Open Rights Group

23 April 2018

Consultation Response

Draft Guidance on Age Verification Arrangements

and

Draft Guidance on Ancillary Service Providers

About Open Rights Group

Open Rights Group is a dedicated group of digital rights defenders working on Internet censorship, free speech, privacy, surveillance and data protection.

Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights.

We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions, public education and tech projects.

Open Rights Group is a non-profit company limited by Guarantee, registered in England and Wales, company number: 05581537. We are based in London and Edinburgh and we were founded in 2005.

Table of Contents

Summary

The age verification scheme as implemented by the Digital Economy Act 2017 (DEA) suffers from a number of pitfalls and potential risks, which will be outlined in detail in this consultation response.

In particular:

- The aim of age verification is defined as being for the “protection of children”, however, under scrutiny, it is clear that the scheme will be unable to achieve this aim.
- This consultation indicates that the BBFC intend to consider material which ought to be out-of-scope for an age verification system, such as extreme pornography and child abuse material.
- The BBFC also indicate that they intend to consider the *effectiveness* of a response to a non-compliant person before issuing it, but do not indicate an intent to consider the *proportionality* of that response.
- The scheme as a whole lacks any specific and higher level of privacy protection, despite the existence of unique problems. In particular, any data breaches cannot be properly compensated for in terms of reputational, career and relationship consequences.
- The scheme risks infringing free expression rights by granting the BBFC web blocking powers.
- The ability of the BBFC to give notice to ancillary service providers creates legal uncertainty and incentivises disproportionate actions on non-UK persons.
- As a whole, the age verification scheme fails to understand the limitations faced by the BBFC in terms of regulating overseas providers in a fair and proportionate manner.

Recommendations

Throughout this document, recommendations are numbered for ease-of-reference. They are also summarised below:

1. The BBFC must ask the Government to re-evaluate the age verification requirement, and assess if or how the legislation could be amended in order to ensure that it is proportionate and able to meet its own stated aims.
2. The BBFC must ask the Government to justify why they feel that the extreme pornography blocking powers appropriately fall within the scope of the stated aims of pornography-related age verification.
3. The BBFC must raise the concern with the Government that some of the material they have been asked to focus resources on dealing with should be out-of-scope.
4. The BBFC must implement a test of proportionality for notices under section 21 and 23.

5. The BBFC must consider the issue of social exclusion from age verification and ensure that there are sufficiently accessible means of age verification for members of society who may not have ready access to credit cards or official documentation.
6. The BBFC must publish practical implementation guidelines for age verification providers to complement any guidelines they make about user privacy. User privacy should be enforced as a strict requirement for age verification providers and providers which do not meet privacy standards should not be considered compliant.
7. The BBFC must highlight the value of maintaining user choice, and recommend that the Government implement additional legislation which obliges pornographic sites to offer users a choice of age verification services.
8. The BBFC must call upon the Government to implement mandatory privacy regulations for pornography-related age verification and a body should be assigned to the task of ensuring compliance with these regulations.
9. The BBFC must conclude from this consultation that the legal framework is not yet in place for age verification to safely commence, and should also communicate this fact to the Government.
10. The system of giving notice to ancillary service providers is fundamentally flawed as it exists with no statutory duty to act, carries significant risks, and puts service providers in a difficult contractual position. Requests to withdraw services will appear unreasonable in many cases, due to the differences in international legal requirements. The BBFC must communicate to the Government that the current regime is inadequate, unfair and needs to be ceased.
11. If the BBFC wish to continue with plans to give notice to ancillary service providers under section 21, the content of these notices must clearly and openly state that the service provider is not under a legal obligation to comply.
12. The BBFC must ask the Government to clarify their expectations about how notices under section 21 will function and should take care to ensure that section 23 blocking notices are not relied on automatically as a remedy against resistant ancillary service providers.
13. The BBFC should ask the Government to ensure that any web blocking power is exercised through court order.
14. The BBFC must not consider social media networks as ancillary service providers.
15. Ancillary service providers must not be added to the current list without being consulted.
16. The BBFC must communicate to the Government the fact that it is unable to assess the impact or proportionality of asking an ASP to take action, and that it it is therefore unreasonable to expect it to issue notices.
17. An appeals process should be implemented which allows recipients of BBFC-issued notices to appeal them via an independent third-party.

Age Verification Arrangements Response

Do you agree with the BBFC's approach as set out in Chapter 2?

Age verification's inability to meet its own stated aims

Section 2.1 of the consultation document confirms that age verification requirements will apply to "all providers of online pornography". However, in the document, the BBFC also note that they intend to take a "proportionate" approach to regulation for the purposes of best-achieving the stated aims of the Act, which it considers to be the "protection of children". The BBFC's focus on achieving the child protection goal of the legislation is highlighted in Sections 1.12, 2.2, 2.5, and 2.10.

This focus on a "proportionate" approach appears to be an acceptance by the BBFC of the practical impossibility of enforcing pornography-related age verification requirements on every pornographic site. In their report, the expert panel convened by the DCMS cited research which suggested that around 4% of the most frequented websites in the world are pornographic.[1] The task of verifying that age verification is correctly implemented on all of these sites would be, as the consultation document appears to have identified, well beyond the budgetary and time constraints of the BBFC. The BBFC as a body lacks the required resources to ensure that the legislation is enforced in such a way as to meet its own stated aims — namely the "protection of children".

When considering the child protection aims of the legislation, it would be unwise to ignore the fact that the policy position underpinning the legislation is that viewing legal adult pornography causes harm to children. As academic research in the area offers no concrete evidence in support of this position, any legislative intervention must therefore be defended solely as an application of the precautionary principle, and not on the basis that it is offering protection from well-defined harms. As noted by the expert panel convened by the DCMS, "this makes it doubly important that those interventions are truly effective in reducing risk, with little collateral damage".[2]

Age verification requirements are only able to prevent children from coming across compliant pornographic sites incidentally and unwittingly. Age verification will never be able to prevent a determined child from accessing pornographic material. As the Government's Impact Assessment acknowledges, the use of technical solutions — such as the Tor network — would allow a user to sidestep the need to verify their age by making it appear to a pornographic site that they are a visitor from outside of the UK.[3] Peer-to-peer file sharing

[1] Ogas O. (2011). *A Billion Wicked Thoughts: What the Internet Tells us About Sexual Relationships*. London: Penguin.
[2] Nash, Victoria; Adler, Joanna R.; Horvath, Miranda A.H.; Livingstone, Sonia; Marston, Cicely; Owen, Gareth; Wright, Joss. (2015). *Identifying the routes by which children view pornography online: implications for future policy makers seeking to limit viewing*.
[3] Department for Digital, Culture, Media & Sport. (2017). *Impact Assessment (IA)*.

networks, offline storage media, and cyberlocker services can also be used by children sharing and consuming pornography outside of the reach of age verification technology.

Determined children can also use interpersonal messaging apps — such as WhatsApp, Kik, or Snapchat — to share pornography directly with each other. As the expert panel's report to the DCMS noted, on such networks, "content is as hard to regulate as would be a real-time face-to-face conversation".[4]

In addition, the BBFC's current position is that social media platforms will fall under the definition of "ancillary service provider". Whilst popular social media platforms like Facebook and YouTube already prohibit users from uploading pornography, other social platforms such as Twitter, Tumblr, and Reddit allow such content freely. These services will not be required to implement pornography-related age verification.

The proliferation of networks by which children will be able to actively seek out pornography outside of the reach of age verification clearly demonstrates the legislation's inability to meet a generalised child protection aim. Any defence of age verification as a necessity must therefore be based solely on the aim of preventing children from accidental or incidental viewing of pornography. This further narrows the scope of the legislation's aims, thereby weakening the argument that pornography-related age verification is a necessity for which the associated impact upon free expression rights can be tolerated.

The expert panel's report noted that, instead of using age verification technologies, an alternative possible route of intervention would be to focus Government resources on developing a mandatory personal sexual and health education (PSHE) curriculum for use in schools. They acknowledged the findings of the House of Commons Education Committee, who stated in 2015:

> "PSHE requires improvement in 40% of schools. The situation appears to have worsened over time, and young people consistently report that the sex and relationships education (SRE) they receive is inadequate".[5]

At a minimum, improving SRE in schools ought to be a parallel focus to implementing pornography-related age verification technology. This point could, however, be taken further to suggest that — with the current legislation apparently unable to meet its own stated child protection goals — focusing resources on age verification technology at all offers a mere mask over a wider societal problem, rather than tackling it directly as may be better achieved through improved SRE.

Serious concerns exist about the proportionality of legislation which is unable to achieve its own stated aims, and this is especially true where that legislation allows for penalties which represent a gross "collateral damage" to fundamental rights and freedoms. Age verification

---

[4] Nash, Victoria; Adler, Joanna R.; Horvath, Miranda A.H.; Livingstone, Sonia; Marston, Cicely; Owen, Gareth; Wright, Joss. (2015). *Identifying the routes by which children view pornography online: implications for future policy makers seeking to limit viewing*.

[5] https://publications.parliament.uk/pa/cm201415/cmselect/cmeduc/145/145.pdf

technology is likely to result in a chilling effect for viewers of legal content, and for the operators — and potential future operators — of pornographic sites.

The blocking powers afforded to the BBFC by the Digital Economy Act 2017 also represent a serious derogation to the free expression right afforded to those in the UK and are thus a human rights issue. With the above in mind, particularly weighty reasons are required to justify the necessity of the pornography-related age verification requirement in law, and such justifications have not been provided.

Recommendation [1]: *The BBFC must ask the Government to re-evaluate the age verification requirement, and assess if or how the legislation could be amended in order to ensure that it is proportionate and able to meet its own stated aims.*

Extreme pornography does not fit within the scope of the legislation's aims

Under the Digital Economy Act, the BBFC are granted statutory powers to request that ISPs block sites which are making "extreme pornographic material" available to users in the United Kingdom. This power is also discussed by Section 2.9 of the consultation document.

Extreme pornographic material is prohibited in the UK by way of s.63 Criminal Justice and Immigration Act 2008. Possession of such material carries a penalty of up to 3 years imprisonment or a fine.

In their 2005 consultation paper which considered the possession of extreme pornographic material, the Home Office highlighted their belief that "very little potentially illegal pornographic material found on the Internet originates from within the UK".[6] Whilst the fact that most of this material is hosted outside of the UK presents understandable difficulties for a Government wishing to reduce the spread of such material, it is not an appropriate approach to attach web blocking powers to legislation which serves a different stated aim. It is also not appropriate to grant such web blocking powers to the discretion of a private company such as the BBFC, regardless of whether Government oversight exists for blocking notices after they are served on ISPs.

Any system of web blocking should be must prescribed by legislation — with clear aims that blocking could reasonably be expected to achieve, must not devolve responsibility to private companies, and must ensure that any notice to block content is judicially authorised before being issued. The system to deal with extreme pornographic material created by the Digital Economy Act does not satisfy these requirements.

As the BBFC have suggested, the aim of age verification is to ensure the "protection of children". Age verification is therefore in pursuit of a different aim to the extreme pornography offence, the aims of which are stated by the Home Office's 2005 consultation document as being:

[6] Home Office. (2005). *Consultation: On the possession of extreme pornographic material*.

> "to try to break the demand/supply cycle and to discourage interest in this material which we consider may encourage or reinforce interest in violent and aberrant sexual activity".[7]

It could be argued that, if extreme pornographic material is harmful to children, that granting blocking powers to the BBFC may not fall outside of the scope of a "protection of children" aim. However — as noted by the Home Office in the executive summary to their 2005 consultation — research on extreme pornography does not support a definite conclusion that the material represents a risk of harm:

> "As to evidence of harm, conducting research in this area is complex. We do not yet have sufficient evidence from which to draw any definite conclusions as to the likely long term impact of this kind of material on individuals".[8]

With respect to the above, serious concerns are raised about the fact that the Government has chosen, through the wording of the Digital Economy Act, to grant the BBFC the power to require blocking action against a class of content which is already dealt with by existing legislation with different aims. The regulation of extreme pornography therefore falls outside of the stated aims of age verification. If the Government wishes to further regulate the landscape of extreme pornographic material, it must be done so through new legislation, and should not be enforced as an add-on to a regulatory system with a different aim. The BBFC should not be required to consider the censorship of extreme pornographic material as part of their remit.

Recommendation [2]: *The BBFC must highlight the above concerns to the Government, and ask them to justify why they feel that the extreme pornography blocking powers appropriately fall within the scope of the stated aims of pornography-related age verification.*

Other material which should be out-of-scope

In Section 2.5, the BBFC make reference to focusing their limited resources on sites which are "most frequently visited, particularly by children". As the information about which pornographic sites are more frequently visited by children would be difficult to research ethically, this statement further brings into question whether the BBFC's approach as outlined can reasonably be expected to achieve the stated aims of the legislation.

In Section 2.5, the BBFC also indicate an intent to target sites which contain "potentially indecent images of children". As such content is prohibited by law, and is subject to a strict liability possession offence, this seems to be an entirely irrelevant consideration for the purposes of age verification. It is unhelpful to confuse discussion of the regulation of legal adult pornography with any matters which involve illegal child abuse material, as this may lead to public confusion around the BBFC's role and the purposes of age verification. The regulation of child abuse material falls outside of the scope of the Digital Economy Act, and it should not be a concern of the BBFC.

---

[7] *Ibid.*
[8] *Ibid.*

Recommendation [3]: *The BBFC must raise the concern with the Government that they are being required to consider material and focus resources on dealing with matters which should be out-of-scope and are unrelated to achieving the stated aim of age verification.*

Section 21 and 23 assessments must include a proportionality test

In Section 2.10, the BBFC confirm that before issuing a notice under section 21 or 23 of the Act, they will make an assessment of "which course of action will be most effective in achieving the child protection goals of the legislation". Effectiveness could be achieved at the expense of proportionality, and the BBFC has a responsibility to ensure both. Given the BBFC's stated commitment to proportionality, they should apply a test of *proportionality* as well as merely a test of *efficacy* when undertaking their assessment. Age verification must not be pursued without regard to cost; any assessment must take account of the wider social impact of methods used, especially with regards to interference with free expression. This test of proportionality should also be applied to the BBFC's actions described in Section 2.11.

Recommendation [4]: *The BBFC must implement a test of proportionality for notices under section 21 and 23.*

Do you agree with the BBFC's age-verification standards set out in Chapter 3?

Age verification risks social exclusion

Section 3.2 of the consultation briefly outlines some of the documents and methods which might be accepted to verify the age of a user. Whilst these documents may suffice to verify age from a practical perspective, particular consideration should be given to the potential for such measures to lead to social exclusion, as not all members of the adult population have access to such documents. An age verification system which risks excluding members of the population from engaging with legal content as a result of their financial situation, citizenship status, or disability represents a serious concern for free expression.

The implication in Section 3.6 that some bank cards may suffice for the purposes of age verification — but only those which can only be held by users above the age of 18 — is particularly problematic, as it offers the implication that credit cards are likely to be one of the widely-implemented methods of verifying age. A system in which a person's freedom to view entirely legal material may be restricted as the result of having a poor credit rating or financial history is particularly hard to defend.

When considering the use of bank cards for the purposes of age verification, the BBFC should also carefully consider the security implications of normalising the process of inputting sensitive payment data into websites to verify age before being granted access to pornographic content.

The risk that users may be deterred from interacting with legal pornographic material as a result of an "inability to prove their age" was acknowledged by the Government in their Impact Assessment.[9]

Recommendation [5]: *The BBFC must consider the issue of social exclusion from age verification and ensure that there are sufficiently accessible means of age verification for members of society who may not have ready access to credit cards or official documentation.*

Privacy guidelines are non-binding

In Section 3.4, the consultation document makes some reference to privacy, mentioning a desire for pornography-related age verification providers to confirm "age but not identity". Whilst this is a worthy goal — as it would increase privacy protection for the users of age verification tools — there are practical difficulties associated with conducting online age checks without also needing to verify a user's identity as part of the process. The rest of the consultation document offers no practical suggestion as to how this could be implemented, and the advice is non binding. Privacy should be a strict requirement, and full technical guidelines should be produced which describe methods of age verification in which a system does not learn the identity of users.

In Section 3.7, the consultation outlines a general privacy recommendation for those wanting to implement pornography-related age verification, suggesting that they "collect the minimum data required to establish that the user is aged 18 or above". Again, no practical implementation guidelines or recommendations are offered which would provide advice on how this might be achieved by pornography-related age verification providers. This guidance is also non-binding.

If the BBFC intend to suggest that providers must collect the minimum data required to verify age, and must verify age without also verifying identity, then they should publish full technical guidelines to accompany this requirement, which should describe possible methods of implementing such a system.

Recommendation [6]: *The BBFC must publish practical implementation guidelines for age verification providers to complement any guidelines they make about user privacy. User privacy should be enforced as a strict requirement for age verification providers and providers which do not meet privacy standards should not be considered compliant.*

Choice of providers

In Section 3.8, the consultation document suggests that operators of sites with an obligation to implement pornography-related age verification should go beyond the mandatory requirements of the Digital Economy Act and ensure that their sites offer users a choice about which tool to verify with. Whilst it is encouraging to see this recommendation, which

[9] Department for Digital, Culture, Media & Sport. (2017). *Impact Assessment (IA)*.

will empower users to make choices about which pornography-related age verification tools they use, it is disappointing that this requirement is not mandatory or enforceable. Secondary legislation clarifying a mandatory privacy framework for sites and pornography-related age verification providers is necessary here, as will be discussed in later sections.

Recommendation [7]: *The BBFC must highlight the value of maintaining user choice, and recommend that the Government implement additional legislation which obliges pornographic sites to offer users a choice of age verification services.*

Do you have any comments with regards to Chapter 4?

The regulatory gap omitting privacy in pornography-related age verification

Throughout the consultation document, the BBFC defer data protection concerns to the ICO, and do not offer practical or binding guidance on privacy concerns. This highlights the existence of a worrying regulatory gap in the structure created by the legislation. The BBFC are able to consider tools only insofar as to assess whether or not they appropriately verify age, and the ICO consider data protection only insofar as whether tools meet their legal obligations under data protection law. This is further confirmed by Section 4.8b of the draft guidance, which outlines the scope of the agreement between the ICO and BBFC as being solely about "data protection compliance concerns". No regulations or regulators are assigned to the task of assessing whether pornography-related age verification tools adequately protect user privacy.

The document does suggest, in Section 4.4b, that the ICO may consider it a "data protection compliance concern" where a provider uses pornography-related age verification data for purposes other than age verification "without the knowledge of the individual concerned". Whilst on the face of it, this may be seen to offer protection for user privacy, it is not made clear whether compliant data re-use requires 'actual knowledge' of the user, or whether it would suffice that this provision existed in a *Terms of Service* or *Privacy Policy* document that the user may blindly accept before using a service. Many *Terms of Service* documents contain clauses which indicate that the terms can be varied by the site operator, often without a requirement to notify users who have previously signed the terms. This raises the concern that this requirement may be treated as 'complied with' even where a set of terms have been changed after a user has accepted them.

The re-use of pornography-related age verification data for purposes other than age verification should require *clear and informed* consent of the user, and this should be strictly enforced by regulatory oversight rather than being treated an issue which "may raise … concerns".

One additional concern is that pornographic age verification tools are not proactively assessed for data protection compliance by the ICO, and are only given an incidental inspection by the BBFC whilst they are assessed for their ability to accurately verify age. As

highlighted by Section 3.9, the BBFC's scope to assess certain data protection compliance requirements is limited. Indeed, the BBFC have previously expressed concern that they are not equipped for a role that involves an assessment of data protection law.[10]

Protecting privacy is not the same as ensuring data protection compliance, and thus the Government cannot expect the ICO to take up the role of protecting user data. It is possible for a service to comply with data protection legislation whilst engaging in data mining or data profiling activities, or selling user data to third parties. Privacy as a human rights concern is broader than data protection, and broader than the remit of the ICO.

Recommendation [8]: *The BBFC must call upon the Government to implement mandatory privacy regulations for pornography-related age verification and a body should be assigned to the task of ensuring compliance with these regulations.*

Risks of age verification for pornographic content

Data protection law does not provide sufficient protection to the sensitive dataset that is represented by the intimate browsing history of a user of pornography-related age verification tools. These risks are not currently being discussed by any official body, including the DCMS or BBFC.

The consultation fails to properly distinguish between the different functions and stages of an age verification system. The risks associated with each are separate but interact. Regulation needs to address all elements of these systems. For instance:

1. Choosing a method of age verification, whereby a user determines how they wish to prove their age.
2. The method of age verification, where documents may be examined and stored.
3. The tool's approach to returning users, which may involve either:
    a. attaching the user's age verification status to a user account or log-in credentials; or
    b. providing a means for the user to re-attest their age on future occasions.
4. The re-use of any age verified account, log-in or method over time, and across services and sites.

The focus of attention has been on the method of pornography-related age verification, but this is only one element of privacy risk we can identify when considering the system as a whole. Many of the risks stem from the fact that users may be permanently 'logged in' to websites, for instance. New risks of fraud, abuse of accounts and other unwanted social behaviours can also be identified. These risks apply to 20-25 million adults,[11] as well as to teenagers attempting to bypass the restrictions. There is a great deal that could potentially go wrong.

[10] https://www.theyworkforyou.com/lords/?id=2017-03-20b.64.0

[11] MindGeek have stated publicly that they expect 20-25 million adults to sign up to their *AgeID* tool within a few months of launching the platform.

Business models, user behaviours and potential criminal threats need to be taken into consideration. Risks therefore include:

Identity risks

1. Collecting identity documents in a way that allows them to potentially be correlated with the pornographic content viewed by a user represents a serious potential risk to personal and potentially highly sensitive data.

Risks from logging of porn viewing

2. A log-in from an age-verified user may persist on a user's device or web browser, creating a history of views associated with an IP address, location or device, thus easily linked to a person, even if stored 'pseudonymously'.
3. An age verified log-in system may track users across websites and be able to correlate tastes and interests of a user visiting sites from many different providers.[12]
4. Data from logged-in web visits may be used to profile the sexual preferences of users for advertising. Tool providers may encourage users to opt in to such a service with the promise of incentives such as discounted or free content.
5. The current business model for large porn operations is heavily focused on monetising users through advertising, exacerbating the risks of re-use and recirculation and re-identification of web visit data.
6. Any data that is leaked cannot be revoked, recalled or adequately compensated for, leading to reputational, career and even suicide risks.

Everyday privacy risks for adults

7. The risk of pornographic web accounts and associated histories being accessed by partners, parents, teenagers and other third parties will increase.
8. Companies will trade off security for ease-of-use, so may be reluctant to enforce strong passwords, two-factor authentication and other measures which make it harder for credentials to leak or be shared.
9. Everyday privacy tools used by millions of UK residents such as 'private browsing' modes may become more difficult to use to use due to the need to retain log-in cookies, increasing the data footprint of people's sexual habits.
10. Some users will turn to alternative methods of accessing sites, such as using VPNs. These tools have their own privacy risks, especially when hosted outside of the EU, or when provided for free.

Risks to teenagers' privacy

11. If age-verified log-in details are acquired by teenagers, personal and sexual information about them may become shared including among their peers, such as particular videos viewed. This could lead to bullying, outing or worse.
12. Child abusers can use access to age verified accounts as leverage to create and exploit a relationship with a teenager ('grooming').

[12] The developers of the *AgeID* tool have already indicated their intent to use a system which allows a user to stay persistently logged-in across all AgeID-enabled sites: https://www.ageid.com/business

13. Other methods of obtaining pornography would be incentivised, and these may carry new and separate privacy risks. For instance the BitTorrent network exposes the IP addresses of users publicly. These addresses can then be captured by services like GoldenEye, whose business model depends on issuing legal threats to those found downloading copyrighted material. This could lead to the pornographic content downloaded by young adults or teenagers being exposed to parents or carers. While copyright infringement is bad, removing teenagers' sexual privacy is worse. Other risks include viruses and scams.

Trust in age verification tools and potential scams

14. Users may be obliged to sign up to services they do not trust or are unfamiliar with in order to access specific websites.
15. Pornographic website users are often impulsive, with lower risk thresholds than for other transactions.[13] The sensitivity of any transactions involved gives them a lower propensity to report fraud. Pornography users are therefore particularly vulnerable targets for scammers.
16. The use of credit cards for age verification in other markets creates an opportunity for fraudulent sites to engage in credit card theft.
17. Use of credit cards for pornography-related age verification risks teaching people that this is normal and reasonable, opening up new opportunities for fraud, and going against years of education asking people not to hand card details to unknown vendors.
18. There is no simple means to verify which particular age verification systems are trustworthy, and which may be scams.

Market related privacy risks

19. The rush to market means that the tools that emerge may be of variable quality and take unnecessary shortcuts.
20. A single pornography-related age verification system may come to dominate the market and become the de-facto provider, leaving users no real choice but to accept whatever terms that provider offers.
21. One age verification product which is expected to lead the market — AgeID — is owned by MindGeek, the dominant pornography company online. Allowing pornographic sites to own and operate age verification tools leads to a conflict of interest between the privacy interests of the user, and the data-mining and market interests of the company.
22. The online pornography industry as a whole, including MindGeek, has a poor record of privacy and security, littered with data breaches. Without stringent regulation prohibiting the storage of data which might allow users' identity and browsing to be correlated, there is no reason to assume that data generated as a result of age verification tools will be exempt from this pattern of poor security.

[13] Sesen Negash, Nicole Van Ness Sheppard, Nathaniel M. Lambert & Frank D. Fincham (2015): *Trading Later Rewards for Current Pleasure: Pornography Consumption and Delay Discounting*, The Journal of Sex Research, DOI: 10.1080/00224499.2015.1025123

Potential enforceable privacy standards for pornography-related age verification

The risks highlighted above are mostly out of scope of the GDPR, which is a general data protection standard. Where risks and consequences in a policy area are significantly worse, other laws and enforceable standards are usually put in place.

One commercial example is the mandatory *PCI DSS* standard. Compliance with this information security standard is required by all bodies processing cardholder data for the purposes of processing electronic payments.

Compliance with PCI DSS is enforced by contract, rather than regulations. The main penalty for non-compliance is cessation of contract and refusal to process payments. Whilst PCI DSS is a better model than the laissez-faire approach taken by the Government to age verification, its contractually-enforced approach would not suffice to regulate in this scenario. Instead, there must be a regulatory power to force providers to sign up to a specified compliance model, or mandatory regulations backed by a regulator. Penalties for non-compliance should be more severe than can be offered by a purely contractual relationship.

Sensitive and potentially very detailed information about a user's sexual activities, interests, and orientation is of equal or greater significance than that of the payment card data that PCI DSS protects. For example, in the wake of the leak of data from the *Ashley Madison* website — a site which allowed like-minded users to arrange extramarital affairs — a number of users were driven to suicide over the public disclosure of their sexual activities.[14] Leaked payment card information can be revoked and fraud can be insured against, whilst highly personal information about a person's sexual interests and orientation cannot be removed from the public domain once it has been exposed.

The e-Privacy Directive is a legislative / regulatory approach to creating higher standards, including legal restrictions, on certain kinds of data collection and usage. It is aimed at ensuring that communications are confidential, and at minimising data collected as a result of the sending and receiving of email, for instance. These aims are not present or specified by the GDPR, so the e-Privacy Directive continues to make electronic communications more protected than will be the case for web visits associated with an age-verified person.

General regulations, like e-Privacy, need to exist over long periods of time, and cover a range of situations, which may not cover all the needs of this specific case. We would therefore recommend that minimum requirements are established in legislation, including the ability for BBFC or its delegate as the regulator to specify a particular standard similar to *PCI DSS* with its specific requirements being contractually enforced.

[14] http://www.bbc.co.uk/news/technology-34044506

Another approach could be to base regulation on an official ICO Code of Conduct.[15] Signatories would be subject to monitoring and fines. However, these are normally voluntary so would suffer the same problem as the present set up, unless a means can be found to make such a code compulsory.

Duty to regulate privacy for age verification systems

The lack of regulation for pornography-related age verification is particularly risky because the technologies are immature and a market has been created through necessity, rather than evolving naturally through consumer demand. A 'gold rush' mentality can be seen amongst age verification providers, who are seeking to profit quickly from an instant new market of over 20 million customers.

It is unclear how the market will develop. However, we noted above that the tendency to digital monopoly, cost cutting providers with poor security records and incentives to reuse data they should not be collecting, all show that the government's decision to leave pornography-related age verification *entirely* to the market is highly irresponsible.

Some problems with age verification may prove very hard to mitigate, even with strong regulation. Ironically, this may be particularly true for young people's privacy, as they are simply, and possibly unrealistically, expected to abstain from accessing pornography, or else must deal with the associated risks of acquiring content through means which sidestep the age verification requirement. This policy is therefore likely to have the unintended effect of putting under 18s at greater risk.

The lack of strong and specific privacy regulation of pornography-related age verification is the responsibility of the Government, who have been responsible for the drafting and implementation of the age verification requirement in law.

The BBFC has a responsibility to make it clear that the current age verification legislation is not fit for purpose, and that any failures will belong not to irresponsible providers or websites alone, but also to the Government for failing to provide an adequate regulatory framework.

Recommendation [9]: *The BBFC must conclude from this consultation that the legal framework is not yet in place for age verification to safely commence, and should also communicate this fact to the Government.*

---

[15] "If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority."

"If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover."

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct-and-certification/

Ancillary Service Providers Response

The approach in the guidance to ancillary service providers (ASPs) is flawed. This relates back to some underlying assumptions in the DEA. For instance, while the BBFC and the Government may regard pornography-related age verification as a significant matter, it is not present as a universal requirement anywhere else.[16] For most publishers and platforms, it is a local regulatory matter which they are entitled to ignore, except for UK purposes. The BBFC's approach does not seem to recognise this or suggest remedies which are UK-specific, except in regard to payment providers.

Furthermore, while the policy as whole focuses on the action of age verification, it has become highly blurred in relation to content, which may sometimes be published without age verification, sometimes not. For instance the same legal image may be:

- Acceptable to publish on a non-commercial pornographic website without age verification;
- Unacceptable to publish on a commercial pornographic website without age verification;
- Acceptable to publish on a social media platform as it is circulated by an individual.
- Subject to notice by the BBFC to a social media platform if it is circulated by a non-compliant person.
- Acceptable to post on a social media platform if it is circulated by a compliant provider.

This patchy, inconsistent and illogical situation is an inevitable consequence of the way the legislation is structured. The BBFC should bear this in mind as they stretch to accommodate the varying and contradictory requirements it has been asked to implement.

Do you agree with the BBFC's approach as set out in Chapter 2?

As much of the text in this section of the consultation document is identical to that found in the *Draft Guidance on Age-verification Arrangements* document, please find below a summary of recommendations provided by our response to that document above:

- A "proportionate approach" of the kind the BBFC intends to take requires that pornography is not universally subject to age verification. Large amounts of pornography will always remain out of reach of the regulator, so the legislation suffers from an inability to meet its own child protection aims. (Section 2.3)
- Extreme pornography does not fit within the legislation's stated aims and should not be the responsibility of the BBFC. (Section 2.5)
- Child abuse material is also out of the BBFC's scope and remit (Section 2.5)
- The BBFC must apply a test of proportionality and not just effectiveness when considering appropriate avenues of enforcement action (Sections 2.10, 2.11)

[16] Germany has an age verification regime, but this only applies to German users accessing sites hosted in Germany.

Notices to withdraw service risk causing significant and irrevocable damage

Requesting that an ancillary service provider (ASP) withdraw services from a non-compliant person puts the service provider in a difficult position. The provider is not legally required to comply with a notice under section 21, but there appears to be an expectation that they will.

Complying with a notice under section 21 could involve terminating accounts, deleting data, or taking action which is otherwise irrevocable. This could lead to significant and disproportionate financial damage for the non-compliant person and revoking the damage done by service withdrawal in the event that a person later becomes compliant may be impossible. For example, a Twitter account of a non-compliant person may be deleted in response to a BBFC notice, along with years worth of content, and a significant number of followers. If that person later becomes compliant, the BBFC indicate that they will inform Twitter that the request to withdraw services no longer applies. This, however, does not necessarily mean that the person's account, content, or followers can be reinstated.

In any case, it does not seem reasonable for a US provider, for instance Twitter, to withdraw its service for a US customer, when no US laws are being broken. At the same time, for Twitter to censor content only for UK customers would normally require that the content itself was not legal in the UK, which would not be the position here.

Whilst the approach makes sense for withdrawing blocking orders issued to ISPs, the desired effect of a notice served to an ancillary service provider, as confirmed by Section 3.6 of the consultation, is for the ancillary service provider to withdraw services to the non-compliant person. The withdrawal of services by an ancillary service provider is not necessarily something which may be "reversed" as simply as a webpage block under section 23, and the BBFC should bear this in mind.

Ancillary service providers may also be contractually or otherwise financially bound to provide services to the non-compliant persons in question. Withdrawing service or terminating accounts may lead to complex contractual issues which may put the ancillary service provider at legal or financial risk.

Recommendation [10]: *The system of giving notice to ancillary service providers is fundamentally flawed as it exists with no statutory duty to act, carries significant risks, and puts service providers in a difficult contractual position. Requests to withdraw services will appear unreasonable in many cases, due to the differences in international legal requirements. The BBFC must communicate to the Government that the current regime is inadequate, unfair and needs to be ceased.*

Notices to ASPs and payment service providers risk sidestepping due process

The framework for submitting notices to ancillary and payment services providers created by the Digital Economy Act create legal uncertainty. The BBFC are expected to issue notices to

ancillary and payment service providers requesting that they take action against legal material, but such providers do not have a statutory duty to act.

Recommendation [11]: *If the BBFC wish to continue with plans to give notice to ancillary service providers under section 21, the content of these notices must clearly and openly state that the service provider is not under a legal obligation to comply.*

Ineffective notices under section 21 will lead to disproportionate use of website blocking orders

Sections 2.9 and 2.10 make reference to the BBFC's power to give notice to payment services providers and ancillary service providers under section 21 of the Digital Economy Act. It is implied by this document and by the legislation that the expected result of serving such a notice is that the service provider will terminate services to the infringing site or remove the infringing content. Despite this, however, the legislation does not create a statutory duty for ancillary service or payment-services providers to comply with a notice when issued. Such notices can freely be ignored without fear of penalty, and this is to be expected of many providers, as compliance may involve taking action which is detrimental to their own business interests. As such, expecting widespread compliance with notices under section 21 is optimistic, and the BBFC may be forced to move directly to issuing blocking notices for the sites under section 23 of the Act. As web filtering is a direct act of censorship, this raises particular concerns with regard to chilling effects and free expression rights when the material to be blocked is, in itself, legal to possess and distribute.

The scheme as a whole risks a deepening use of blocking powers over time. It is also purely administrative. While appeals exist, website blocking ought to be subject to a court-based process rather than handed to a non-judicial organisation such as the BBFC. This would also make it less likely that BBFC would be placed under pressure to expand the extent of website blocking to compensate for any incomplete roll out of age verification.

Recommendation [12]: *The BBFC must ask the Government to clarify their expectations about how notices under section 21 will function and should take care to ensure that section 23 blocking notices are not relied on automatically as a remedy against resistant ancillary service providers.*

Recommendation [13]: *The BBFC must ask the Government to ensure that any web blocking power is exercised through court order.*

Do you agree with the classes of ASP set out in Chapter 3?

Issues raised by considering social media platforms as ASPs

As noted in our response to the *Draft Guidance on Age-verification Arrangements* above, the classification of social media platforms as "ancillary service providers" rather than as commercial providers of online pornography is an admission that the age verification

legislation cannot in practice meet its own stated aims — the "protection of children" — by reducing the availability of pornography.

Social media platforms, if considered as ASPs, are not subject to the obligation to implement age verification, and are not under a statutory duty to ensure that pornographic content on their platforms is removed or only accessible by those over the age of 18.

This approach is a significant challenge to the Government's assertion that pornography-related age verification is a necessity, as the classification of social media sites in this way will mean that some of the most widely-accessed websites in the world are considered as 'exempt' for the purposes of the age verification requirement.

As noted by the expert panel in their report, responses by children surveyed by the *Net Children Go Mobile* study suggest that social media is one avenue by which children may be exposed to sexual imagery online.[17] Unfortunately, requiring social media sites to implement age verification would be even less practical and disproportionate than with websites which are solely pornographic.

Nevertheless, social media platforms are providing a non-essential and peripheral or promotional service to pornographic publishers. While the Government and BBFC may desire that less pornographic material is circulated on social media, they should not try to oblige platforms to act in this way. Deletions of accounts would be disproportionate, and would also affect international audiences. Most publishers and platforms are not based in the UK.

The BBFC should also consider the inconsistencies caused by attempting to censor legal material purely on the basis of which actor is circulating it. The same images or links that the BBFC tries to remove by giving notice may otherwise be out of scope if posted by a different account holder on the ancillary service provider's platform. Even more inconsistently, a person whose pornographic sites correctly comply with age verification requirements may continue to post whatever content they wish without fear of receiving a notice. If the Government wishes to create a power to censor specific user accounts, it should seek that power separately, and ensure that such censorship is done only by court order.

Recommendation [14]: *The BBFC must not consider social media networks as ancillary service providers.*

Extension of definition should require consultation

Section 3.4 of the document notes that the BBFC reserve the right to extend the list of ancillary service providers beyond the list currently found in the guidance. The BBFC indicate that they will "seek to" inform ancillary service providers if they are being considered for addition to the list. This ought to be reformulated as a requirement, ensuring that the

[17] Nash, Victoria; Adler, Joanna R.; Horvath, Miranda A.H.; Livingstone, Sonia; Marston, Cicely; Owen, Gareth; Wright, Joss. (2015). *Identifying the routes by which children view pornography online: implications for future policy makers seeking to limit viewing*.

BBFC consults with providers or classes of providers who are under consideration, to avoid a situation in which ancillary service providers may receive an unexpected notice under section 21 without prior knowledge.

Recommendation [15]: *Ancillary service providers must not be added to the current list without being consulted.*

Effect of withdrawing services: legal uncertainty, and inconsistency

Section 3.6 notes that, when serving an ASP with a notice under section 21, the BBFC will request that the ASP in question withdraw services from the non-compliant person or site. This seems like a particularly heavy-handed approach on the part of the BBFC. Ancillary service providers can differ wildly in the practical aspects of the service they offer, and therefore the damage that is created by ASPs taking action will also differ wildly. In many cases, both the ASP and the pornographic producer will not be based in the UK. It would be unreasonable for the BBFC to expect a non-UK-based service provider to take action against a non-UK-based publisher on the advice of a UK-based regulator.

Recommendation [16]: *The BBFC must communicate to the Government the fact that it is unable to assess the impact or proportionality of asking an ASP to take action, and that it it is therefore unreasonable to expect it to issue notices.*

Appealing notices

Section 3.9 outlines a right for an ASP to make representations in the event that it feels that it has been wrongly notified by the BBFC. However, this section confirms that the withdrawal of a notice following such a representation is entirely down to the discretion of the BBFC. At a minimum, an ASP receiving a notice should have a right to appeal such a notice, which should involve an assessment undertaken by a body independent of the BBFC.

In addition to situations of wrongful notification, ancillary service providers should also be granted a right of appeal where they feel that a notice is disproportionate. The BBFC are not necessarily familiar with the technical structure and arrangement of the services provided to non-compliant providers, and thus compliance with some notices may represent a much wider disruption than the BBFC may anticipate. An ASP wishing to appeal a notice on the basis of proportionality must be able to do so. Again, any such appeals should be handled by an independent body.

The lack of this process, and the demands that the BBFC are making on third-parties again show the danger of relying upon administrative powers for law enforcement. In our view, any such notices must be independently authorised.

Recommendation [17]: *If the right to give notice to ASPs is retained, then an appeals process must be implemented which allows recipients of BBFC-issued notices to appeal them via an independent third-party.*