to minors, to use reasonable age verification methods as described by Section 129B.003 to verify that an individual attempting to access the material is 18 years of age or older.

(b) Prohibits a commercial entity that performs the age verification required by Subsection (a) or a third party that performs the age verification required by Subsection (a) from retaining any identifying information of the individual.

Sec. 129B.003. REASONABLE AGE VERIFICATION METHODS. (a) Defines "digital identification."

(b) Requires a commercial entity that knowingly and intentionally publishes or distributes material on an Internet website or a third party that performs age verification under this chapter to require an individual to:

(1) provide digital identification; or

(2) comply with a commercial age verification system that verifies age using:

(A) government-issued identification; or

(B) a commercially reasonable method that relies on public or private transactional data to verify the age of an individual.

Sec. 129B.004. APPLICABILITY OF CHAPTER. (a) Provides that this chapter does not apply to a bona fide news or public interest broadcast, website video, report, or event and is prohibited from being construed to affect the rights of a news-gathering organization.

(b) Prohibits an Internet service provider, or its affiliates or subsidiaries, a search engine, or a cloud service provider from being held to have violated this chapter solely for providing access or connection to or from a website or other information or content on the Internet or on a facility, system, or network not under that provider's control, including transmission, downloading, intermediate storage, access software, or other services to the extent the provider or search engine is not responsible for the creation of the content that constitutes sexual material harmful to minors.

Sec. 129B.005. CIVIL PENALTY; INJUNCTION. (a) Authorizes the attorney general, if the attorney general believes that an entity is knowingly violating or has knowingly violated this chapter and the action is in the public interest, to bring an action in a Travis County district court or the district court in the county in which the principal place of business of the entity is located in this state to enjoin the violation, recover a civil penalty described by Subsection (b), and obtain other relief the court considers appropriate.

(b) Authorizes a civil penalty imposed under this section to be in an amount equal to not more than the total, if applicable, of

(1) $10,000 per day that the entity operates an Internet website in violation of the age verification requirements of this chapter;

(2) $10,000 per instance when the entity retains identifying information in violation of Section 129B.002(b); and

(3) if, because of the entity's violation of the age verification requirements of this chapter, one or more minors accesses sexual material harmful to minors, an additional amount of not more than $250,000.

(c) Requires that the amount of a civil penalty under this section be based on:

(1) the seriousness of the violation, including the nature, circumstances, extent, and gravity of the violation;

(2) the history of previous violations;

(3) the amount necessary to deter a future violation;

(4) the economic effect of a penalty on the entity on whom the penalty will be imposed;

(5) the entity's knowledge that the act constituted a violation of this chapter; and

(6) any other matter that justice may require

SECTION 3. Requires each manufacturer to implement a software update to automatically enable an electronic device filter on an electronic device activated in this state as required by Chapter 121, Business and Commerce Code, as added by this Act, not later than January 1, 2024.

SECTION 4. (a) Effective date, except as provided by Subsection (b): September 1, 2023.

(b) Effective date, Chapter 121, Business and Commerce Code, as added by this Act: January 1, 2024.

[1] UNITED STATES DISTRICT COURT WESTERN DISTRICT OF TEXAS AUSTIN DIVISION

Case Number 1:23-CV-00917-DAE

FREE SPEECH COALITION, INC.

Plaintiff,

vs.

ANGELA COLMENERO, in her official capacity as Interim Attorney General for the State of Texas,

Defendant.

Austin, Texas
August 23, 2020

TRANSCRIPT OF PRELIMINARY INJUNCTION HEARING BEFORE THE HONORABLE DAVID A. EZRA SENIOR UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFF:

Scott L. Cole
Michael T. Zeller
Derek Shaffer
Arian Joseph Koochesfahani
Taylor Comerford
Emily Couture
Quinn Emanuel Urquhart & Sullivan, LLP

FOR THE DEFENDANT:

John T. Ramsey
Kelsey L Warren
Office of the Attorney General of Texas

COURT REPORTER:

Angela M. Hailey, CSR, CRR, RPR, RMR
Official Court Reporter, U.S.D.C.
262 West Nueva Street
San Antonio, Texas 78207
Phone(210)244-5048;
angela hailey@txwd.uscourts.gov

Proceedings reported by stenotype, transcript produced by computer-aided transcription.

[2] INDEX

WITNESS :	PAGE
TONY ALLEN	
By Ms. Warren	6, 26
By Mr. Zeller	19

[3] *(Wednesday, August 23, 2023, 1:30 p.m.)*

* * *

COURT SECURITY OFFICER: All rise.

COURTROOM DEPUTY CLERK: Austin, 23-CV-917, Free Speech Coalition, Inc., et al versus Angela Colmenero, in her official capacity as Interim Attorney General for the State of Texas.

THE COURT: All right. Good afternoon. Can I have appearances please.

MR. COLE: Your Honor, Scott Cole with Quinn Emanuel for the plaintiffs, together with Michael

Zeller, Derek Shaffer, Arian Koochesfahani, Taylor Comerford, and Emily Couture.

THE COURT: All right.

MR. RAMSEY: Your Honor, I'm John Ramsey here on behalf of the State, or defendant Colmenero. I have with me Kelsey Warren.

THE COURT: Good afternoon, all of you. Now, I do understand that you have witnesses on standby, but to be honest with you, the Court has spent a considerable amount of time going through the materials that have been submitted. We have declarations and other materials submitted from both sides. Maybe I'm missing something, but I fail to see what witnesses who have already given declarations and are going to say the same thing on the stand that they've already said are going to [4] add today. So I really don't think it's necessary, unless there's something that you see that I don't see.

MR. SHAFFER: Your Honor, Derek Shaffer for the plaintiffs. We agree with that, Your Honor, and we're prepared if it comes up a particular factual issue to offer a witness that would be helpful to the Court, but we agree with Your Honor's assessment, that papers should suffice.

THE COURT: I mean, we know what the statute says, we know what the arguments are. I don't know where the dispute is.

MR. RAMSEY: We have with us an expert on age verification technology, and so to the extent that this Court is going to be trying to make a decision regarding whether or not the age verification law is effective and the least restrictive means for which the State is trying to pursue its compelling interest, we want to make this witness available, especially if there are any questions in the Court's mind about whether the law is effective in the least restrictive means to achieve the government's interest.

THE COURT: Didn't he present a declaration?

MR. RAMSEY: He did, he sent a declaration.

THE COURT: So is he going to say anything different than he said in his declaration?

MR. RAMSEY: I think he might have some information that would be responsive to the reply brief. At the same time, [5] Your Honor, I'm happy to go along with the plaintiff's counsel and proceed on argument. And if it seems to you that you still want more information about the exact technology involved and how effective it is, we could at that point call Mr. Allen to the stand.

THE COURT: Do you have any problem with him taking the stand and cross-examining him?

MR. SHAFFER: We don't, Your Honor.

THE COURT: All right. Let's call him to the stand if you wish to. Other than that, I don't see any need for any of the other witnesses. I think I appreciate and understand what this technology is, because you have the declaration, but go ahead and call him.

MR. RAMSEY: Do I understand, Your Honor, you would like to start the proceeding by calling Mr. Allen?

THE COURT: Right. I don't need an opening statement here. I've got a ton of briefing here. We don't have a jury.

MS. WARREN: Your Honor, with that, we would call Tony Allen to the stand. Your Honor, would you like me to use the podium at counsel table or the actual podium?

THE COURT: No, use the podium here.

MS. WARREN: Yes, Your Honor.

COURTROOM DEPUTY CLERK: Please raise your right hand.

* * *

(Oath administered, and TONY ALLEN, defense witness, [6] *Sworn.)*

* * *

THE WITNESS: I do.

MS. WARREN: May I proceed, Your Honor?

THE COURT: Yes.

(1:35 p.m.)

DIRECT EXAMINATION

BY MS. WARREN:

Q. Good afternoon, Mr. Allen. Can you please introduce yourself to the Court?

A. My name is Tony Allen, I am a global subject matter expert on age verification and age assurance.

Q. I apologize, if I can ask you to make sure you're speaking a little slower than normal just so we can all understand, it's a big room.

A. Okay.

Q. I want you to just go ahead and tell us a little bit about age verification technology, the three kinds of age verification technology that's available to sites such as the plaintiff websites?

A. Yes, so generally speaking, age verification technology is split into three distinct areas. One is related to what is known as age verification, so that is looking at gaming information about how old you are from official documents or sources such as your driving license or passport or other [7] documentation. Another one referred to as age estimation deals with looking at you and using computer technology to assess how old you are from your appearance or from your voice or from other biometric features. And the third one is age inference which is inferring how old you are from the existence of something else.

Q. So the first category is the document verification; is that right?

A. Mainly, yes, it can be against either documents or against things like digital wallets or apps or digital information.

Q. What kind of documents would age verification use to verify your age? You said driver's license, passport. Anything else?

A. Yeah, anything from authoritative source, so things like a firearms license or a ID card, an actual ID card or Social Security data or anything else really.

Q. And can you walk us through how that process would work? Say I wanted to gain access to one of the plaintiff websites, let's say Porn Hub, and say they had age verification technology in place. Can you walk us through what it would look like, the steps I would need to take to verify my age using the document system?

A. So the steps are the same across the areas, so they might be in a different order, but they're broadly the same steps, so generally speaking, you would have to present a document that you wish to rely on.

[8] Q. Let me stop you right there. I want to start on the web page, on the web page I'm trying to access. Tell me what I'm going to see.

A. Okay. So you would be – you'd try to access it, it would come up with a screen which would say we need to verify how old you are. Generally speaking, that would go off to another site, to a place where that happens, either a third-party site where you would carry out the process of verifying your age through that site.

Q. And then what would I have to do on that third-party verification site in order to verify my age?

A. So it will ask you to produce a document, so if you're using your driving license, for instance, you would present that document and you could do that to a camera on your Smart phone or on your screen, or in some cases it will allow you to upload a document from a trusted wallet or a digital mobile driving license or something like that, if you have that available to you.

Q. Can I ask you to bring that mic just a little bit closer to you please, or you closer to the mic? Thank you.

A. Is that better?

Q. That's better. Thank you. So once I have presented those documents, either taken a picture or used a digital wallet, then what happens in the age verification software?

A. So then it has to verify that you're the person presenting [9] it, so asking you to present your face, usually your face or image of yourself, and it will then verify the– in technical terms that's called one-to-one matching, but in normal parlance it's called selfie matching.

Q. Once that is finished, how long will it take for me to be Able to access the website that I am trying to access?

A. It's fairly instantaneous, so as soon as it carried out those two things, it will then send back a piece of code to the website. That code doesn't contain any information other than a transaction code and the answer to the question, *Is this person over 18? Yes or No*. That enables the website then to allow you to carry on to view the products and services that you want to view.

Q. What happens to the data that I have presented to the age verification website, like my passport or my driver's license and the actual selfie of my face, what happens to that data?

A. In most cases it's instantly deleted, they don't keep it, but there are sometimes legal requirements that they do have to keep it. So the way that the sites work is that unless there is a legal requirement that they have to keep it, they would delete it. If there is a legal requirement they have to delete it, which is indeed the case with this particular piece of legislation, they would instantly delete it, it's not kept. The only thing that's kept is the transaction ID. And if law enforcement came along and said the website have told us that [10] they've carried out age verification, they got this transaction, the age verification service provider would be able to tell them, yes, that's a genuine transaction ID, yes, that was carried out on a particular day, yes, they looked at a driving license, but they wouldn't be able to show them the driving license or the information or the selfie or anything else that they were presented with.

Q. You mentioned that some statutes require age verification technology to retain the information. Do you know if that's the case here in Texas with HB 1181?

A. In HB 1181, it specifically says you can't retain it. I'm not sure about your gambling legislation because it's normally gambling legislation which requires the retention of the data, and I haven't looked at the gambling legislation here in Texas, but it wouldn't be uncommon for gambling legislation to require the retention. But in the case of HB 1181, it specifically prohibits from retaining the information.

Q. And that would be any kind of age verification, any of the three types that you described?

A. Yes.

Q. Let's talk about the second kind of age verification, I think that was age estimation; is that correct?

A. That's correct, yes.

Q. Can you just give us a brief overview of how that works?

A. So similar to age verification, you go onto a website, it [11] will direct you to somewhere to verify your age, you select the option to use age estimation, and you would present either your face or you would say a short sentence, if it's doing voice or there's other technologies out there as well. And it's very similar to how you open your cell phone, so if you use face ID on your phone just as an example.

Q. Would age estimation software would actually take a photograph of your face?

A. No, it doesn't take a photograph of your face. What it does is it takes data points. It doesn't take enough data points to be able to recreate your face in an image, but it uses those data points and the algorithms that train it to be able to make an estimation of how old you are from those points.

Q. So it's kind of like whenever I take a – whenever I try to open my phone with my glasses on versus my glasses off, it's not actually looking at a picture of my face, it's looking at certain points of data on my face?

A. Yeah, I can get very technical, there are 126 of them that it uses as part of the international standards on how it does these, how it does these things, but it doesn't have enough there to be able to – if someone says show me the dots, it wouldn't be enough to show me a picture of you.

Q. But even those dots, those cannot be retained under the Texas law?

[12] A. That's correct.

Q. And then what was the third kind of age verification that you mentioned?

A. Age inference, that is being able to infer that you're over 18 from the existence of some other fact. So as example you might be a commercial airline pilot which would require you to be over 18 to hold that role or you might have a .gov e-mail address. There are all kinds of reasons why you might be able to infer that someone is over 18.

Q. So I might be able to verify my age using my .gov e-mail address?

A. You could, yes, so that would work by the age verification service provider effectively pinging you a message and then giving you a code and you enter that code. It's normally six digits, doesn't have to be, but it's normally a six-digit code that you enter in and that would verify that you have access to that e-mail address, and from that they can infer that you're over 18.

Q. And I certainly wouldn't want my employer to know that I was accessing pornography, so is that something that anybody would ever be able to figure out if I supplied my government e-mail address?

A. So, first of all, the age verification providers, they are not – they don't give a reason why they're asking, so they could be asking for any reason. It could be access to [13] pornography, it could be to buy liquor, could be to buy cigarettes, it could be any reason at all that requires that age verification. The second thing I would say about that is generally speaking your e-mail address is not kept, unless you want to go on to create an account, but that's the next stage of the process. If you go back to the porn site and you want to create an account with them to be able to access in the future, you may choose to use that e-mail address or you may choose to use a different e-mail address at that point. You don't necessarily have to use the same one to create your account and do your age verification.

Q. I want to switch gears a little bit and talk about something that Dr. Sonnier brought up in his declaration that accompanied the reply brief in this case. He was discussing essentially parental controls. What is the technical term?

A. Parental controls or filtering software.

Q. Filtering software.

A. Device-based software, various other things.

Q. Can you explain to us what filtering software is?

A. Yes, it's basically tools that can be used in most or pretty much all the browsers or routers which are in your home have these tools where you can set within that filters. Now, these filters are widely available. They are used extensively, so here in this building, for instance, you will have a filter that will prevent people on the PCs that we have here from [14] accessing certain sites, so they are set up to be able to do that.

Q. And how effective are those in the home as opposed to in a business?

A. One of the key differences – I mean, here in a federal building you've got the filtering software working, but you also have an IT team here all the time checking that that's working and working properly, set up properly, operating properly, got all the correct fills, it's got all the correct updates. That's their job and that's what they do, that's how they keep you protected in this building. At home you don't have that, so you do rely to a certain extent on, first of all, parents knowing they're available and then understanding how to implement them and how to put them into place. And then even thereafter, how to keep them updated, how to deal with the fact that children get older and so, therefore, what they might want to experience changes over a period of time. So the studies and research there has been on filtering that they work, as a tool they work, but they rely on parental knowledge and information and education, and they rely on them keeping them up to date. And it's those two latter things that generally are lacking.

Q. So what if a parent downloaded some kind of filtering software or got it from their carrier and just decided to set one of the predetermined levels of security, say medium [15] security, what would they have to do to maintain that security on the devices connected to their network?

A. So it depends on the settings that they set, it also depends on the filters, different ones do different things, but generally speaking you're right, they do present you with an option to have – effectively have a recommended filter or a user filter, you can usually set those at low, medium, high. You can then also create alongside those they're sometimes called white lists or black lists depending on the filtering software. But you can create ones that you want to give special permission to or ones that you want to deliberately prevent from accessing. So it depends on the software and the filter and how you want to set it up.

Q. Are you aware of research as to the effectiveness of these filtering softwares and their ability to prevent children from accessing sites that they shouldn't be accessing such as pornographic websites?

A. Yeah, I mean, the research I've seen generally comes to the conclusion that while that filtering software is capable of working, it isn't being deployed in the home in a way that makes it effective.

Q. We don't all have IT Departments at home?

A. Yeah.

Q. And I want to briefly touch on –

THE COURT: Just a minute. Do you need an IT [16] Department to deploy a filtering software in your home?

THE WITNESS: You don't need an IT Department, you just need –

THE COURT: You just need software.

THE WITNESS: You need the software and you need some knowledge about what you're setting up.

THE COURT: You don't need an IT Department.

THE WITNESS: No.

THE COURT: These things are meant to be deployed by individuals, isn't that true?

THE WITNESS: They can be deployed by individuals, yes.

THE COURT: Okay. I just want to be sure that I wasn't missing something here.

THE WITNESS: Fine.

BY MS. WARREN:

Q. Let's explore that just a little bit more. So if I was to set parental controls on devices in my house and then I never touched them again, what could happen?

A. Generally they will work, they will do what you set them to do. As you go through usage of the Internet, what will happen is that when your children either use the permission function or they ask to change something or ask to access something, that then gets set within those controls and that becomes continuous. And depending on how good they are would depend on [17] how much they're updated for either new sites or new access means or new browsers or new functionality. That depends on how good the filtering software is and whether it's being done at a device level on your phone or at a router level, i.e., where you connect to WiFi, where it's being deployed, so there's lots of dependencies there.

Q. If I was to set up the software at a router level and then the router needed a hard reset, would that then reset the controls?

A. With a hard reset it would take you right back to the factory settings, so you would have to go through the process again. If you just switch it on and off again, it doesn't have that impact, it normally will retain the settings if you're just powering it down and powering it up again.

Q. I want to talk about VPNs just briefly. What is a VPN?

A. So a VPN is a virtual private network, it effectively is a method by which you can hide where you are in your – from your Internet address, and enable you to browse a web from an anonymous location.

Q. How do age verification websites grapple with the, I guess, threat of a VPN circumventing their system?

A. Yeah, there are various different ways. Some of them will look at geo location software that supports the age verification function, some of them will have things that try to detect whether or not it is from a known VPN, IP address. [18] I'm being technical, an IP address, the Internet protocol address. Some of them will look for dynamic VPNs. There are various different ways in which they use to detect that. There are also people that connect not so much via VPN, but via things like cell tower networks so they can use geo location software in relation to that as well.

MS. WARREN: Your Honor, we have nothing further at this time.

THE COURT: I have a question about VPN because there's been a lot of talk about that. I know that, for instance the – you're from England originally?

THE WITNESS: Yes.

THE COURT: You're familiar with the BBC?

THE WITNESS: Yes.

THE COURT: And you're not supposed to be able to get the BBC iPlayer unless you are in the UK, but VPNs have been very successful in circumventing the BBC, wouldn't you agree?

THE WITNESS: Yeah, they're used for that for Netflix.

THE COURT: Netflix as well. There's a different Netflix in the UK than there is in the United States and they've got very sophisticated software that's trying to stop that, but they've been very unsuccessful; isn't that correct?

THE WITNESS: Yes, that's correct.

THE COURT: Any cross-examination?

MR. ZELLER: Just very briefly. Mike Zeller for [19] plaintiffs.

(1:52 p.m.)

CROSS-EXAMINATION

BY MR. ZELLER:

Q. Just to start off, is there anything that you said here in your testimony today that you think was not in your declaration, so we can focus on that?

A. I think the bit more detail around the issues to do with parental controls and filtering software, I think I covered it very briefly in my declaration.

Q. You don't think you adequately addressed that in your declaration?

A. I covered it briefly, but I think I've covered it in more depth in the questions.

Q. You understand that the law that's at issue here today doesn't require any particular kind of age verification of the various methods that you've mentioned, right?

A. No, I think it's open about your choice, whichever you want to do.

Q. And you acknowledge that at least some of those methods require the disclosure of personal information, passports, driver's license, other kinds of highly personal information for at least some of these age verification methods to even function at all, right?

A. Yes, some of them do.

[20] Q. Does content filtering require that the users impart to third parties their personal information of that kind?

A. Depending on the type of one it is, then generally no. Some of them do, some of them don't.

Q. The law that's at issue here today doesn't require that any of the third-party age verification technologies that you mentioned actually meet the standards of what you refer to as this Age Verification Providers Association, right?

A. No, I think the law is just generally you have to apply age verification, I think it uses the term commercially reasonable sources or something like that.

Q. Right, but they don't have to meet any particular standard such as an industry standard, right?

A. Not by the law, no.

Q. And the law doesn't actually prohibit the, say, the sharing of this personal information with third parties during the validation process, right?

A. Just let me just unpick that slightly. The process would be that the – what we call the relying party, the website that wants to allow the user access would refer the user to a third party to collect that information and process it, they wouldn't collect it themselves, they then send it on to the third party.

Q. The law only says that it cannot be stored, right? It doesn't say it can't be transmitted elsewhere, correct?

A. It says it can't be kept, yes.

[21] Q. Now, you mentioned parental controls, but that's only one kind of content filtering, correct?

A. Yes.

Q. And you're aware that content filtering is widely adopted here in the United States by corporate America in order to stop employees from, and blocking employees from seeing adult websites or other kinds of sites that the employer doesn't want to see, right?

A. Yes, that's what I was describing–

Q. In fact, many, many tens of billions of dollars are spent on that every year by corporate America with this technology, right?

A. I'm quite sure that's true, yes.

Q. And you do understand that at least by that measure, content filtering is far more successful than these age verification methods that you've mentioned, correct?

A. I think that's an entirely different context. I think they are successful at content filtering and removing these from access in the workplace, and the evidence doesn't suggest that's quite the same in the home.

Q. You'll acknowledge that content filtering is far more ubiquitous as a method to block access to adult websites in the United States today than age verification?

A. Yes.

Q. You understand that the – I think you've already addressed [22] that there are certain kinds of technologies that the law does not address at all here, such as VPN technology, right?

A. There's nothing specific in this legislation about VPNs.

Q. And you also understand the law has exceptions in the sense that it doesn't apply to social media sites, correct?

A. I believe that's correct, although I'm not a legal expert on the interpretation of that law.

Q. And you understand that adult images and pornographic materials and that sort of thing are widely available on social media sites, correct?

A. Yes, correct.

Q. You also understand the same is true for search engines?

A. Yes.

Q. You referred I think briefly in your testimony to some research that you were relying on? What are you referring to specifically?

A. In relation to content filtering?

Q. Yes.

A. Yeah, there's been lots of research done on this. I think the one I particularly highlighted was research done from the Oxford Internet Institute in relation to the effectiveness of parental content filtering and on the access that I think that particular survey was about adolescent boys having access to pornography.

Q. Are you referring to this Nash study?

[23] A. Yes.

Q. And that's referred in your declaration, correct?

A. Yes.

Q. So you're not relying on anything else in your testimony here today other than what you've already cited in your declaration, correct?

A. That was just an example of research in this base, there has been other research in this base too.

Q. The Nash study doesn't say anything actually about the effectiveness of the technology itself, does it?

A. No, as I said, the technology itself works.

Q. You mentioned this concept of white listing, right? And that's one way that certain kinds of software, say, parental controls, can ensure that even new websites that have, say, for example, malicious content on them are, in fact, blocked by that software, right?

A. The other way around. White listing is where you permit access to something. Black listing is where it's blocking it.

Q. Maybe I poorly phrased it. What I'm driving at is is you understand that by using white listing software, that that will block access to new websites because it's not listed on the white list, right?

A. Not necessarily. It depends on the settings in the individual filter control. Generally speaking, white listing is where you specifically go in and say I do want to give [24] permission to be able to access this site.

Q. You're aware that most of what you're calling this parental control software blocks access to new websites, correct?

A. Some of it does. Some of it uses labeling, called the RTA label which is restricted to adults label, some of it uses that. If the website contains that particular RTA coding, that it would pick that up as part of its filtering function.

Q. And you'll agree with me that content filtering software in many iterations actually has a dynamic realtime process where it scans the website, even if it's a new one and has never been encountered by the software previously to block it if it falls in the category of, say, adult website, correct?

A. If they are labeled with the things like the RTA label, then it will spot those and it will add them to its list of restricted sites.

Q. When you say "label", what do you mean by that?

A. So there's a function on the website which is fairly widely used in the adult industry, not universally used, but it's fairly widely used, which is called

Restricted To Adults, the RTA, it's run by a U.S. NGO and it is used by things like filtering software to be able to pick up sites, as the name says, restricted to adults.

Q. You're aware that this content filtering will actually block adult websites even if it had not encountered that website before specifically because, say, for example, it was [25] new?

A. It would need to know that it was not a website, it would need to do that and so some of them do have artificial intelligence tools as part of them that look at sites to see what kind of content do they have. Some of them rely on the company behind the software maintaining continuous surveillance of the Internet, and some of them rely on things like, as I said, the RTA label, some of them rely on data put out by law enforcement agencies of websites of concern and they will rely on different things.

THE COURT: Let me ask you a question before we go any further. This legislation doesn't require any adult websites that are seeking to have customers in Texas, doesn't require them to have an RTA function; is that right?

THE WITNESS: No.

THE COURT: I didn't see any legislation that requires an RTA. But if the Texas legislature were to pass a different law that required an RTA label or chip or whatever it is, code, in the website and then gave parents the choice of placing blocking software, filtering software on their computers, anything accessing anything that could be accessed by their children, the RTA code would then work with that software to block the software; is that right?

THE WITNESS: It should, yes.

THE COURT: Okay.

[26] MR. ZELLER: I have nothing further, Your Honor.

Thank you.

THE COURT: Any redirect?

MS. WARREN: Very briefly, Your Honor.

THE COURT: Okay.

(2:02 p.m.)

REDIRECT EXAMINATION

BY MS. WARREN:

Q. Mr. Allen, how difficult would it be for websites like PornHub and XNXX to use this age verification technology, is it completely new to them?

A. It's not new to them, they use it elsewhere in the world. They already have age verification technology built into their systems. There are a number of global providers of age verification technology, one of them actually based right here in the City of Austin, one of the main ones in the world, and they have this functionality already.

MS. WARREN: Thank you. Nothing further, Your Honor.

MR. ZELLER: Nothing further, Your Honor.

THE COURT: Sir, thank you very much. You can step down.

THE WITNESS: Thank you, Your Honor.

THE COURT: Do we have any other witnesses? Do you want to call somebody, some expert you want to call?

MR. SHAFFER: Thank you, Your Honor, not from the [27] plaintiffs.

THE COURT: Since the plaintiffs are the ones that are seeking this injunction, you can go first.

MR. SHAFFER: Thank you, Your Honor. Derek Shaffer for the plaintiffs. Your Honor, we're here challenging what is an entirely new an unprecedented statutory regime in Texas before it takes effect. HR 1181 imposes hundreds of thousands of dollars in liability on anyone who provides the disfavored content over the Internet without complying with Texas's newly minted burdens and strictures of age verification. This is not the first time something like this has been attempted, Your Honor. As you know, this is the latest in a string of similar efforts by other jurisdictions including the United States government to shut down or straightjacket disfavored speech on the Internet. All of those efforts have been couched as protecting minors and all of them have been uniformly rejected by courts from the U.S. Supreme Court on down the line as violating the First Amendment. All we're respectfully asking today is that this Court grant a preliminary injunction so as to preserve the status quo while the Court adjudicates the First Amendment and other merits. As I'll explain, and I think the merits of our First Amendment challenge are strong and this is a case for granting a preliminary injunction. I know Your Honor's read the papers, so my most important job of course is to answer Your Honor's questions, but do I want –

* * *