Consultation response form

Please complete this form in full and return to Part5Guidance@ofcom.org.uk.

Consultation title	Guidance for service providers publishing pornographic content

Your response

Question	Your response
Question 1: Do you agree with our proposed guidance on scope? If not, please provide any information or evidence in support of your views, including descriptions of services or content where you consider it is unclear whether they fall within the scope of Part 5.	Confidential? – ~~Y~~ / N
Question 2: Do you have any comments on how our proposed guidance applies in respect of pornographic content created by generative-AI services within the scope of Part 5? Please provide any information or evidence in support of your views.	Confidential? – ~~Y~~ / N
Question 3: Do you have any comments on our proposed guidance in respect of the kinds of age assurance which could be highly effective? If you consider there are other kinds of age assurance which have not been listed that you consider could fulfil	Confidential? – ~~Y~~ / N There is currently little evidence that an at-scale deployment of age verification/assurance which does not include the banking system can be successful. This covers the vast amount of content online and much of what

Question	Your response
the proposed criteria, please identify these with any supporting information or evidence.	could considered sexual or pornographic. It is nearly impossible to benchmark what could be considered highly effective. At the same aiming for an unquantifiable measure introduces significant privacy risks, threats to freedom of expression, places many adult users at risk of blackmail and even creates personal safety threats as identities and locations could be revealed. While there have been some claims that age verification by websites could be conducted in a fully secure manner, the reality is that cases of identity theft, fraud, and the many examples of data leaks and servers being compromised, show online data remains vulnerable. It is also at risk from hackers who are already inside a system. IBM's estimates place the average time it takes a company to detect a breach at around two hundred days. This provides ample time for hackers to set up a 'man in the middle' attack to capture people's data as it is provided. In Australia, the federal government has announced it will not force adult websites to use age verification due to concerns about privacy and the 'lack of maturity' of the technology. With their government stating on record that 'at present, each type of age verification or age assurance technology comes with its own privacy, security, effectiveness or implementation issues.' As the British Computer Society (BCS) argued, regulation should "not put its trust in emerging technology solutions to deliver child protection without rigorous analysis of their flaws, evaluation of the privacy trade-off, and a balancing emphasis on education and awareness." Campaign groups such as the Electronic Frontier Foundation have also argued that the ubiquity of data storage could lead to bad actors selling private information "to data brokers, seized by police or immigration officials, stolen by data thieves, or misused by employees". (See

Question	Your response
	https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10). I note that in the US state of South Dakota, four state senators recently opposed age verification legislation. State Senator Michael Rohl (who represents the conservative Republican Party) said that "We heard testimony from the age verification company, that they would be able to sell the information collected to 3rd party companies," he added, arguing that people who use their ID to verify their age and watch pornography could have their data sold." Quite clearly, without legislation to the contrary, there would be nothing to prevent any company established to provide age verification services from selling the data that they have been provided with. I note that any warnings or purported agreement clauses are ordinarily in small print and are usually clicked through, rather than read carefully. Implementation of the legislation risks causing more harms than they solve. It is also worth citing Senator Rohl (*ibid*) further. He said that the bill "doesn't stop the problems of VPNs, has significant issues enforcing, requires no parental steps to try to stop it, doesn't hold parents liable for negligent behaviour (like we do with alcohol), would include social media sites like Twitter, and doesn't ensure the privacy of South Dakota residents." Significantly, Senator Rohl appears to be in favour of parents taking responsibility for their child's Internet usage, including protection online. (https://www.washingtonexaminer.com/opinion/2898673/south-dakota-senators-put-the-pornography-industry-first/). A recent news item reported an upsurge in identity theft arising from the requirement in some age-verification systems to upload government-issued identity documents. Regrettably, I didn't note the URL and, despite searching, have not been able to find the news item

Question	Your response
	again. However, one of the things which the report mentioned was opening bank accounts in somebody else's name by using documents stolen from websites. Examination of the HSBC Group website (https://www.hsbc.co.uk/help/banking-made-easy/help-us-identify-you/) discloses that if an account applicant uploads a copy of their driving licence, that's sufficient to prove the applicant's identity and their address, i.e., no further documents are required. Ofcom may be aware of another scam in which fraudsters make a redirection request to the Post Office and forward all post for the named person to another address and would, therefore, be able to intercept any account opening documents sent to the postal address. I am not familiar with the Driver and Vehicle Licencing Agency's security protocols when a change of address request is made but suggest that it is possible that, armed with a driver's details from their licence, it would be possible for a fraudster to obtain a genuine licence, in the victim's name, but at whatever address the fraudster required and all without the licence holder being aware. A further twist on that scheme is that now armed with genuine government-issued ID, it would not be impossible for the fraudster to take over the victim's accounts. I suggest that the routine uploading of government-issued documents is highly undesirable. Beyond the threat of bad actors, age verification methods could create data on browsing habits and internet use likely to be appealing to niche advertisers. There is currently no acceptable or sufficient privacy code governing the use of this data by age verification providers, and no provision for this in the Act. Considering these threats, I urge Ofcom to focus on systems where no new data is created – for example, content filtering at the device or ISP-level (similar to the mobile network operator) option in the guidance should be recommended. Should other forms of age verification technology be recommended, I urge Ofcom to follow a similar approach to the government's announcement on

Question	Your response
	end-to-end encryption, that technology should only be implemented when ready and proven.
Question 4: Do you agree that service providers should use the proposed criteria to determine whether the age assurance they implement which is highly effective at correctly determining whether or not a user is a child? Please provide any information or evidence in support of your views.	Confidential? – ~~Y~~ / N While the age assurance technologies proposed in the draft guidance could be implemented and several may effectively verify the ages of users, I are not confident that the Act will be as effective as assumed in Parliament therefore failing in its stated aims to improve online safety. The issue of children accessing potentially harmful material online requires a societal response. There is no technological solution that will tackle the root causes of the issue of children's safety online. Children are tech savvy and may be able to circumvent controls by borrowing parent's or elder sibling's ID. This will not leave a footprint whereas the use of bank documents may do so. (Additionally, bank documents are likely to be more closely controlled by the holder, whereas passports, etc., may left in a drawer and not examined until holiday time comes.) Any attempt by a regulator will be unlikely to succeed without an accompanying focus on education, a call also made by the British Computer Society. This means a proper digital literacy programme (which Ofcom can champion), guidance on relationships and sex education as it relates to online content and in the context of championing communication, consent and respect (which Ofcom can curate) and greater support to caregivers (which Ofcom can encourage).
Question 5: Do you have any information or evidence on the extent of circumvention risk affecting different age assurance methods and/or on any steps that providers might	Confidential? – ~~Y~~ / N Already, there are multiple ways for individuals to use technology to freely explore the internet in a privacy-preserving manner, including through the use of virtual private networks (VPNs) and other security technologies. Accessing and using such technology is relatively easy –

Question	Your response
take to manage different circumvention risks for different methods?	especially for technologically literate young people. Age verification will simply create an 'age-gate' to accessing adult content. All it will take for content to be downloaded, accessed and shared by under-18s is for them to use easily available technologies like VPNs (which make it appear that a user is accessing a website from another country) or simply to visit access the Dark Web through the TOR browser. In the latter, there is the risk that young people encounter more dangerous material and could even be exposed to criminal content and interactions. 'Dark Web' is the name given to that part of the deep web used for criminal purposes, including the hosting of hate material and harmful imagery. The deep web, in contrast, is that part of the web which is unindexed and cannot be searched other than by a specialist search engine. With the prevalence of these technologies, it is likely the effectiveness of age verification systems at the website level, will be limited. At the same time, enforcing such solutions risks creating even greater harm to young and otherwise vulnerable people. It is important to note that VPNs and other IP masking technologies are also a social good in many cases and for some content creators a vital safety tool. Efforts that stop people from being able to find and access them could lead to content creators having their locations revealed and their physical safety threatened. Uploading government-issued documents to demonstrate a person's age cannot be described as reliable. I cite these three matters in support. 1. In the early-1980s, a young woman who used the stage name of Traci Lords rose to prominence in the US pornography industry. She had produced a genuine US government-issued ID document which was accepted. The precise history of the document is not clear. However, famously, it wasn't Traci Lord's document and it misrepresented her age. She was, in fact, under 18.

Question	Your response
	2. Some years ago, I conducted a number of photo shoots with a very well known, now retired, photographic model who had a large spider tattoo on her buttock. During one of the shoots she mentioned that she was going to have something done about the tattoo which no longer suited the image that she sought to project. She also told me that the tattoo was done when she was fifteen and added that she'd used her sister's identity document to fool the tattoo artist. It is clear that, even when the document is present with the person offering it, it does not reliably demonstrate the age of the person holding it. Ofcom will be aware that photographs on identity documents rarely look like the holder and that's before a change in hairstyle or simply aging—passport photos can be ten years old—is taken into account. 3. In the recent past, payment processors Visa and Mastercard have tightened their requirements for sites selling pornography. These requirements relate to the identification of performers and the supply of copy information required by US federal law to the client site. (The relevant US law is at Title 18, US Code, at parts 2257 and 2257A; and Title 28 of the Code of Federal Regulations at part 75.) Anecdotally, this change arises from a UK-based site, which required uploaders to identify themselves with a copy of government-issued identity documents, being fooled by a 17-year-old who had used her grandmother's passport for the purpose of opening an account in order to sell imagery of herself. As in the previous example, the possession of a passport or other identity document doesn't prove that the person offering it is the holder or of age. The Verge, a US-website, citing CNIL (the French National Committee on Informatics and Liberty) wrote, in respect of various online age verification schemes, that "all these methods have serious flaws." (https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.) The Verge also writes that face-based age detection systems may not be accurate. It cites Yoti, the service used by FaceBook and Instagram, as claiming that with regard

Question	Your response
	to children between 13 and 17 as 'under 25 with 99.93 per cent accuracy'. The Verge continues that '[t]his study doesn't include any data on distinguishing between young tens and older ones'. Yoti is claimed to assert that its system has no 'discernible bias across gender or skin tone'. The Verge goes on to cite previous research which indicates that facial recognition is 'less reliable for people of colour, gender-nonconfirming people, and people with facial differences or asymmetry. The Verge asserts that these issues would unfairly block some people from accessing the services. I observe, however, that failures of face-based age detection systems may, in addition to blocking legitimate users, also permit juveniles to access services to which they're not entitled. Ofcom may be aware of the tale of young women of 16 or 17 applying makeup in order to get cigarettes or accompany their older boyfriend into the pub. Whether such a ploy would fool a face-based age determination system may need further research but is closely allied to the issues I raise above.
Question 6: Do you agree with our proposed guidance that providers should consider accessibility and interoperability when implementing age assurance? Please provide any information or evidence in support of your views.	Confidential? – ~~Y~~ / N
Question 7: Do you have comments on the illustrative case study we have set out in the guidance? Do you have any supporting information or evidence relating to additional examples of how the criteria and principles might apply to different age assurance processes?	Confidential? – ~~Y~~ / N

Question	Your response
Question 8: Do you agree with our proposed guidance on the record-keeping duties? Please provide any information or evidence in support of your views.	Confidential? – ~~Y~~ / N
Question 9: Do you have any comments on our proposed approach to assessing compliance with the duties on service providers who publish or display pornographic content, including on the proposed examples of non-compliance? Please provide any information or evidence in support of your views.	Confidential? – ~~Y~~ / N
Question 10: Do you have any comments on the impact assessment set out in Annex 1? Please provide any information or evidence in support of your views	Confidential? – ~~Y~~ / N The Act also creates a significant risk of 'outing' LGBTIQA+ people, who access websites that will now need to verify their identities. According to La Trobe University (at https://www.latrobe.edu.au/students/support/wellbeing/resource-hub/lgbtiqa/what-lgbtiqa-means) LGBTIQA+ is an evolving acronym that stands for lesbian, gay, bisexual, transgender, intersex, queer/questioning, asexual. Protecting their real-life identities allows LGBTIQA+ people to share their experiences and sexuality while protecting their privacy. Putting this at risk poses a direct threat to their safety and creates a serious issue for those who, for whatever reason, are not public about their sexual and gender identities. While it may also not be the intention of this regulation to place non-pornographic material that is connected to sex behind strict age-gates, there are countless examples of material related to female sexuality and LGBTIQA+ experiences being incorrectly marked as pornography as well as loud campaign groups bent on arguing for this. It is concerning that this impact is lacking from Annex 1.

Question	Your response
Question 11: Do you agree that our proposed guidance is likely to have positive effects on opportunities to use Welsh and treating Welsh no less favourably than English? If you disagree, please explain why, including how you consider the proposed guidance could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.	Confidential? – ~~Y~~ / N

Please complete this form in full and return to Part5Guidance@ofcom.org.uk.