

**bbfc**

**Draft Guidance  
On Age  
Verification  
Arrangements &  
Draft Guidance On  
Ancillary Service  
Providers**

**CONSULTATION RESPONSES  
ORGANISATIONS AND INDIVIDUALS**

# CONTENTS

## FOREWARD & DISCLAIMER 6

## ORGANISATIONS

Action4	7	Marc Dorcel	48
AgeID	10	Mastercard	55
Ageify	14	NSPCC	59
AV Secure	16	Naturist Action Group	63
Backlash	19	Open Rights Group	65
Barnandos	25	Parentzone	88
Brass Horn Communications	27	PSHE Association	90
British Standards Institute	30	Restrained Elegance: Fetish Photography and Romantic Barefoot Bondage Magazine	93
Campaign Against Censorship	33	South West Grid For Learning	104
Childnet	35	Tara E. Beattie - Durham Law School, Durham University	105
Children's Charities' Coalition on Internet Safety	36	Under Age Sales Ltd/Age Check Certification Scheme	113
The Children's Commissioner for England	39	Verime	119
Frolicme	40	Yoti	124
GB Group (GBG)	42	Anonymous Organisation #1	128
Internet Advertising Bureau (IAB)	45	Anonymous Organisation #2	133

## INDIVIDUALS

### A

Agius, A 137  
Ainscoe, N 138  
Alexandru, F 140

Allan, A 140  
Ashby, L 142  
Ashford, S 142

Astbury, B 143

### B

Bailey, R 144  
Bain, D 144  
Bannister, T 145  
Barker, T 146  
Bathory, E 147  
Bates, T 148  
Beard, A 149  
Beesley, B 150  
Beldingford, R 151  
Bell, A 151  
Belmont, K 152  
Bennett, M 153

Benson, P 153  
Beresford, S 154  
Bidmead, C 154  
Birks, C 155  
Black, B 155  
Blackburn, S 156  
Blake, P & Jackson, M 157  
Bond, N 175  
Boschetti, C 175  
Bowden, P 176

Bowman, L 176  
Boydson, D 177  
Bradshaw, R 178  
Brock, S 178  
Brown, C 179  
Brown, F 179  
Brown, J 180  
Brown, R 180  
Brough, C 181  
Byrne, M 181

### C

Campbell, S 181  
Carrithers, M 182  
Carney, B 182  
Chamberlain, M 183  
Champion, N 183  
Cheetham, C 184

Clay, C 185  
Cobb, G 185  
Codd, P 186  
Collins, N 186  
Colman, M 187  
Connor, S 187  
Cossham, J 188

Courtneil, J 189  
Cox, J 189  
Crowther, A 190  
Cummins, M 191  
Curl, G 191

### D

Dabrowski, K 192  
Day, A 193  
Dickinson, S 193

Dixon-Phillips, P 194  
Doherty, B 194

Dore, J 195

### F

Farrow, M 195  
Feely, J 196  
Fennell, W 197  
Flaherty, S 198  
Florêncio, J 199

Foote, R 200  
Forrester, G 200  
Fountain, B 201  
Fox, P 202

Frewin, N 203  
Frewin-Ridley, M 204  
Frost, E 205

### G

Garnett, J 205  
Gershon, T 206

Gillespie, T 206  
Graham, B 207

Grinham, C 207  
Gunn, A 208

### H

Hall, C 209  
Harris, R 210  
Harrison, A 210  
Hembury, P 210

Henderson, I 211  
Herriges, M 211  
Hicks, D 212  
Hilliard, C 213

Hooper, R 214  
Lady Howe, E 215  
Howell, R 217  
Hughes, R 217

### I

Inglesant, P 218

*J*

Jardine, C 218  
 Jary, A 219  
 Jerome, M 219

Jolly, S 219  
 Jones, C 220  
 Jones, L 220

Jones, R 221

*K*

Kahlon, P 222  
 Kandola, N 222  
 Kay, F 223  
 Kennedy, S 223

Khan, K 223  
 Kilham, D 224  
 King, A 225  
 King, B 225

Kirshen, M 226  
 Kotenko, A 227

*L*

Laycock, R 227  
 Le Mare, P 228

Leeming, R 229  
 Linfield, A 230

Livesey, D 231  
 Lotito, J 231

*M*

MacAdam, A 232  
 Mallinson, P 232  
 Marsden, G 233  
 Marsh, J 235  
 Marshall, S 236  
 McCafferty, D 236  
 McDonnell, K 236  
 McDougall, A 237

McGowan, B 237  
 McGowan, M 237  
 McNally, C 238  
 McNab, A 238  
 McQueen, A 238  
 McRobert, C 239  
 Middleton, C 239  
 Morgan, A 239

Morley, W 240  
 Morris, S 240  
 Mosson, P 241  
 Mount, P 241  
 Mower, M 242  
 Moyes, M 243  
 Muffett, A 244

*N*

Neill, R 248

Neilson, J 248

*O*

O'Sullivan, J 248

Owen, D 249

*P*

Pearce, G 249  
 Pfister, N 249

Piper, J 250  
 Price, B 251

Putt, M 251

*Q*

Quin, L 252

Quinn, A 252

*R*

Raymond, J 253  
 Richards, C 253  
 Rigley, L 254

Risdon, J 255  
 Rix, D 256  
 Robertson, L 257

Ruark, M 257  
 Rushworth, A 258  
 Russell, S 259

*S*

Sambrook, I 259  
 Sandfield, A 259  
 Sargeant, T 260  
 Sarll, A 261  
 Saxon, B 262  
 Saxton, I 262  
 Scratcher, J 263  
 Scott-Moncrieff, C 264

Shah, P 265  
 Shaw, C 266  
 Shephard, R 266  
 Smedley, N 267  
 Smith, J 267  
 Snyder, M 268  
 Stackhouse, T 268  
 Steeg, T 269

Steiner-Goldberg, S 269  
 Steward, R 270  
 Stonebanks, L 270  
 Styles, D 271  
 Swift, M J 272  
 Symes, D 272

## T

Taylor, C 273  
Taylor, D 274  
Temple, J 276  
Templeman, C 277

Thomas-hayter, A 277  
Thomson, C 278  
Thomson, R 279

Tolmie, J 279  
Trainer, T 280  
Tybalt, Z 281  
Tyszko, S 281

## U

Underhill-Tyrell, C 282

Urquhart, S 282

## V

Valenti, F 283

Voisey, F 284

## W

Wannell, S 284  
Ward, C 285  
Ward, D 285  
Warren, J 286  
Webb, R 287  
Wheeler, M 287  
White, R 288

Whitley, E 288  
Wickenden, P 288  
Wilding, P 289  
Williams, M 289  
Williams, M 290  
Williams, M 290  
Williamson, Z 291

Wilson, A 292  
Wingmore, I 292  
Woolfe, M 293  
Wragg, D 293  
Wright, D 294

## Y

Youett, C 295

Young, A 295

Young, C 296

## Anonymous Responses

Number 1 297  
Number 2 298  
Number 3 299  
Number 4 302  
Number 5 303  
Number 6 304

Number 7 306  
Number 8 307  
Number 9 310  
Number 10 314  
Number 11 315  
Number 12 316

Number 13 316  
Number 14 324  
Number 15 335  
Number 16 337  
Number 17 338  
Number 18 338

## FOREWORD

The British Board of Film Classification was designated as the age-verification regulator under Part 3 of the Digital Economy Act on 21 February 2018. The BBFC launched its consultation on the draft Guidance on Age-verification Arrangements and draft Guidance on Ancillary Service Providers on 26 March 2018. The consultation was available on the BBFC's website and set out the following questions:

### Guidance on Age-Verification Arrangements

- Do you agree with the BBFC's Approach as set out in Chapter 2?
- Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?
- Do you have any comments with regards to Chapter 4?

The BBFC will refer any comments regarding Chapter 4 to the Information Commissioner's Office for further consideration.

### Draft Guidance on Ancillary Service Providers

- Do you agree with the BBFC's Approach as set out in Chapter 2?
- Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

The consultation ran for 4 weeks and closed on 23 April 2018, although late submissions were accepted until 8 May 2018.

There were a total of **624** responses to the consultation. The vast majority of those (**584**) were submitted by individuals, with **40** submitted by organisations. **623** responses were received via email, and one was received by post.

The following document contains the **267** responses which gave express consent for their publication.

The BBFC have published a separate consultation response document.

## DISCLAIMER

Some responses contained in this document contain hyperlinks to other websites which are not under the control of the BBFC. The BBFC is not responsible for the nature, content and reliability of those links. The inclusion of links does not imply a recommendation or endorsement of the views expressed within them.

## **Action 4 response to Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers**

Action 4 welcomes this opportunity to respond to your Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers.

As a membership driven trade association representing commercial businesses operating within the Premium Rate telephony sector whatever medium that may be communicated by we are starkly aware that effective regulation is intrinsically linked to the good levels of industry and consumer trust and in turn a buoyant industry. Key to this effective regulation and protection is not making onerous demands on commercial entities.

Action 4 has only recently been made aware of the BBFC consultation regarding Age Verification Arrangements and Ancillary Service Providers. It is regrettable that a consultation of this nature, having as it does major implications for the privacy of individuals, graphically highlighted by the Cambridge Analytica scandal, has been rushed out at short notice and prior to a public holiday period with a consultation period that has imposed an equally short deadline. Added to this the author was only made aware of your consultation in the last 48 hours and therefore the below is a synopsis in response.

You have set out below specific questions, however we have responded by providing our overarching comments to the whole document, due to timescales the ability to provide full analysis of the consultation has been limited. We would welcome further dialogue with you if this would be helpful.

### **Guidance on Age-Verification Arrangements**

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

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

Do you have any comments with regards to Chapter 4?

The BBFC will refer any comments regarding Chapter 4 to the Information Commissioner's Office for further consideration.

### **Draft Guidance on Ancillary Service Providers**

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

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

We would make the following points:

- The appointment of BBFC is welcomed as is any focus on seeking to protect and care for “minors” (a child/ren), and the vulnerable.
- We note that considerable emphasis is placed on the need to prevent access by “minors” (a child/ren), and the related process whereby that may be achieved. However, adults (aged 18+) should be able to access lawful content without unreasonable difficulty and in a manner that affords them **full and adequate protection** against misuse of their personal data.

We understand that BBFC will have no powers to set strong privacy standards; similarly the Government has not done so. Yet it is obvious that the Age Verification (AV) poses a grave danger to user privacy. The recent Cambridge Analytica scandal graphically highlights what may happen in the absence of strong and robust privacy requirements particularly in relation to data protection.

Since the Government has not taken the lead in protecting users privacy, Providers of AV tools should be required to adhere to strict privacy guidelines prescribed by BBFC and they should be required to demonstrate how they will satisfy these Guidelines before the proposed AV system is implemented. These Guidelines should compel AV Providers to procure that their software ensures that user's data will not be abused, sold or hacked.

- More emphasis needs to be made on how BBFC will ensure that websites that have been subject to sanction/taken offline, can get back online/restore their merchant accounts as soon as reasonably possible after complying with BBFC's requirements.



- BBFC annual audits as to the effectiveness of their process should be transparent, with industry being consulted.
- We need more details regarding the Appeals Procedures/Dispute resolution process.
- There is a need to ensure that regulation is applied in a unified manner across all platforms and media rather than piecemeal and selectively.
- We need more clarity regarding how a previously non-compliant website can reverse the process once its AV is judged by BBFC to be properly in place.
- BBFC should come forward with pro forma examples of the style of notices that may be issued e.g.: enforcement notices?
- Consideration could be given to BBFC issuing a certificate to confirm that a website is compliant? This may be a requirement of suppliers/banks/insurers
- Reporting needs to include stakeholder input and be transparent whenever possible.

## **Conclusion**

Key to effective regulation and protection of all consumer's what age is not making onerous demands on commercial entities, particularly in regard of ensuring that "minors" (child/ren) cannot access information, material or content which is deemed unsuitable, it is unrealistic to think that a "minor" (child/ren) cannot obtain the ability to meet age verification criteria that may be set out. We would always support education of parents/carers and those with parental responsibility to ensure that "minors" (child/ren) have all the relevant and realistic protections in place for their charges.

In the Premium Rate Sector we have encountered age verification problems numerous times in the past. Be minded that it is not in our industry best interests to allow those who are "vulnerable" in society to access inappropriate content; our industry relies on repeat business, effective and workable regulation and fundamentally good will. We welcome your consultation and look forward to working with you in the future.

## **AgeID response to BBFC consultation on the “Guidance on Age-Verification Arrangements”**

As stated in the Introduction of the Guidance, the primary purpose of Part 3 of the Act is the protection of children from pornographic material online. All our comments below have this primary purpose in mind. If the outcome of the law is that children can continue to stumble upon pornographic images, then the law will have failed.

We firmly believe it is the role of parents, not government, to monitor children’s browsing habits, and whilst this law attempts to add a further layer of protection, it also runs the risk of sending a message that the government have taken this issue out of parents’ hands. This can lead to a reduction in parental supervision. We therefore recommend that the government and/or regulator commits to a significant education initiative for parents, making them aware of the many available tools to help protect children online.

This is a complicated area and if significant issues are ignored, the law will not achieve its goal. Worse still, it could create new, larger problems which will have a detrimental effect on both children and adults.

### **A Proportionate Approach**

We understand that the regulator must begin enforcement somewhere, and it is reasonable they should start with highly trafficked sites. However, the overall approach is flawed and will not stop children from stumbling across pornographic content. A plan with more common sense would be a non-proportionate, advanced notice approach, i.e. The regulator identifies all pornographic sites (ISPs retain such a list for the current active filtering program, which amount to upwards of 4.5 million domains), and inform them in advance that they will all be enforced against on X date unless they enable age verification. This would result in a significant effect on day one of enforcement, rather than a slow drip of compliance as and when the regulator prioritises each site.

During the passage of the Bill through parliament, David Austin, CEO of the BBFC, gave evidence to the Committee that there are “1.5 million new pornographic URLs coming on stream each year”. Simply monitoring these new domains would take a rate of over 4,000 per day, not including any downtime for weekends or holidays. This alone seems like an impossible task, without even taking into account the existing 4.5 million domains which could be taken out of the equation immediately by following a non-proportionate, advanced notice approach.

Assuming the proportionate approach stands, and the BBFC will be tackling a figure far below the 16,000 domains they would have to monitor in the first year – some examples of how children whose methods of internet access have not been secured by parents, will stumble across pornographic content online:

- 1) Curiously accessing a site they may have heard mentioned by adults
- 2) Searching for an innocuous term on a search engine, which could lead to:
  - a. A link to a pornographic website
  - b. An image displayed directly in the search engine
- 3) Using social media platforms which permit children to access them, but also permit pornographic content

In the examples above, (1) is likely to be caught by the law as famous brands will be the first to comply. The links displayed in (2a) will change daily, and depending upon the speed the regulator can act, will likely not be caught under a proportionate approach. Likewise (2b) would also result in exposing children to pornographic images – further details on the issues surrounding search engines

are given later in this response. (3) is out of scope of the law as defined in the Online Pornography (Commercial Basis) Regulations 2017, so children will be no more protected than they are today.

A proportionate approach simply does not work even if the regulator has an army of compliance officers.

### **Search Engine Ranking**

Search engines like Google return search results based upon many factors with the obvious aim being that users find what they are looking for, usually on the first page of results. Sites can drop down the list if customers click the link and “bounce” back, i.e. they enter the site then leave, rather than continuing to view pages on the site. As users will usually follow the path of least resistance, age verification will cause bounce rates to increase heavily on compliant sites. This may reduce over time as the public is made aware and more sites comply, but determined teenagers will likely continue searching and clicking links until they find a site which does not require age verification. This behaviour has a very concerning outcome:

If bounce rates increase, then compliant sites will start falling down the ranking on search engines, and conversely non-compliant sites will start climbing higher. This will unfairly penalise compliant sites and give promotion to non-compliant sites, therefore dramatically increasing the risk of children stumbling across pornography. It is therefore essential that search engine owners are involved in this process so they can amend their algorithms to push non-compliant sites down the list, and give compliant sites a higher ranking.

### **Search Engine Image Search**

Search engines return images within the search engine based upon the terms entered. Some of which could be archived or deleted images which are still cached in the search engine. This is a major issue which should be discussed with search engine owners to ensure it does not happen, else stumbling will still occur on quite a large scale. We would therefore expect the BBFC to have mandatory powers to require search engine owners to cooperate with these very important aspects of child protection.

### **Speed of enforcement**

Speed of enforcement is key to both encouraging compliance, and ensuring non-compliant sites are inaccessible.

The Guidance presents some problems in this area:

- Adult sites may try to capitalise by not enabling age verification until they receive their first letter. The Guidance is clear that no enforcement action will take place prior to receiving such a letter. This sends a very poor message to adult site owners, in essence “There is no need to comply until you receive a letter”. This will delay compliance and leave pornographic material open to children.
- There are no timeframes set for compliance within the notification process. Whilst sites should of course be given a reasonable window of opportunity to respond, the entire process from notification to enforcement should be a matter of days, not weeks or months. Mass notification prior to the law going live would greatly help, and the proportionate approach again rears its ugly head here. If compliant sites are disadvantaged it will not only discourage compliance, but also leave children unprotected for much longer.

- The notification process appears lengthy, and it appears that the BBFC wish to encourage compliance through dialogue. However, adult sites could attempt to stall enforcement with empty promises of future compliance to benefit from the additional traffic they would receive whilst non-compliant.
- The Guidance states that when a non-compliant pornographic service becomes compliant, then all enforcement action will cease and notices withdrawn. However, there is nothing mentioned about repeat offenders. A site owner could wait for all the letters, enable age verification to have them withdrawn, and then disable age verification to reset the notification/enforcement timeline. The Guidance should therefore make clear that enforcement will be fast-tracked in cases such as these. The regulator may also wish to consider a penalty for the period of time a site remained non-compliant.

Overall, the speed of enforcement is paramount to the success of the law. The regulator has a duty to ensure that compliant sites are not penalised. If non-compliant sites receive a 30/60/90 day window to comply, they will gain a huge commercial advantage. Anything which discourages compliance to this degree will significantly slow the adoption of age verification and therefore leave children no more protected than they are today.

### **Enforcement Tools**

The list of enforcement tools appears to be sound, the tools are wide-reaching and multifaceted. However, only ISP blocking appears mandatory, all others will be requests. We hope companies assisting in the enforcement process will act responsibly and respond swiftly to such requests as this could add yet another delay to enforcement, leaving non-compliant sites open to minors. Ideally all requests should be switched to mandatory requirements to ensure they are not ignored.

### **Privacy and Security**

There is a raft of misinformation available regarding the security and privacy of age verification systems. The public need to feel confident that their personal data cannot be exposed and their personal browsing habits are incapable of being identified. Whilst there are many supporting statements to this position within the guidance, age verification services and pornography providers must be under no illusion that such protections are mandatory. Some simple changes to certain terms would help achieve this, such as “...*should have regard to* the ICOs guidance” – a somewhat non-binding statement as it currently stands. Additionally, all “good practice” and “recommendations” should be mandatory, not optional, and a ToS/Privacy Policy should not usurp this. If the public do not feel comfortable using age verification systems they may seek to circumvent the law or search for non-compliant sites. Again, this discourages compliance, leaving children unprotected.

We note that a Publicly Available Specification (PAS) 1296 has been recently published by the British Standards Institute, specifically aimed at online age checking. This contains a lot of useful information to assist the regulator and ICO, and we feel incorporating or referencing it within the Guidance would be a useful step for all parties.

### **Assessment of Age Verification Arrangements**

We welcome the assessment of age verification arrangements, but would like to see a “stamp” or “seal of approval” given to providers who have passed, ensuring that the public can easily identify compliant systems and are wary of non-compliant or fake systems. There is a significant danger that fake age verification systems could become rife, they may not even protect adult content, designed

to harvest personal data from a customer via phishing. This could result in a serious problem with identity theft.

We are also concerned that the onus of compliance lies entirely with individual adult sites. If an adult site uses an age verification provider listed as positively assessed on the BBFC's website, then the onus should be on the BBFC to remove such a listing and inform the adult industry if the tool is no longer compliant. Whilst it may be relatively easy for sites to run periodic checks on their age verification arrangements, they may not be able to conduct a deep dive to prove such things as data protection and privacy.

### **Age Verification Methods**

The criteria specified in the Guidance is good, and it achieves the correct balance of ease of use/user friction and robustness. We are hoping that the assessment of age verification arrangements will include individual assessments of each method from different companies, so that no one is left unaware as to whether a method is permitted.

### **Pornographic content definition**

A question discussed often within the adult industry is what level of content can be shown in front of an age verification wall? Whilst the Guidance gives several definitions of what is unacceptable, some examples of what is allowed would be helpful. For example, is topless material classed as "pornographic"?

### **Online Pornography (Commercial Basis) Regulations 2017**

These seem very much designed to carve social media platforms out of scope. If such platforms contain pornographic material, then not requiring them to age verify their users is contradictory to child protection laws. Children are also more likely to stumble across pornographic content on a social media platform.

# Guidance on Age-Verification Arrangements

## Comments on Chapter 2

The assessment and enforcement actions described in chapter 2 are limited to one (first) time assessment. Particularly paragraphs 12 to 15 imply quick remedy of actions against a non-compliant provider without considering previous activities. The BBFC should increase frequency of assessments and severity of enforcement actions for repetitive non-compliance.

Overall, the guidance assigns the responsibility to prove an illicit action to BBFC and the governing bodies, while the Digital Economy Act does not preclude full responsibility of the pornographic content provider, including their responsibility to prove compliance to the law and the guidance. The proposed difference in the philosophy of the implementation will assign the appropriate roles to all parties involved in this sensitive issue; content providers will take all measures to follow the law/guidance, end-users will accept their interest in proving their age and request their interests properly secured, ancillary service providers will take their responsibilities. As an example, the following cases may not be addressed properly by the proposed guidance:

- end-user complaints about improper use of their data; the guidance makes no provision for audited access, making impossible the traceability of the use
- granted access to individual or restricted group minors; content providers may communicate privately to minors non-verified access to their content; the process described gives the content providers enough time to stop, erase any traces and restart the illicit process just after the control by BBFC!

### Comments on Chapter 3

**In Paragraph 9, the guidance states that “the BBFC will normally be able to identify the following in relation to data protection compliance concerns: ... requesting more data than is necessary to confirm age, for example, physical location information”. Even though we agree that accurate physical location information should not be used/collected/processed, we consider that location information related to the country where the user is present during the age-verification process is very important to avoid massive use of simple technological mechanisms by minors to circumvent the envisaged limitations (such as VPN proxies located outside the country).**

**We believe that the guidance should specify that content providers should keep logs of access for a certain period (such as 6 months or a year) and guarantee that BBFC may trace every age-verification to its original source. At the same time, in order to protect privacy, the ability to relate individual access to age-verified information should be limited to BBFC and/or their inspectors. AGEify is currently developing a solution that can satisfy those requirements and we are ready to showcase it whenever needed; we can prove then that those requirements are not fictional, but can be implemented for the benefit of all involved parties.**

# AVSecure Response

AVSecure fully supports the intentions of the Digital Economy Act and its objectives with respect to making the internet safer for under-18s. We agree with the approach taken to date by the BBFC in balancing the needs of protecting children versus the challenges associated with personal privacy of all consumers.

There are significant potential risks to personal privacy arising from requiring consumers to prove that they are over 18 when visiting adult websites. Since consumers may be using personal information to verify their age, the way that is collected, used and managed, is critical to how effectively their privacy is protected. Even variables such as the economic model the verification company adopts, which systems they use and their modes of support, can all impact the consumer's risk profile.

Consumers should be fully aware of the privacy risks associated with each solution. We believe that a large majority of normal internet users lack sufficient technical expertise to understand the risks they may be taking. This is a significant problem as it could lead to consumers unwittingly accepting a higher risk than they would choose if fully informed.

We believe all age verification service providers should have the following core attributes:

1. The business model should be geared towards preservation of privacy and not on making money from data collected.
2. The technical components in the solution should neither collect nor store personal information, unless necessary to protect operational integrity. Required information should be stored in encrypted form without logging, have clear accountable access controls and be deleted at the earliest opportunity.
3. The technical implementation should create a Chinese wall which provides clear separation between the act of age verification and its resultant use when accessing adult content. Ideally this wall should be under the control of the user. Where it is managed by a third party the user should have complete transparency as to its mode of operation.
4. The technical architecture should be such that the service provider and business suppliers are unable to track the internet browsing habits of the consumers. The ability to track consumers' behaviour could, when combined with other external data, de-anonymise them and pose a significant risk to their privacy.

If compromises exist to these core attributes, then risks to consumers arise. Service providers have a duty to implement the highest forms of privacy protection for consumers, given the sensitive nature of the subject matter and the level of technical understanding of the average internet user.

The AVSecure model is designed and developed to use blockchain and in our view demonstrates the gold-standard for privacy preservation of consumers. It has user options



which prevent visibility on any device where it has been used, thereby allowing plausible deniability of use.

- We will offer an Age Verification Card that can be purchased in retail outlets across the UK. Much like buying alcohol, if the consumer clearly looks of age they will not be asked to show any identification. This satisfies points 1 & 2 of the criteria listed above.
- Our architecture is designed specifically to allow the consumer to provide 'proof of age' directly from their browser. This is key. Once the consumer is validated their browser will generate a one-time token, that is passed to the website they are visiting, without any additional external involvement. As a new token is generated at every visit the consumer cannot be tracked. It can be cryptographically proven to have been issued to someone previously validated as over 18 by a trusted source. Neither AVSecure nor the trusted source knows that a token was generated. This lack of need for any external management means that AVSecure's approach satisfies points 3 & 4 above.

Importantly, even if a consumer chooses to age validate using a method that leaves a digital trace they will still benefit from the tracking prevention in the AVSecure browser authentication.

**A key summary of AVSecure's approach is as follows:**

- AVSecure does not retain any personal information that can be tracked back to an individual.
- AVSecure does not track or log a history of a user's browsing behaviour.
- AVSecure does not require a consumer to provide an email address due to the inherent risks of identification if data is compromised.
- AVSecure has no store of data that could be sold for commercial gain.
- AVSecure does not know who its users are.
- In the event of the blockchain being hacked the data retrieved will be a random series of numbers and characters and thus eliminates the possibility of an "Ashley Madison" problem.
- AVSecure is free to industry and has several age verification methods which are free to consumer. This ensures that any business, small or large, can comply with the regulations without cost.
- AVSecure's independence provides merchants with a trusted partner, thereby removing the perceived risks associated with engaging solutions managed by adult industry participants.

## Guidance on Age-Verification Arrangements

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

Yes

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

Yes. However, we would like to see greater emphasis on age verification methods that minimise risks to privacy of individuals. It is our proposition that typical internet users are unaware of the lack of security and privacy associated with internet use. Any new age verification service could collate valuable and highly sensitive data about consumers, which could pose a significant risk to their anonymity. We strongly encourage a grading system of potential age verification providers, that can demonstrate not only pseudonymous but also anonymous methods of validation, which even exclude tracking. The intent is to place all users in a situation where they are fully informed about the choices that they make.

Do you have any comments with regards to Chapter 4?

There is no explicit mention of tracking users across sites. We have a concern that consumers may be unaware of the tracking information they may generate, which in the wrong hands could pose a significant risk to consumer privacy.

The BBFC will refer any comments regarding Chapter 4 to the Information Commissioner's Office for further consideration.

## Draft Guidance on Ancillary Service Providers

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

Yes.

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

Yes



25 Telfords Yard,  
The Highway  
London  
E1W 2BQ

22 April 2018

British Board of Film Classification  
By email.

Dear Sir/Madam,

I am responding to this BBFC consultation on the Digital Economy Act 2017 and the draft guidance on age-verification arrangements and draft guidance on ancillary service providers: -  
<http://www.bbfc.co.uk/about-bbfc/dea-consultation>

## **Introduction.**

Before responding to the questions posed in the consultation I want to stress four points: -

### **1. Opposition to AV: This regime is not a proportionate response**

The proposed BBFC AV regime will do more harm than good and is not a proportionate response to what is a legitimate concern (the legitimate desire to protect young children from explicit adult material).

**Backlash** has sent representatives to previous meetings with the Department for Digital, Culture, Media & Sport (DCMS) and other bodies but we have yet to see any evidence of the creation of a regulatory regime that addresses our concerns. We are so concerned that we have written to the Information Commissioner (IC) asking that body to intervene and provide your office with the instructions needed to ensure a life threatening breach of data does not take place.

The Ashley Madison (AM) breach is well documented, as were the suicides that followed. It is important to also understand the scale of marital breakdown/divorce and wider emotional damage done by that data breach. This article provides some insight into the scale of harm: -

<https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>

I am at pains to emphasise that the scale of harm that will be caused by your proposed AV regime is much greater than occurred following AM. Far more people view pornography than registered with AM. Perhaps as many as 25 million UK citizens will seek to access explicit material in the first year of operation and, over their lifetimes, perhaps two thirds of the UK population will at some point want to view such material.

The number of people being put at risk is unprecedented. The potential scale of harm is unprecedented and so the regulatory regime must be unprecedented in the strength of the protections that are put in place for UK citizens and law abiding consumers.

Healthy people enjoy a range of sexual preferences and their internet searches reflect what many consumers view as their unique desires. But it would be absolutely devastating for most viewers of explicit material if the types of material they had sought or accessed became public knowledge. Many would be distraught if their

sexual desires were to be released publicly and far more people would kill themselves than happened following the AM hack.

It is important that you understand that there will be some malicious hackers who seek to gain access to confidential material to cause embarrassment or to commit fraud. But, in the age of cyberwarfare, where state actors will hack stored data to harm their opponents, it is obvious that cyberattacks will soon be attempted upon the data held on those who access explicit sites. It is entirely foreseeable that foreign operators will soon seek to hack such information simply to hurt the population at large. It won't matter if those hurt are civil servants, MI5 staff, police officers, doctors, nurses, MPs, or those who feel they don't care and have nothing to lose by a hack; all that will matter to an aggressor is that they cause mayhem and significant public alarm.

Under no circumstances should the IC permit BBFC to allow that to happen. It is imperative that AV providers are properly assessed regarding their data security measures and practices to ensure they comply with UK & EU data protection legislation and that the IC ensures consumers are guaranteed absolute protection.

Backlash supports efforts to protect young children from unsuitable material but this AV regime is dangerous and is disproportionate and will do nothing to stop the determined 16 year old from using the number of online tools that are available to access explicit material.

## **2. Financial liability of BBFC and Information Commissioner**

Under Introduction ( 1 ) Para 13 you say: "The BBFC does not accept liability for any loss or damage alleged to result from reliance placed either on its published guidance or any supplementary informal guidance it may give." See: -

[http://www.bbfc.co.uk/sites/default/files/attachments/BBFC\\_Draft\\_Guidance\\_on\\_Age-verification\\_Arrangements\\_March\\_2018.pdf](http://www.bbfc.co.uk/sites/default/files/attachments/BBFC_Draft_Guidance_on_Age-verification_Arrangements_March_2018.pdf)

I need to emphasise now that when a breach of confidential data does take place, if the BBFC's regime is in part to blame for that breach, this organisation will explore with others the potential to seek financial compensation from BBFC for the harm that is done. The statement that you do not accept liability is designed to be misleading and misinform the public on their legal rights, and you must remove it from all future material that you publish.

## **3. Extreme pornography laws**

This public consultation and the proposed regime are being publicised as being in connection with AV; but it is only upon closer inspection that readers will see that the regime is being used as a tool to extend the reach of CJIA 2008 to block access to extreme pornography. The public consultation process should not be misused in this way. If a public body wishes to extend the way in which CJIA 2008 is regulated and enforced, then a public consultation on that should be advertised in the proper way.

## **4. Infringement to the right of freedom of expression and speech**

There are many negatives associated with the proposed AV regime but I wish to express concern about the wider chilling effect this will have upon freedom of expression and speech. The blocking powers of the BBFC represent derogation to the free expression right of both consumers and site operators. There will be thousands of publishers who do not generally provide sexually explicit material for financial gain but who might occasionally stray into territory that could be seen as being for purposes of arousal. Even if that is not the intention of the artist/publisher, many will conclude that they must self-censor in order to avoid the financial and administrative burden of installing an AV system.

I will add that Backlash has previously represented a number of small, ethical producers of explicit material who promote the acceptance of non-heteronormative sexualities, some of whom do so in an artistic and

imaginative way. Many of these small ethical producers will feel squeezed out, further diminishing the right of UK citizens to freedom of thought and expression.

**Response to the paragraphs 2 – 4 of the draft guidance document.**

[http://www.bbfc.co.uk/sites/default/files/attachments/BBFC\\_Draft\\_Guidance\\_on\\_Age-verification\\_Arrangements\\_March\\_2018.pdf](http://www.bbfc.co.uk/sites/default/files/attachments/BBFC_Draft_Guidance_on_Age-verification_Arrangements_March_2018.pdf)

**2.2:** refers to how BBFC will “discharge the functions”. I gather that the BBFC will be given two additional members of staff to handle hundreds of millions of adult sites. If this is correct it must surely be impossible for the BBFC to handle this task in an objective, consistent and transparent manner. Surely very large numbers of omissions and errors will occur?

**2.4:** refers to the commercial services which the BBFC will investigate. Backlash has represented many sex workers and we are therefore concerned to establish the effect the AV regime will have upon the way sex workers advertise their services. Will independent sex workers advertising online be considered to be making pornographic material available for the purposes of the Act?

The guidance says the material has to be “produced solely or principally for the purposes of sexual arousal” but sex workers advertise to persuade clients to book services. Their primary objective is to meet clients, not to cause sexual arousal. It should also be noted that sex workers are not receiving any payment for making advertising materials available. Sex workers receive payment or benefit from providing sexual services, not from advertising service. A sex worker might place an advertisement but not get any bookings. Are they still obliged to AV?

If sex worker advertising is considered to be “making pornographic material available on a commercial basis” then this will cause immense harm. Consenting adult sex workers will be prevented from posting their own advertising, screening and vetting their own clients, and choosing what services they offer, if they are obliged to lock their adverts behind AV tools. The consequences will be that sex workers are instead obliged to go back to working for exploitative bosses or on the street because they cannot effectively advertise online. This will put them at greater risk of violence, exploitation and abuse.

I put it to you that the inclusion of sex workers within the AV regime would be disproportionate, life threatening and open to Judicial Review.

I also wish to express concern about the impact upon sex bloggers, educators and those who provide advice to sexual minorities. Backlash has bitter experience of legislation being misused to attack sexual minorities (CJIA 2008) and so we appeal to you to make your guidance clear that those who provide advice, commentate upon or seek to educate upon sexual matters will be exempt from the AV regime. It is entirely foreseeable that those who are vehemently opposed to sexual minorities will seek to use the AV regime to close down sites they disapprove of. So it is essential that those who publish material designed to educate, inform and reassure must be assured freedom from the AV regime and not be put under pressure to self-censor what are often essential services.

**2.5:** refers to the “priority of protection”. Our expectation is that determined, internet savvy, 16-18 years olds (above the age of consent) will ignore the AV regime and access material using Tor browsers and VPNs. It has already been put to the BBFC that this will be the case but the priority of protection paragraph makes no reference to this fact. Before proceeding with the AV regime I ask that the BBFC advise government ministers of the evidence that the desired outcome of the regime cannot be fulfilled.

I note that you have identified a number of sites that young adults most wish to access. Please state which sites they are so that we can better inform those we represent on the likely impacts of the AV regime.

I also express concern that the BBFC is straying into the area of responsibility of the Internet Watch Foundation. BBFC have no statutory authority to duplicate efforts of IWF, nor the Police, and this is an inefficient use of public resources.

**2.8:** notes the opportunity for the person or people concerned to make representations to the BBFC. However, these representations must then be taken into account in the decision made. The BBFC must be able to justify the recommended action based on proportionality and balance; taking into account the interests and safety of all stakeholders.

**2.9:** discusses the infraction of “making extreme pornographic material available on the internet to persons in the UK”. This is an offence covered by the Criminal Justice and Immigration Act (2008) and the Obscene Publications Act (1959). This is outside of the remit of age verification and suggests a further will to police sexual freedom beyond the notion of protecting young people.

**2.16:** Backlash has represented small independent producers of pornography who trade under a pseudonym but are self employed for tax purposes and often trade from their home addresses. We have seen instances where the media has published home addresses in order to hound minorities and so are anxious to ensure that you do not “out” publishers by displaying full names and personal home addresses.

**3.1:** You state that providers “must adopt effective and robust age verification arrangements” but you do not use the same strength of language when referring to the AV tools. At **3.7** you say “the BBFC recommends that age verification providers adopt good practice in the design and implementation of their solutions.” This is wholly inadequate and we call upon the BBFC to discuss with the IC’s office the standards that it would expect from operators that hold data that, if breached, would lead to loss of life.

I cannot emphasise strongly enough that the BBFC is not taking data protection seriously and has not shown an appreciation of the scale of harm that its lax guidelines represent. I call upon the BBFC to require that AV providers guarantee totally secure services that cannot be hacked. If the BBFC does not use powerful language that sets the standards required of providers then it will be complicit in the potentially catastrophic effects that follow.

**3.2:** lists a number of ways in which age verification can be carried out using documents. However, these documents will not be accessible for everyone, whether this is due to financial difficulties, disability or citizenship. A method of making sure age verification can be achieved by any eligible party regardless of these is necessary to prevent people from being shut out from material they wish to access and further perpetuating social and sexual inequalities.

**3.4:** encourages “the use of mechanisms which confirm age but not identity”, which is contrary to the methods listed in 3.2, all of which can be tied to a person’s personal information. The BBFC must explain clearly what its intentions and standards are.

I must also express concern regarding the company MindGeek and its AgeID product. Very many consumers will use this product due to the popularity of the tube sites MindGeek hosts. MindGeek’s main source of revenue is advertising, and therefore such a company would have significant interest in storing and using individual user data for profit. Given that this company is based abroad and will attract very significant UK traffic, I ask that the BBFC explains what checks it has already undertaken to ensure that the company will comply with the AV regime proposed? UK consumers have every right to expect the BBFC to have conducted thorough research before implementing the new regime.

**3.7:** acknowledges that AV providers should “provide ease of use for end users”. Given that the enjoyment of a healthy sex life, including accessing explicit adult material, is a lawful activity and one that government has not set out to ban, “ease of use” is what the BBFC should ensure without jeopardising data security. But it is surely unrealistic and unworkable to expect users to age-verify on each visit, which might be several times in one day. The alternative that users will be forced to use will be websites that maintain databases of age verified users, permitting them to login using a password or personal ID number, which creates a real risk of this very personal sensitive data being leaked or hacked. The retention of this data creates a conflation of identifying details such as username and password, with information about what pornography sites and which specialist areas of those

sites users have visited. The BBFC is creating this new risk while taking no responsibility for keeping user data safe.

**3.7 and 3.8** use the word "recommends". This makes both of these clauses non-binding and cannot guarantee protection for AV users. This is a recurring theme throughout the document and is a source of grave concern. There is no obligation for AV providers to ensure any greater level of protection to their users than that specified within the General Data Protection Regulations, which are wholly inadequate for such a sensitive, personal and private matter such as one's sexuality.

**3.9:** fails to include the necessity to ensure adequate protection against breaches of privacy. I have referred to the Ashley Madison (AM) incident above, which led to multiple suicides, and the BBFC must not allow this scale of harm to be repeated. It is imperative that AV providers are assessed regarding their data security measures and practices to avoid future leaks or hacks.

**3.10:** is an inadequate response to the scale of the threat. It is not sufficient to refer non-compliant providers to the IC after failures have been discovered. The BBFC should devise a robust regime that protects users from the outset, not respond to catastrophic failures after the event.

**4.3:** says that "Age verification services and online pornography providers **should** have **regard** to the ICO's guidance on data protection and specifically data minimisation, security and data protection by design and default." This language is not sufficiently robust and needs to be mandatory.

**4.4:** is a wish list that does not do enough to set the absolute standards that AV providers must adhere to. It is entirely foreseeable that during an AV process a number of sites will use a tick box system to both provide AV and seek permission to provide other services. Many sites will have clauses that permit them to change their terms after an initial authority has been given. The vast majority of users are not sufficiently aware of the risks they face and I put it to the BBFC that you must not compound those risks and you must not enable disreputable firms, often based abroad, to exploit large numbers of UK users.

**4.5:** refers to GDPR, stating that "have a general obligation to implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities". Again this woefully inadequate language reflects a lack of understanding of the scale of the threat to life associated with data breaches that will occur with the AV regime as currently designed. It is absolutely essential that the BBFC takes responsibility for ensuring the safety and security of AV providers. Leaving this to chance is a dereliction of duty and a breach of your duty of care.

If the BBFC's failure to set the required standards is due to poor guidance from the IC or if it is due to a poor appreciation of the scale of the risks by government ministers then the BBFC has a duty to explain that now. If a regulatory regime has been designed that has inherent flaws, whereby the BBFC cannot do anything about the safety of the AV platforms, then it has a duty to ensure everyone knows that now. It is not enough to warn government ministers that serious breaches of data will occur. It is essential that the BBFC is honest with the public and ensures that both the public and the media is informed that the systems are unworkably, insecure and data breaches are guaranteed to occur. You have a duty of care to ensure the public understands the scale of risk people will be taking under your AV regime.

Response to the paragraphs 1 – 4 of the draft guidance document.

[http://www.bbfc.co.uk/sites/default/files/attachments/BBFC\\_Draft\\_Guidance\\_on\\_Ancillary\\_Service\\_Providers\\_March2018.pdf](http://www.bbfc.co.uk/sites/default/files/attachments/BBFC_Draft_Guidance_on_Ancillary_Service_Providers_March2018.pdf)

The comments I have made on the first paper are equally relevant to this paper and I will make these additional comments.

**1.11:** refers to occasional research to check the effectiveness of the AV regime. I call upon the BBFC to undertake thorough research before initiating the regime and to guarantee that it will report once every three months on the effectiveness of the AV products. A robust research and reporting system is essential because it

is very likely that serious data breaches will occur which will have huge adverse implications for large numbers of people.

2.2: says that the BBFC will it will act in an “objective, consistent and transparent manner”. The test of that will be how the BBFC now responds to my comments above on the draft guidance relating to the age verification arrangements.

Yours faithfully,

J N Fuller  
Chair: Backlash



**Barnardo's response to the BBFC Guidance on Age-verification  
Arrangements  
Digital Economy Act – Part 3 Online Pornography**

1 May 2018

---

Barnardo's works directly with vulnerable children, young people, parents and carers in communities around the UK. From this experience we have gathered evidence about negative experiences of the internet, including for children and young people who have been sexually exploited. Over the last few years we have seen the impact of the internet in the way perpetrators can have access to young people to groom and abuse them.<sup>1</sup> This abuse can happen both offline, when the child meets the abuser after communicating online, and online, through non-contact sexual abuse and the sharing of images. The internet has allowed abusers to take on false personas and become "friends" with young people, earning their trust and luring them into a false sense of security, which creates conditions in which abuse to take place easily. It has also enabled new forms of abuse to develop, such as non-contact abuse.

Barnardo's also knows from our frontline work that children and young people often view pornography, including extreme pornography, online. Not all children are severely affected by this, but in some cases it can affect a young person's sexual development, and more widely it is felt that this could be changing young people's understanding of sex and relationships. In some cases, the internet is where children first 'learn' about sex, meaning they can attempt to imitate what they have viewed online, which may be extreme and violent. The recent Parliamentary Inquiry into Harmful Sexual Behaviour (HSB), which Barnardo's provided the Secretariat for, highlighted this as a matter of concern in its concluding report *Now I Know It Was Wrong*.<sup>2</sup>

---

<sup>1</sup> Palmer, T (2015) *Digital Dangers: the impact of technology on the sexual abuse and exploitation of young people* [http://www.barnardos.org.uk/onlineshop/pdf/digital\\_dangers\\_report.pdf](http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf)

<sup>2</sup> *Now I Know It Was Wrong* (2015) [https://www.barnardos.org.uk/now\\_i\\_know\\_it\\_was\\_wrong.pdf](https://www.barnardos.org.uk/now_i_know_it_was_wrong.pdf)

Barnardo's welcomes the introduction of the Digital Economy Act, 2017 and the age-verification for commercial pornographic sites that the Act introduced. While we acknowledge that age-verification will not prevent all children and young people accessing pornography, it will go some way to preventing the easy access to pornography and to incidences where younger children stumble onto pornographic websites. It is also recognised that children and young people are able to view pornographic content on social media and websites that are not considered commercial. However, age-verification is a start to a process that should ensure that the laws that are applicable in the 'real' world are also applicable to the online world.

Barnardo's are members of the Children's Charities Coalition on Internet Safety and support the consultation response that has been submitted on behalf of the Coalition.

### **BBFC Guidance**

The guidance that the BBFC proposes defines how the age-verification process is set out and how the BBFC will oversee age-verification.

In relation to part 2 we recommend that:

- In Chapter 2, paragraph 5, the guidance outlines ways that the BBFC will decide on which websites to investigate. Included in this list should be the ability for members of the public and professionals to refer sites that they believe are being accessed by under 18s.
- In line with the above, there is a need for regular revision and review of the guidance to ensure that the guidance is working and that loopholes are closed as technology changes.
- On page 7, the document refers to 'enforcement' notices but does not include what enforcement means and what the penalties are if a site is found to have no age-verification. While the repercussions may be included in the Digital Economy Act it would be useful to include it here. This document would then contain all necessary information on age verification.

In Chapter 3 the guidance sets out the age-verification standards.

- The BBFC should regularly review and explore which age-verification providers are being used by the sites so to ensure they are using adequate age-verification standards, which would preferably require two factor authentication.

1 May 2018

# Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers

This response is written on behalf of Brass Horn Communications; a UK ISP / ASP.

## Guidance on Age-Verification Arrangements

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

We welcome point 16 regarding the publishing of notices and appeals but would suggest that further transparency is needed.

In regards to point 1 the BBFC should publish worked examples of the sort of websites that would fall foul of s. 3(a) / s. 3 (b) / s.3 (c) of the Online Pornography Commercial Basis Regulations 2017. e.g. will the BBFC block a website that simply directs visitors on how to access adult material (*e.g. "here is the link to AgeID, you will need a credit card and your identity details" through to "here is how you gain access to our Adults only website"*).

It would be unacceptable for the BBFC to order a block of both `howtoaccessmyadultwebsite.tld` as well as `myadultwebsite.tld` if the former does not contain any adult material itself. This will prevent a repeat of the issues we saw with Nominet's "commercial basis" changes to WHOIS privacy<sup>1</sup>.

Once a decision has been made regarding which course of action to take regarding any given website the BBFC should publish the decision (*including the reasons as to how the decision was reached*) **before** the website is ordered to be blocked or ASPs / payment providers are sent a notice. This is important to ensure that the BBFC remains accountable and so that the wider community can keep track of current levels of UK Internet censorship.

If the BBFC has decided that a website should be investigated because it is "frequently visited by children" the evidence to support this statement should be published.

Child protection concerns should be reported to the IWF or escalated to NCA CEOP – these organisations are far better equipped to deal with such situations.

All notices, as discussed in section 9, should be published to ensure transparency and to ensure that the BBFC is using language commensurate with their powers – all too often we see the Police attempt to misrepresent s.29 of the Data Protection Act when communicating with ISPs.

As both an ASP and ISP we have moved to ensure we have no information to share under s.18 DEA 2017 nor any information to act upon under s.23 DEA – however this does beg the question as to how s.18 of the Digital Economy Act can balance with the protections afforded by the Data Protection Act 1998 and upcoming GDPR / Data Protection Bill. The Digital Economy Act does not require an ASP respond to an s.18 notice.

---

<sup>1</sup> <https://www.theguardian.com/technology/2014/jun/11/nominet-new-rules-uk-domain-end-privacy>

In relation to point 13 – how will the BBFC check the website is now compliant if they have ordered it to be blocked? Will the BBFC be utilising a VPN or other such circumvention method?

As to point 14, will the BBFC specify a time limit as to when service must be restored or blocks be removed by those notified? The BBFC should publish a notice stating when a website has become compliant so that the delay before service is restored can be independently measured.

### **Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?**

No.

The BBFC should mandate that compliant solutions put user privacy ahead of any other consideration.

Age verification providers should be prohibited from “profiling” those who have had to prove their ages – when a user has successfully proved their age to the AVP no identifying token should be returned to the website(s) and any token should change on each verification to prevent linking a user across websites or between visits.

Data protection and user privacy should be foundational standards despite the lack of obligation under section 14(1) of the Digital Economy Act.

### **Do you have any comments with regards to Chapter 4?**

Please see notes above

## **Draft Guidance on Ancillary Service Providers**

### **Do you agree with the BBFC's Approach as set out in Chapter 2?**

Whilst Chapter 2 lays out the proportionate steps the BBFC intends to follow and clarifies in section 6 that it intends to “encourage” compliance it is unacceptable that a modern society would allow censorship of the Internet.

Furthermore, sections 13 – 15 are insufficient – in the event that content has been misclassified or that a legitimate business is at risk the BBFC should insist on an immediate re-instatement of service / removal of blocks.

As discussed earlier if there is no *requirement* to restore service then it is unlikely that the ASPs / ISPs / Payment Providers that complied with the original notice will prioritise the reinstatement of a user.

### **Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?**

No.

Putting aside that ASPs have no obligation to assist in the UK Government’s Internet censorship the classes are far too broad and could be used to critically damage the business of a website operator.

## **Online platforms, including social media, on which a non-compliant person has a presence**

This could apply to anything connected to the Internet – a users Spotify account, their eBay account or anything else. Simply having a presence should not be sufficient grounds for issuing a notice under section 21 (1).

## **Search engines which facilitate access to non-compliant services**

The BBFC can no more insist that a search engine remove a website listing that has been algorithmically matched to a given search term than demand a Library or academic journals remove mentions from an index or footnotes etc.

That the website exists and matches a given search term is a fact. If the website is non-compliant and blocked by ISPs then it doesn't matter if someone attempts to follow the link from the search engine.

## **Providers of IT services to a non-compliant person**

Again, this is too broad. This definition would allow the BBFC to ask PC repair businesses, email providers, document processing providers etc to withdraw services from the business owner. The intention of the Act is to prevent access to **websites** with adult material not to cripple business owners.

**18 April 2018****Written evidence submitted by the British Standards Institution to the British Board of Film Classification on the draft Guidance on Age-Verification Arrangements consultation****Introduction**

1. BSI (the British Standards Institution) is making this submission as the National Standards Body for the United Kingdom. BSI has a public function in support of the UK economy. We bring together stakeholders (including government, industry and consumers) and facilitate the development of “what good looks like”.
2. Voluntary standards offer a flexible, adaptive and collaborative alternative to regulation by providing common languages, terminologies, guidelines and good practice developed by and for stakeholders. **As the UK’s National Standards Body, BSI operates in accordance with an MOU with the UK Government.** Our robust standards development process requires open and full consultation with stakeholders to build consensus based outcomes. This gives standards the legitimacy and degree of market acceptance to be used for public policy purposes.
3. **BSI welcomes the British Board of Film Classification’s consultation on age verification and wishes to highlight a recently published code of practice PAS 1296 that can support the BBFC in its role as an age-verification regulator.** BSI would encourage BBFC make use of this industry led publication by referencing PAS 1296 in future age-verification good practice approaches.

**How standards can support regulation**

4. **As the UK’s National Standards Body, BSI’s standards offer an alternative to regulation that can protect consumers and business at the same time as helping businesses to innovate.** While regulation may be required to correct a market failure or to address an urgent consumer protection issue, standards offer a market led opportunity that may provide better and more flexible solutions.
5. BSI is independent of any one stakeholder interest; our standards development process requires the involvement of all relevant stakeholders (including consumers, businesses and government) along with an open public consultation process. This provides the credibility for standards to be used as an alternative to regulation, to support regulation or to demonstrate compliance with **regulation. BSI’s standards offer the opportunity to achieve government’s policy objectives and provide the flexibility not afforded by the regulatory process.**
6. One route to developing standards that is particularly suited to emerging areas is a Publicly Available Specification (PAS). A PAS uses a fast-track process to develop standards that can provide the base documents for full British, European or International (ISO/IEC) Standards. PAS documents can be funded by industry, trade associations or government departments and are commonly developed with the intention of being global in scope and application.

**Age verification standard**

7. BSI has, for the last two years, been working with the Digital Policy Alliance (DPA), a group of industry technology specialists and key digital stakeholders chaired by The Earl of Erroll, to

devise a PAS that gives recommendations for a framework for the provision and use of online age check services.

8. *PAS 1296:2018 Online age checking – Provision and use of online age check services* is written to assist those businesses that are mandated to comply with legal requirements to conduct age checks. This includes, for example, checking the age of those:
  - a) buying age-restricted merchandise online (e.g. e-liquids (nicotine), adult materials, dangerous goods);
  - b) accessing online content (e.g. streaming media, adult content);
  - c) using online services (e.g. dating services, gaming or gambling websites);
  - d) enabling access to online age-gated material and services (e.g. education for minors and health for seniors).
9. As a result of an industry led approach, the PAS gives clear guidance on a best practice solution to prevent online age restricted products and services from being accessed by inappropriate users. The PAS provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the solution that will meet a business's specific regulatory compliance needs.
10. This code of practice aligns to the Digital Economy Act Part 3 and can be used as a template for future age verification activities. We would encourage BBFC to provide reference to PAS 1296:2018 in future guidance documentation for adult product and services providers, age check providers, facilitators and auditors.
11. If you would like more detail on the development of PAS 1296:2018 or to request a copy of the code of practice please do not hesitate to contact us on at the address below.

## **Background on BSI**

**BSI is the UK's** National Standards Body, incorporated by Royal Charter and responsible independently for preparing British Standards and related publications and for coordinating the input of UK experts to European and international standards committees. BSI has over 115 years of experience in serving the interest of a wide range of stakeholders including government, business and society.

BSI represents the UK view on standards in Europe (via the European Standards Organizations CEN and CENELEC) and internationally (via ISO and IEC). BSI has a globally recognized reputation for independence, integrity and innovation ensuring standards are useful, relevant and authoritative.

BSI is responsible for maintaining the integrity of the national standards-making system not only for the benefit of UK industry and society but also to ensure that standards developed by UK experts meet international expectations of open consultation, stakeholder involvement and market relevance.

British Standards and UK implementations of CEN/CENELEC or ISO/IEC standards are all documents defining best practice, established by consensus. Each standard is kept current through a process of maintenance and review whereby it is updated, revised or withdrawn as necessary.

Standards are designed to set out clear and unambiguous provisions and objectives. Although standards are voluntary and separate from legal and regulatory systems, they can be used to support or complement legislation.

Standards are developed when there is a defined market need through consultation with stakeholders and a rigorous development process. National committee members represent their communities in order to develop standards and related documents. They include representatives from a range of bodies, including government, business, consumers, academic institutions, social interests, regulators and trade unions.



...making excellence a habit.™

### **Further Information**

BSI would be pleased to provide further information or to discuss the content of this submission with the Committee. For further information please contact:

Steve Brunige  
Head of Government & Industry Engagement  
British Standards Institution  
Email: [steve.brunige@bsigroup.com](mailto:steve.brunige@bsigroup.com)  
Tel: 020 8996 7517



## BRITISH BOARD OF FILM CLASSIFICATION

### DEA Consultation

Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers

### Response by the Campaign Against Censorship

The Campaign Against Censorship (CAC) is a voluntary organisation which supports and defends freedom of expression and opposes restrictions on its exercise. For further information please see the website at [www.dlas.org.uk](http://www.dlas.org.uk).

### Guidance on Age-Verification Arrangements

#### Chapter 2

#### Paragraph 2

The Campaign is not satisfied that control of access to sexually explicit material as imposed by Part 3 of the Digital Economy Act 2017 is either absolutely necessary or possible. Obviously young children should not have access to material so unsuitable for their age group but the same does not apply to people much over the age of puberty, let alone the age of consent. (It seems a pity that there is no such thing as 15 certificate online.) However, we recognise that the BBFC is not responsible for the legislation but only for enforcing it.

It is, of course, impossible to prevent people over 18 sharing material with people below the designated age limit.

#### Paragraph 4

“which services” – this means that not all services that provide online pornographic material on a commercial basis will be investigated. It would be interesting to know which services are to be exempt from the BBFC’s attentions and why those particular services have been chosen. Surely legislation should apply equally to all those likely to be affected by it?

#### Paragraph 5

“most frequently visited”, “have attracted media or social media attention” – the BBFC appears to be unaware that this information may be manipulated.

In the past, the BBFC has shown itself resistant to hostile media campaigns where film or video were concerned. The same values should apply to online services.

#### Paragraph 11

“links”, “search engine results”, “visitor numbers” – please see the first sentence of the response to paragraph 5.

## Chapter 3

### Paragraphs 2 and 8

The Campaign wishes to emphasise strongly that not everyone over 18 possesses or can use a credit card, passport, driving licence or even mobile phone. The BBFC should insist, not merely recommend, that providers do not exclude people who are poor, disabled or both from their services.

No other comment on Chapter 3.

## Chapter 4

Privacy issues fall outside the Campaign's remit. No comments on Chapter 4.

## Guidance on Ancillary Service Providers

### Chapter 2

This is a duplicate of Chapter 2 of the Guidance on Age-Verification Arrangements. Please see the Campaign's comments on paragraphs 2, 4, 5 and 11 of that chapter.

### Chapter 3

#### Paragraphs 3 and 4

The Campaign notes that the list of classes of ancillary service provider has been compiled to include as many situations as possible and is not exhaustive. The objective appears to be to trap as many people and firms as possible in the legislation and hence to make access to sexually explicit material more difficult even for those theoretically of an age to view it.

The Campaign shares the concerns of other organisations which have suggested that once a system of controls on internet access is in place it can be extended from one category of content (sexual material) to others perceived as socially or politically undesirable by the government of the day.

Response ends.

Mary Hayward (Hon. Secretary, CAC) 19th April, 2018.

# CHILDNET

Hi,

Apologies, as I have been unable to respond until now. However, I am hoping that perhaps there is some way you can incorporate my supportive words for the BBFC's approach in this area.

The BBFC approach is encapsulating what we want to see - carry over the same protections that we afford children in the offline world, to protect them from accessing pornography, to the online world. We are certain of the value of taking this step, as research has shown us that online pornography is the top issue that bothers children online, as well as the high proportion of young people who have come across online pornography by accident, so they are exposed to this content rather than access it. The BBFC approach is an important one in responding to this, taking a practical and proportionate approach, focussing on child protection.

Do let me know if you have any questions.

All the best,

Will

## Guidance on Age-Verification Arrangements

- Do you agree with the BBFC's Approach as set out in Chapter 2? Yes
- Do you agree with the BBFC's Age-verification Standards set out in Chapter 3? Yes
- Do you have any comments with regards to Chapter 4? no

The BBFC will refer any comments regarding Chapter 4 to the Information Commissioner's Office for further consideration.

## Draft Guidance on Ancillary Service Providers

- Do you agree with the BBFC's Approach as set out in Chapter 2? Yes
- Do you agree with the classes of Ancillary Service Provider set out in Chapter 3? Yes

**Will Gardner**

**Chief Executive Officer**

Childnet International

Studio 14, Brockley Cross Business Centre, 96 Endwell Road, London, SE4 2PD

e: [will@childnet.com](mailto:will@childnet.com)

t: 020 7639 6967

 Childnet International

 @Childnet



**children's charities' coalition on internet safety**

***Digital Economy Act, 2017  
response to the BBFC's public consultation***

CHIS was formed in 1999. In our first “Digital Manifesto”, published ahead of the 2001 General Election, we alluded to the problematic nature of children’s access to pornography on the internet. It appeared in all the Manifestos CHIS published ahead of each subsequent General Election. Our successful lobbying around the Gambling Act, 2005, saw the introduction of an age verification requirement in respect of gambling web sites and this helped sustain us in our belief that, despite widespread protestations to the contrary, requiring age verification for pornography sites was an achievable goal. It was a matter of political will. We continued to advocate for it.

Against that background CHIS is delighted to see the relevant provisions of the Digital Economy Act, 2017 are moving closer to becoming operational.

CHIS has never seen age verification in respect of pornography sites as an alternative to children and young people receiving age appropriate advice and guidance about sex and relationships, both at home and at school or indeed via thoughtfully prepared educational resources available online.

However, age verification is an important complementary component. Inter alia, it helps show children that, as with alcohol, gambling and similar, a serious effort is being made to ensure the laws mean something and that the advice being given is not something to which grown- ups only pay lip service and is not truly meant to be taken seriously.

The Digital Economy Act, 2017 therefore helps bring about a closer alignment of the norms and expectations which apply in the physical world with those which apply in the virtual one. We don’t have rules which apply here and none or others which apply there.

Below are our responses to the questions posed in the draft ***Guidance on Age-verification Arrangements*** and the specific questions posed in relation to the draft.

- Do you agree with the BBFC's Approach as set out in Chapter 2?
  - While all commercial sites are caught by the Act CHIS appreciates that the principle of proportionality requires the BBFC to focus on sites that are attracting significant

amounts of traffic, particularly where there is evidence that the sites are likely to or are in fact attracting the attention of children.

- It is self-evident that in a fast-moving environment such as the internet new sites and Apps can emerge and attract traffic very rapidly. It will be vitally important for the BBFC to find a way to track and discover new sites and Apps to ensure they do not operate smash and grab raids on the attention of large numbers of children.
  - It will also be vital for the BBFC to develop ways of monitoring the overall effectiveness of the legislation and develop ways of determining whether successful circumvention strategies emerge at scale.
  - It is clear there is likely to be a need for regular revision and review of the guidance to ensure it is working satisfactorily and loopholes are closed as technology changes.
  - Subject to our earlier comment about needing to keep up with technological change, the enforcement tools currently at the disposal of the BBFC seem tailored to the needs of the task in hand.
- Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?
    - Clearly the most important aspect of an age verification standard is that it is seen to work to keep under 18s out of the site i.e. that there are no ways to obtain an ID which suggests you have been verified as being over 18 when, in fact you are not. This would be a particularly unwelcome circumvention strategy.
  - Do you have any comments with regards to Chapter 4?
    - The principle of data minimization is of paramount importance.
    - While it may be going too far to say there ought to be an outright ban on pornography publishers also having any sort of links with businesses that perform or provide age verification services, the perception that such links exist may harm public confidence in the system as a whole.
    - If we are right about that the ICO may need to consider what extra steps need to be taken to shore up or maintain a high degree of confidence in the integrity of AV.
    - Where there are links between AV providers and pornography publishers the publishers should not be allowed to limit access only to those people who have used an associated AV solution. That is an unacceptable restrictive practice and it will also undermine confidence in the systems being used.
    - CHIS has grave reservations about accepting any age verification solution which relies solely on the possession of a credit card. Two factor authentication ought to be declared as a minimum requirement, as it commonly is in several other areas where security is important. This is in part because of the simple fact that credit cards are often left lying around in family homes.
    - In addition certain classes of online payments cards may use the payments networks of established, well known providers but in circumstances where the apparent credit

card's identifying numbers do not allow the age verification provider to determine whether it is a genuine credit card that has been issued to an adult or it has been bought for cash, typically in a retail or other outlet where there is no age checking.

- Both the ICO and the BBFC should disallow any card or other payment mechanism that can be acquired for cash or can be acquired in any other way that is not routinely associated with prior robust AV.

In respect of the draft ***Guidance on Ancillary Service*** providers CHIS agrees with the approach outlined in Section Two.

Save in one respect, CHIS agrees that in Section Three the BBFC has accurately identified the principal classes of ancillary service providers.

It is difficult to predict how the technology might change in the coming period consequently, as mentioned in relation to the previous consultation document, the BBFC will need to be alert to developments which may alter online patterns of behaviour. It will need to be sufficiently nimble to be able to address developments in a timely way.

CHIS believes that in an increasingly "App-centric" internet the role of the App Stores may need to receive greater scrutiny. Here is where it is relevant to mention our one reservation. App Stores are not specifically referred to in paragraph 3.3.

If App Stores are not caught by 3.3 (a) or 3.3 (e) it may therefore be necessary to revisit this should evidence emerge that Apps are providing a significant circumvention route.

App Stores are major gatekeepers, they profit from their role as gatekeepers, the fact that an App is available through them may imply it reaches certain ethical and other standards, consequently it may be right to insist that App Stores take greater responsibility for ensuring that any Apps they allow on to their platform are not subverting the policy of the Digital Economy Act, 2017.

---000---

22<sup>nd</sup> April 2018

John Carr OBE  
Secretary  
Children's Charities' Coalition on Internet Safety  
10, Great Queen Street  
London WC2B 5DD

[www.chis.org.uk](http://www.chis.org.uk)

## Consultation on Age Verification Guidance from BBFC

### Draft guidance on Age Verification

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

Yes. The CCO welcomes the decision to implement age verification for pornography websites in the UK. The Commissioner feels that this is an important step to meaningfully ensuring that children are safeguarded from inappropriate content online. The CCO's joint report on the impact of online pornography on children and young people in 2016 reflected the view that children felt that age verification could potentially be a positive step forward.<sup>1</sup>

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

We agree that age verification should be robust and requires more scrutiny by the provider than some current systems in place, such as check box confirmation that the user is over eighteen. The CCO recognises the concerns raised by NGOs and members of the public regarding privacy and data collection. However, the CCO is satisfied that technology exists to enable age verification without the collection and retention of personal data.

Do you have any comments with regards to Chapter 4?

Yes. We agree. It is clear that the BBFC has strategies in place to foster a close working relationship with the Information Commissioner's Office (ICO) to ensure that data protection and security is a key point of consideration with the implementation of age verification.

### Draft Guidance on Ancillary Service Providers

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

Yes, with caveats. The BBFC's approach will likely lead to age verification becoming an effective system for preventing children and young people from accessing pornographic websites directly from links via ASPs. There is a concerning gap in the effectiveness of age verification because of the accessibility and the availability of pornographic content on social media websites and search engines such as Google Image Search, Instagram and Twitter. Further, the CCO would expect ASPs to explore and come up with approaches to protect younger users from accessing pornographic content hosted on their sites. In the absence of legislation, it is their responsibility to ensure that they promote healthy and safe spaces for young people online. This is in line with previous reports and statements the CCO has made regarding children's digital lives and the corporate responsibility of social media companies towards their younger users.

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

Yes, with caveats. The CCO agrees with the approach that the ancillary service providers should monitor what can be found on their sites, and have a responsibility to block linked websites that do not comply with age verification. It is important that the definition of an ASP continually be monitored and reflected upon, and updated were new sites to be created and used for accessing pornography online. Further, this should be updated to consider developments in technology such as virtual reality.

---

<sup>1</sup> <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/MDX-NSPCC-OCC-Online-Pornography-Report.pdf> p.61.

## Consultation on draft Age Verification Arrangements March 2018

DEA-consultation@bbfc.co.uk

FIRSTLY... I do not believe there is a need to introduce a 3rd party verification option with the data and censorship concerns this comes with. As a country we already have perfectly adequate 'parental controls' structure in place via all internet providers be they mobile or landline/cable which will control access to not only websites but all other graphic imagery on Twitter, Tumblr and other social media platforms too. Of which all accounts are homeowners and therefore over 18 and capable of restricting adult content should they wish. All public wifi systems have an automatic block on adult content and do not represent a threat. Therefore why do we need a new age verification system which is far more limited than the systems already in place?

SECONDLY... I do not understand why a 'blanket wide' approach is being proposed. As a responsible business specialising in the producing 'beautiful erotica', with no explicit sex scenes published to non paying visitors, I do not understand why my business should be placed in the same category as the likes of Brazzers, RedTube, MyDirtHobby etc who all show extreme and frankly 'unacceptable' sexual acts on their landing pages.

This approach to such a hard censorship is simply wrong in a free world internet use. As producers we all have a choice and there is absolutely no reason why extreme pornography needs to be openly shown to the world. As such I would urge the BBFC to consider a two tiered structure allowing sites such as mine and many many other responsible sex related business remaining accessible to users.

Those publishers wishing to provide 'extreme pornography' should be the ones made to sit behind a age verification gateway. This one size fits all approach is wrong. Also how does the BBFC propose to remove the extreme and unacceptable images within Google Image Search and Twitter when terms like sex, pussy are entered?

THIRDLY... it is stated in Chapter 3.2 of the draft guidance on Age-verification Arrangements that :- *The use of age-verification in relation to the sale of age restricted goods and services online is well established. A range of solutions to age-verify online is currently available on UK-hosted pornography services.*

Yet out of the following Age Verification companies ( [AgeChecked.com](http://AgeChecked.com) [AgeGo.com](http://AgeGo.com) [AVyourself.com](http://AVyourself.com) [AVsecure.com](http://AVsecure.com) [AgeID.com](http://AgeID.com) ) that I have contacted (on multiple occasions) to enquire about their product and offering, only 2 have come back to me. AVsecure providing a 'free for user' and 'free for publisher' service. Excuse me how does that work...this is highly alarming as to what will happen to this sensitive data, as this proves everything we all fear! AgeID who didn't have a working product last month and when you dig into their Private Policy discover that they intend to use data obtained and I quote... *"In particular, we may transfer non-personal information and process it outside your country of residence, wherever the Platform, its affiliates and service providers operate. We may combine non-personal information we collect with additional non-personal information collected from other sources."*

Need I remind BBFC that AgeID are owned by MindGeek the very company that has provided access to the explicit porn available so freely via their many platforms as



RedTube, Pornhub and YouPorn to name just a couple and yet look to become the gatekeeper to UK adult traffic as the owner of AgeID. How very alarming is that.

Now I would like to think I am not a cynical person, but the thought of having a company such as MindGeek controlling who gains access to my site and product is simply horrifying and completely unacceptable. These will be unknown, unpoliced and unregulated databases without any government assurances of those data-holding companies and it will be outside my site and the privacy I offer to my own members.

As a company MindGeek appear to have little if any ethical values and openly host content stolen from my site to which I have to fight to have takedown. You only have to read MindGeek's website to understand that DATA is at the heart of everything they do. In light of the recent FaceBook scandal I simply do not see how our government can proceed with such a proposal in its current form when people are openly rebelling in the millions with the deletion of their social media accounts. Yet the UK government wants us give access to our most personal and private of viewing habits to companies that frankly would make Facebook look like angels!

I URGE the BBFC to reconsider the implementation of this extremely complex issue and the safety of law-abiding UK citizens data when no system is required when we already have much better safe guards in place for parents to use. Parental controls also help block across all social media and the incoming of any alarming imagery as well as access to explicit sites. Maybe just better education of what controls are already in existence via our phone companies and internet providers would be more beneficial.




# **BBFC Guidance on Age Verification**

## **GBG Response & Questions**

---

Richard Spink

23<sup>rd</sup> April 2018

A large, solid red curved shape that starts from the bottom left and sweeps upwards and to the right, occupying the bottom right portion of the page.

## BBFC Guidance on Age-Verification Arrangements

### GBG Responses and questions

#### Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?

Chapter 3 section 3 (page 9): Please can you describe exactly what “a principle-based approach when assessing new age-verification arrangements” will look-like?

Chapter 3 section 4 (page 9): “As envisaged in the Secretary of State’s Guidance to the Regulator, this guidance does not provide an exhaustive list of approved age-verification solutions, but sets out the criteria by which the BBFC will assess that a person has met the requirements of section 14(1) of the Act to secure that pornographic material is not normally accessible by those under 18.”

Please can you advise why? GBG thinks that a list similar to that displayed on JMLSG website would be very helpful for companies providing access to Adult content - <http://www.jmlsg.org.uk/other-helpful-material/article/providers-of-electronic-identity-databases>.

It is understood that you would not want to promote service providers but we have found that the approach taken by the JMLSG enables customers to make quicker and safer decisions on the tools that they use for verification. If you will not approve providers will you detail an approved process, which is updated by the BBFC as and when changes take place. This would allow solution providers to clearly demonstrate that their solution meets the requirements under section 14.

Chapter 3 section 5b (page 10): “use of age-verification data that cannot be reasonably known by another person, without theft of data or identification documents or readily predicted by another person”

Can BBFC publish a list of which combinations of data are acceptable? Below are some which could potentially be used:

Name and Address plus one of the following:

Passport MRZ

UK Driving License Algorithm – only GBG has permission to reverse engineer this

European ID Card Algorithm

UK Electricity Supply Number

Credit or Debit Card Authorisation

Bank Account

Mobile Phone liveness check

UK National Insurance Number Algorithm

ID Document Scan – image is valid

It would be helpful to understand if the BBFC thinks these are acceptable as proof of age as well as being pieces of information 'only known to the individual'.

What is the BBFC's stance on UK citizens using VPNs to change their browsing country of origin? This is a common solution for country restricted content already online so will likely be used in this scenario also. I.e. in an instance where an under 18 from the UK has been proven to access adult content but used a VPN to do so to appear from a non-UK location is the liability on the adult web site or not?

Can the BBFC provide any indication on timeframes on prosecuting non-compliant adult sites from identification / remediation / action milestones?

### **Do you have any comments with regards to Chapter 4?**

4 section 3f (page 12): "the need to ensure that personal data is not retained for longer than is necessary to achieve the purposes for which it was originally collected"

How long do records of checks need to be kept? Can you please advise on what audit-trail, if any needs to be kept? This will need to be determined under the regulation to enable GBG and customers to store records in line with GDPR so clarity would be appreciated.

## **Draft Guidance on Ancillary Service Providers**

### **Do you agree with the BBFC's Approach as set out in Chapter 2?**

### **Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?**

Yes and Yes. But we're very keen to understand more detail about how the big Social Media Platforms which display pornographic content and earn advertising revenue from it will be regulated? Will this be through the age of their user being verified?

## **BBFC Digital Economy Act Guidance Consultation: Draft guidance on Ancillary Service Providers**

IAB UK response

### **Background**

IAB UK is the trade association for digital advertising, representing over 1,200 of the UK's leading brands, media owners, technology providers and agencies. Our purpose is to build a sustainable future for digital advertising.

The IAB is actively engaged in working towards the optimal policy and regulatory environment for the digital advertising market to continue to thrive. We also seek to promote good practice to ensure a responsible medium.

The Digital Economy Act 2017 identifies certain advertising services as 'ancillary service providers' who may receive a notice from the regulator that a person is non-compliant. We have reviewed the draft guidance from that perspective and our comments are set out below.

### **1. Do you agree with the BBFC's Approach as set out in Chapter 2?**

Overall this Chapter does not sufficiently reflect that the *Guidance from the Secretary of State for Digital, Culture, Media and Sport to the Age-Verification Regulator for Online Pornography* (referred to in this response as 'the SoS guidance') makes clear that there are two overarching principles to which the regulator should have regard: effectiveness and proportionality. Proportionality should include whether it is proportionate to expect or rely on action by an Ancillary Service Provider (ASP) (notwithstanding our comments in relation to Chapter 3 – notification below) having considered and taken into account the impact on and consequences for them of doing so, in addition to the impact on and consequences for the non-compliant person.

Specifically, proportionality needs to be reflected in the following parts of the guidance:

- Paragraph 4: the criteria here should include whether the ASP could feasibly take action that is likely to support the regulator's enforcement action; whether it is reasonable for them to do so; and what impact such action might have on the ASP both in relation to the specific case, and more widely. This paragraph needs to set out in more detail how proportionality will be judged.
- Paragraph 10: Again, as drafted, the BBFC's decision-making here is limited to only considering the effectiveness of a particular course of action, not its proportionality.
- Additionally, this point is relevant in relation to Chapter 3. Paragraph 9 should allow for an ASP to make representations in relation to the proportionality of a notice, not only

whether that notice is technically ‘correct’, and for the regulator to withdraw a notice if it is shown to be disproportionate.

## **2. Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?**

Paragraph 3 lists some of the ASPs that the regulator may consider under s.21(5) of the Act. The guidance does not make clear whether these ASPs are being considered under paragraph 21(5)(a) or (b). This should be clarified, and where any service is included in this list as an ASP under paragraph 21(5)(a), it should be made clear that a service is only in scope if and to the extent that the service enables or facilitates the making available of pornographic material or extreme pornographic material on the internet by the non-complying person.

To date, our discussions with the BBFC in relation to advertising ASPs have been limited to those services captured by para 21(5)(b) of the Act (i.e. those in para 3.f. of the draft guidance). Two other types of advertising ASP are included in the list in paragraph 3 (d) and (e) and these warrant further discussion with the digital advertising sector, not least in order to clarify what services are being referred to and what the difference is between the two. Digital advertising is a complex ecosystem and the draft guidance is not clear what ancillary services are intended to be caught in practice by the definitions used here (e.g. ‘provide advertising space’), or under what provision of the Act they are included in this list, which means that we cannot assess the appropriateness or otherwise of their inclusion or judge whether further discussion on the notification process is needed. In the case of (e), the making available of advertising space is usually controlled by a web publisher not providers of ancillary services.

Paragraph 4 notes that additional services may be considered to be ASPs in the future. However, this guidance simply repeats the SoS guidance on this issue, and there is no additional information given about how potential ASPs will be informed, or how notification arrangements will be agreed. More detail should be included here on what the process will be and how relevant stakeholders will be involved and consulted.

### **Other comments**

#### Chapter 1: guidance

Paragraph 8: changes to this guidance should also be subject to consultation with stakeholders before being laid before Parliament, in line with section 5 of the SoS guidance, and that should be reflected here.

Paragraph 13: this paragraph should allow for a process whereby stakeholders can request additional, formal guidance from the regulator where that is necessary and appropriate, including on specific issues. This is an entirely new regulatory regime and it is highly likely that questions will arise once it begins to be enforced that require additional guidance. ASPs should not be in the position of having to rely on informal guidance.

### Chapter 1: reporting

Paragraph 10: this paragraph outlines the regulator's approach to reporting and states that it is required to report annually on the regulatory regime. This narrow definition does not appear to us to accurately reflect the SoS guidance, which states that the regulator should report on the exercise of its functions and their effectiveness. The report should therefore not only address the three areas identified in the guidance, but also the regulator's approach to enforcement, the effectiveness of that approach, and how it has met its duties of effectiveness and proportionality in discharging its responsibilities. The regulator should consider how it will seek views from stakeholders to inform its reporting.

### Chapter 3: Notification

The guidance states that notices given under s.21 of the Act will request the ASP to withdraw their services. There is no basis for such a request in the Act, and given the voluntary nature of any action by an ASP, the regulator should not seek to influence an ASP's response. This may not be withdrawing a service, which could have serious consequences, legal or otherwise. There are also perceptual risks for the ASP if a notice implies that a particular course of action is expected to be taken but, for whatever reason, is not. This point should also be reflected in paragraph 8, which also refers to a 'request to withdraw services'. The text from '...so that the' to the end of the sentence should be deleted.

MARC DORCEL

Dear Sir,

First thanks for adding you into your consultation.  
You will find in this email our views about the documents and about the questions mentioned in your email.

**“Draft Guidance on Age-verification Arrangements**

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

We appreciate the approach proposed about being concerned of adoptability by end user and as well by website owner.

We understand that BBFC wants the solutions to stay cost effective and UX compliant in order to be as frictionless for users as possible.

It's also considered that it needs to stay open to innovation and that solutions shall not lead to strangle nor the market nor independent website by giving uncontrolled power to age verification processors.

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

We do agree on most Age-verification Standards set out in chapter 3 but we encourage the BBFC to raise the level of expectation regarding some datasets.

A low level of expectation could lead to a weak system easy to manipulate and could undermine the success of the all Age Verification project.

- **Article 2** mentions the PASSPORT and DRIVING LICENCE as solutions to age verify online but copies of captured ID are available online.

In order to avoid a significant level of fraud risk that would discredit the Age verification project with age proof (ID can be available online, shared, as well as login and password...)

- This information should be crossed checked with another info/source/document  
Such as the 3DSECURE system (used for Visa and Mastercard security), for each access demand, a code have to be sent to the unique registered phone number and/or mail associated to the account.  
Rule is = 1 authorization = 1 user

- **Article 5** mentions password or identification number. Without any guideline toward this specific topic, BBFC is opening a breach in what we call a major challenge: “not giving to a processor the power of being a gateway or a toll to adult contents able to take advantage of internet user's data”

The majors requirements to define an independent Age Verification system that would not serve specific corporate interest are:

- 1st requirement: An adult authenticated shall not belong to any processor as well as his Data.



- 2nd requirement: Processor system should be chosen freely because of their efficiency and not by forcing with a dominant position.

## 2 solutions possible :

- **Any Age verification processor scope should be limited to a verification task without registration system**
  - As a consequence, age verification company could not get benefits on any data user or traffic control (*sadly such mkt intentions was already express publicly*)
  - Each Website or Website networks could create independently user account and store that the client is age verified
  - But User would have to get age verify on each website or each network of websites

or

- **Any Age verification processor allowed by BBFC to manage login and password and to control a visitor data base, should be only if they commit to share the +18 login/password with the others certified processor.**
  - User would have only one age verification enrolment on its first venue to a pornographic website
  - User would be able to log on any age verification system to proof his age which will assure the largest use and facility for this Age proof.
  - Adult will not belong to any processor and it is the condition to avoid any dependency conditions.

In those case, we believe that an age verification solution will act like a MPSP (multiple payment service provider) which proceed client payments but where client doesn't belong to the payment processors but to the website and where credit card numbers can be used by any processor.

Do you have any comments with regard to Chapter 4?

We don't have any comments on this chapter.

Any comments regarding Chapter 4 will be referred to the Information Commissioner's Office for further consideration.

## **Draft Guidance on Ancillary Service Providers**

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

We don't have any comments on this chapter.

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?"

We don't have any comments on this chapter.

We would be really pleased to follow this exchange with the BBFC if you would require furthermore information

You will find enclosed to this email a power point presentation that illustrate again our position toward that topic and the consultation response cover sheet.

Best regards,

*Directeur des Opérations Digitales - C.O.O.*





**MARC DORCEL**  
L U X U R E D E P U I S 1 9 7 9

**AGE VERIFICATION & INSIGHTS**

03/19/2018

# AGE VERIFICATION NEEDS & SOLUTIONS

## Age verification tools need to fulfil 3 targets

- Guarantee efficiency in age controlling, trust and safety for control and data protection
- Ensure a frictionless journey with quick and easy enrolment
- Remain cost effective and technically acceptable for websites owners

## 3 ways to age verify our client



### CREDIT CARD PROCESSOR

- Safe, secured and usual
- Already validated by BBFC
- Trustfulness increased by a payment traceability and 3D secure protocol



### MOBILE OPERATOR

- Safe, secured
- Common and user friendly
- Linked to a registered proof of ID collected by telecom operators
- Access code dedicated to one mobile



### AGE VERIFICATION PROCESSOR (ID, MOBILE N°... CONTROL)

- Usual for gambling or bank services
- Safety level down due to easy access ID copies and sharing of password

- Payment service provider (PSP) are already considered as an independent efficient age verification solution (independent, no data storage, interoperability, 3D secure : One access authorisation, one user)
- Age control by other processor reinforcement with the use of a code or password as 3D secure protocol (one access authorisation, one user)

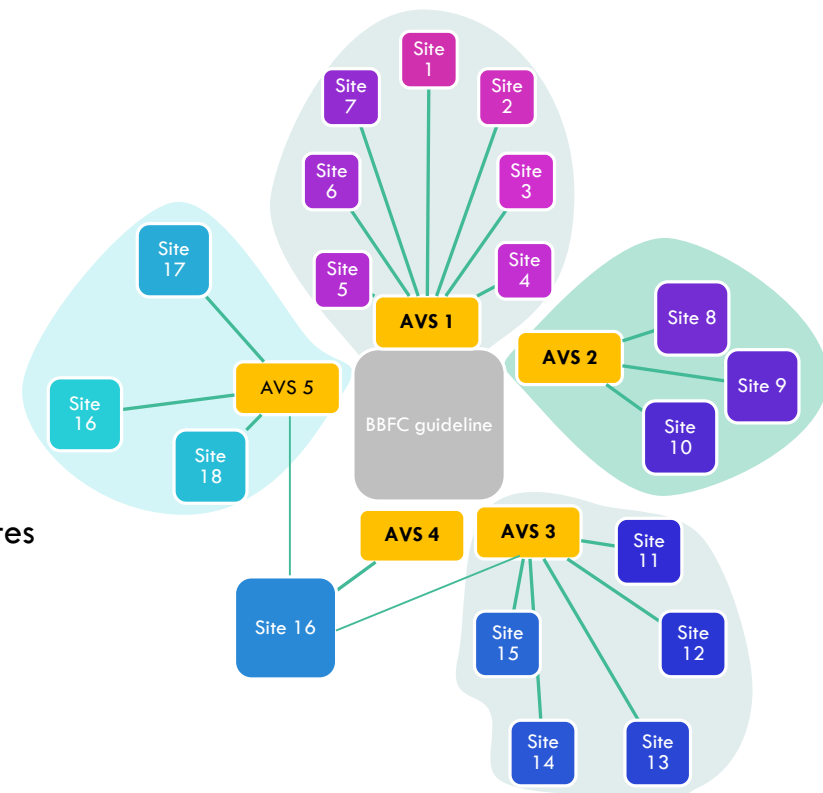
# INDUSTRY MUST REMAIN VIGILANT TOWARD AV SOLUTIONS



- BBFC challenge is not to give to a processor the power of being a gateway or a toll to adult contents able to take advantage of internet user's data
- Processor system should be chosen freely because of their efficiency and not by forcing with a dominant position
- An adult authenticated shall not belong to any processor as well as his Data

## FOCUS ON A GLOBAL RISK FOR THE INDUSTRY

- BBFC pronounce guideline to verify client age
- Some Age Verification providers builds solution where they:
  - Control client information
  - Store client information
  - Provide client with a login password
- Doing this:
  - Client is linked to an Age Verification provider who will strangle websites
  - Age Verification provider build strong dependence for the website
  - Age Verification provider build their market value on their client database instead of their technical capability or pricing



# 2 PROPOSITIONS TO GO AHEAD

## 1. Age Verification providers could be **limited to age controlling** (no registration management)

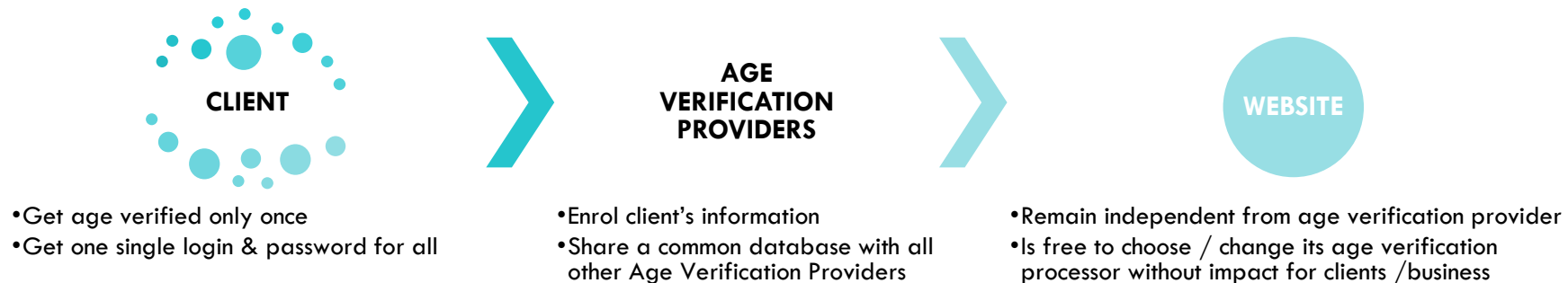
- Age verification provider would act like a Payment Service Provider (PSP) with VISA by being an independent processor without enrolment
- Client & Website wouldn't be dependant of any Age Verification Processor



OR

## 2. Age verification providers **could share together clients' credentials** (login / password) in a standard protocol

- Age verification providers would act like multiple payment service processor (MPSP) by being an independent processor using a single authentication process
- Clients would have one single Age Verify login to use all the website possible independently to the age verification processor



Mastercard response to *BBFC*  
*‘Consultation on draft Guidance on*  
*Age-Verification Arrangements and*  
*draft Guidance on Ancillary Service*  
*Providers ‘*

23 APRIL 2018

## Introduction

Mastercard welcomes the draft guidance published by the BBFC, although it is unclear why it is that the legislation only requires the BBFC to publish guidance in relation to ancillary service providers and not in relation to payment service providers.

This is unhelpful from Mastercard's perspective and we regret that the BBFC has not so far taken the initiative to provide greater clarity or guidance as to how it will engage with payment services providers. We would urge it now to do so, which is the purpose of this short response.

## Identity of Payment Services Providers

The definition of payment services providers is potentially broad and wide-ranging, although it has been assumed throughout the course of the legislation that it encompasses card schemes, such as Mastercard. However, it could also include others in the payments value chain including card issuers, but more particularly merchant acquirers, but also wallet providers or others.

Assuming that as a card scheme Mastercard is caught by the definition, we would welcome clarification as to whether the BBFC may be intending to notify providers other than card schemes, as payment services providers, or whether the schemes alone will bear this responsibility.

## Notification of Payment Services Providers

Mastercard continues strongly to urge the BBFC to provide greater clarity as to its intended process for notifying payment services providers. Regrettably, we have seen no progress on this point for many months and we are very keen to engage with the BBFC in substantive discussions to understand how it intends the notification process to operate and to provide our feedback and input into that process.

By way of reminder of points previously raised, the BBFC will be aware that the relevant Mastercard rule which provides the basis for any action we may take, states as follows:-

*"A Customer may not directly or indirectly engage in or facilitate any action that is illegal or that, in the opinion of the Corporation and whether or not addressed elsewhere in the Standards, damages or may damage the goodwill or reputation of the Corporation or of any Mark. Upon request of the Corporation, a Customer will promptly cease engaging in or facilitating any such action."*

The 'customer' in this case refers to the merchant acquirer, rather than the merchant/website operator. The action which Mastercard could take would therefore be based upon the premise that the acquirer is at least indirectly facilitating an illegal action i.e. by acquiring a merchant which was operating an infringing ('illegal') website.

Therefore, the situation envisaged by the legislation is that the illegal activity is not the provision of an illegal product or service in return for payment (which is normally the case) but rather it is the entirely unconnected operation of a website without age verification controls in place.

This unusual disconnect between the illegal activity and the provision of the payment service, creates unique challenges which the BBFC must consider in designing its process for notifying payment services providers,



once it has satisfied itself that that the website in question is operating in breach of s14(1) of the Act. They can be summarised as follows:-

- How to establish and evidence that the merchant identified in the BBFC's notification to payment services providers is in fact the owner/operator of the website that the BBFC has found to be in breach of s14(1). In order to target non-compliant websites providing free content (and therefore not accepting Mastercard) the legislation envisages that Mastercard will take action against entirely separate websites (which do accept Mastercard), if they are owned by the same entity which owns the infringing free content website. It is unclear how easy it may be to evidence an ownership/control connection between websites in these circumstances and whether the owners/operators of potentially non-compliant free to access websites might take steps to disguise their ownership or control.

This is the key concern for Mastercard which will determine the extent to which we will or will not be able to take action and in relation to which we have so far not received any clarity.

- How to establish that the merchant notified by the BBFC to Mastercard accepts payments from UK-issued Mastercard cards. This should be a more straightforward part of the process, but it is a crucial step nonetheless because Mastercard needs to be able to identify the acquirer and be satisfied that the merchant is 'live' and accepting payments, in order to be able to require the acquirer to terminate Mastercard payment acceptance.

As we highlighted to the Government throughout the legislative process, Mastercard will itself be undertaking investigations to verify the evidence which we receive from the BBFC on these points, as is usual business practice. We have therefore not given any guarantees that we will take action in any individual case if we are not able conclusively to establish that that acquirer (merchant) is in fact facilitating an illegal action or if the acquirer provides alternative or contradictory evidence to us. In those cases, we would expect the BBFC to provide further assistance and evidence to substantiate its claims, if it still wishes Mastercard to take action against the acquirer (merchant).

However, in principle Mastercard remains committed to the intentions of the legislation and assisting the BBFC whenever sufficient evidence has been provided. But in practice Mastercard's ability to assist the BBFC to take action is likely to be very largely determined by the quality of that evidence which the BBFC provides. Mastercard has established notification processes which we would like to discuss with the BBFC, in order to ascertain whether it will be able to work within them and specifically whether the type of evidence which the BBFC envisages supplying will be sufficient to enable us to take the desired action.

## **Comments on the draft Guidance**

Although the guidance has limited relevance to payments services providers, we will comment briefly on Chapter 2, which provides some high level indications as to how the BBFC may engage with payment services providers.

In particular, paragraphs 9-12 attempt to provide guidance as to the circumstances in which the BBFC may choose to give notice to a payment services provider, but unfortunately give no real sense as to whether, when or how often this may occur in practice. Specifically, the guidance makes almost no distinction between the enforcement options available to the BBFC and therefore provides no means of judging which will be used in any particular situation.

Paragraph 9 simply lists the enforcement options without any ranking or further context. Paragraph 10 adds merely that *“the BBFC will be guided by its assessment of which course of action will be most effective in achieving the child protection goals of the legislation”* and will consider which enforcement option *“will have an effect on the non-compliant person’s behavior”*. Paragraph 11 adds that the BBFC may assess whether non-compliant services *“have content or services that require payment”*. Paragraph 12 concludes by saying that *“the BBFC will take a case-by-case approach, and will also consider what enforcement action has proven to encourage compliance in previous cases of non-compliance”*.

The single line in paragraph 11 is the only one which references payment services providers directly, but in so doing it effectively only confirms the obvious point, namely that the BBFC will have to determine whether or not a provider accepts payment before considering whether notification to a payment services provider is appropriate (or indeed possible). In practice, this provides no useful additional information or guidance.

Whilst noting that the BBFC wants the flexibility to *“take a case-by-case approach”*, Mastercard believes that it could go further in clarifying (at least at a high level) the circumstances in which it is more or less likely to want to provide a notification to a payment services provider. Although not every case will be the same, in practice many of them will be very similar and so the BBFC should be able to go further in providing guidance to Mastercard as to when it is likely to receive a notification.

For example, in circumstances in which advertising appears on a website that also accepts payment (which would seem to be a fairly common scenario) a notification to an ISP, a payment services provider and an ancillary service provider will always be available options. The BBFC should be able to say whether a notice to ISPs to block access to the website is likely to be a first or last option, when compared with a notice to a payment services provider. Similarly, is the BBFC likely to want to target payment services providers or advertisers first? Mastercard does not believe that there are so many variables that it should not at least be possible for the BBFC to provide a broad indication of the ranking or order in which it is likely to want to use its enforcement options.

Such guidance need not bind the BBFC irrevocably, but it would allow Mastercard to make an assessment as to the probable demands or expectations that it will face as part of this new process. There is likely to be a significantly different impact between being the first or last port of call for enforcement notices, which will have a resulting consequences for resources. As matters currently stand, Mastercard has no means of judging whether it can expect to receive notifications in the majority of cases of non-compliance or if its involvement is likely to be incidental.

Once again, we would urge the BBFC to provide further clarity and guidance on this point as a matter of increasing urgency.

## NSPCC Response to the BBFC consultation on Age Verification & Ancillary Service Providers Guidance

- The NSPCC welcomes the steps taken by the regulator to emphasise that age verification is about protecting children from pornographic content, and the steps they have outlined on how they will achieve this.
- We are concerned about a lack of information relating to how the BBFC will monitor changes in children's access to pornography, and strongly believe that a commitment to robust, regular research with young people and professionals is vital for enabling the BBFC to fulfil its regulatory functions effectively.
- The Guidance does not include details of how trusted organisations or individuals can make referrals to the BBFC in relation to non-compliant sites, and we would welcome further information about this.

### Guidance on Age-Verification Arrangements

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

1. The NSPCC welcomes the focus on protecting children that this Guidance emphasises. We agree that age verification of online pornography is an important step in protecting children from seeing content that is inappropriate and can be upsetting to them.
2. The NSPCC understands the need to take a proportionate approach to regulating age verification given the high number of pornographic sites available in the UK. As outlined in Chapter 2, paragraph 5, we welcome the commitment to focusing on sites which 'are most frequently visited, particularly by children'.
3. To achieve this, the BBFC must conduct robust, regular research with children and professionals. Only then can they reliably know the sites that young people are most frequently using to access pornography online. Doing so draws on existing BBFC practices and evidence based standards, as followed during their classification guidelines review, in which 10,000 adults are consulted.
4. As stated within the Digital Economy Act, the regulator may 'carry out, commission or support (financially or otherwise) any research which it considers appropriate for the purposes of exercising, or considering whether to exercise, any function' under part 3. This research should:
  - a) Be undertaken on a longitudinal basis, at least annually, with the first round being completed before the legislation goes live to set a benchmark for young people's current access to online pornography;
  - b) Use a large, representative sample of young people from across the UK;
  - c) Include quantitative data to understand the prevalence and location (including pornography sites and social media sites) of young people's access to pornographic content;
  - d) Include qualitative research to understand the impact of AV;
  - e) Seek to gain insight into any circumvention methods that young people are using; and
  - f) Include professionals working with children, to gather their insight into the impact of the legislation.

5. The NSPCC welcomes the wider consideration that the BBFC have stated they will make of content on sites which may 'raise other child protection concerns' (paragraph 5). We would welcome the opportunity to further discuss what these 'other child protection concerns' may be.
6. Under S29 of the Digital Economy Act, the Secretary of State must report on the impact and effectiveness of this legislation, and consult on the definitions used in part 3 of the Act. As the Secretary of State will require information from the regulator to do so, the BBFC should record the type and prevalence of other pornographic content that currently falls outside the scope of this legislation. This should include content that the BBFC would refuse to classify offline under the BBFC's most recent classification guidelines, such as content that is 'likely to encourage in interest in sexually abusive activity, which may include adults role-playing as non-adults'.<sup>1</sup>
7. The inclusion in paragraph 11 of 'links to the non-compliant service on platforms such as social media' may act as an enforcement mechanism against non-compliant sites. However, we note this is contingent on whether social media firms choose to comply with regulatory notices when they are issued. We would encourage the BBFC to explore how it has secured agreements with other sectors, such as payment providers, and to consider how best it can secure compliance from social media companies, given there is no legal requirement for them to do so.
8. More generally, we consider that these proposed arrangements will be insufficient for preventing young people from viewing pornography on social media. We know through Childline, our services and our research that young people often come across pornography on social media sites, whether inadvertently or through intentional searches. However, compliant sites will continue to be able to post pornographic content onto their social media accounts, where young people will be able to freely access it.
9. This is particularly concerning in relation to platforms such as Twitter and Tumblr, which allow adult content to be shared on their site. Although other platforms do not allow pornographic content on their platforms, in some cases it is necessary for this material to be reported in order to be taken down, and some social networks are often slow to act to remove such content. As stated in the DCMS Guidance, there is no requirement for ancillary service providers to take any action on receipt of a notice. We have seen time and again that social media sites are rarely responsive to non-regulatory requests for compliance. We are sceptical that including social media sites as an ancillary service will encourage compliance from pornography sites, or reduce young people's access to this content on social media.

## How young people access pornography

During our research with over 1,000 young people aged 11-16, we asked how and where young people were viewing pornography.

- Children and young people were most likely to have first been exposed to pornography inadvertently (e.g. via pop-ups or shown by someone else unexpectedly).

---

<sup>1</sup> BBFC (2014) 'BBFC Guidelines', available online: [http://www.bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014\\_0.pdf](http://www.bbfc.co.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf)

Here are some of the things they told us about where they saw it:

*“Often when on Tumblr, someone would have reblogged a post, or a post leading to recommendations of pornographic .gifs. Normally, these take me by surprise and make me feel quite uncomfortable” (Female, 13-15).*

*“On Facebook people’s accounts get hacked and then the hackers post pornographic videos and tag my friends in them and it pops up on my news feed” (Male, 11-12).*

*“On popular hashtags on Instagram, which younger children can access, there are some explicit pictures. Makes me feel irritated that people can come across these when they don’t want to or have tried to” (Female, 13-14).*

10. Paragraph 16 states that details of notification actions will be published on the BBFC’s website. This should include naming non-compliant sites and Service Providers to increase opportunities for public pressure as a means of encouraging compliance or removal of services.
11. This Guidance should include information on the BBFC’s intended process for young people, schools, parents, and trusted organisations to refer non-compliant sites to the regulator. In the last three years Childline has received over 2,000 calls from young people about seeing online pornography. This could provide useful insight to the BBFC, to supplement robust research, to allow them to take action on sites that we know are frequently being visited by children. For this reason we would welcome a discussion particularly looking at how trusted, child-facing, expert organisations can refer non-compliant sites to the regulator.

### **Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?**

12. Broadly speaking, we agree with the standards set out in chapter 3. Our concern in this approach is that the use of passwords and PINS provides an easy opportunity for young people to access age restricted sites on shared devices. We would recommend that, working with child protection experts such as the NSPCC, further advice and guidance is provided to age-verification providers and pornography sites as to how best they can build child protection steps into their processes. We therefore welcome the recommendations in paragraph 7, and would encourage the BBFC to actively promote good practice measures to sites and AV providers.
13. We are concerned that some of the methods for age verification are not sufficient in and of themselves. For example, credit cards should only be used as part of a multi-tiered approach given how common it is for credit cards to be left around family homes.
14. Much of the media coverage around age verification has focussed on adult privacy concerns. This has the potential to create fear among adult users of legitimate, compliant pornography sites, potentially driving traffic to the dark web or other sites with concerning and illegal material, including child sexual abuse material. We are pleased that the BBFC will be assessing data protection compliance as part of their age-verification assessments, as set out in paragraph 9. However, as regulator, we hope that the BBFC will take a proactive approach in reassuring consumers of the steps that are being taken to protect and secure confidential data, even before the legislation goes live.
15. While the focus has been on adult’s data, there is also a need for reassurance that the data of children who attempt to access adult sites will also be protected. As stated in the ICO’s

Children and GDPR Guidance consultation document, 'children need particular protection when [sites] are collecting and processing their personal data. [Sites] should consider the need to protect them from the outset, and design... systems and processes with this in mind'.<sup>2</sup> This is important to build confidence in the new regulatory arrangements, and to ensure there are effective measures in place to prevent children's data from being misused in any way that could result in risk of exposure to harm.

## Do you have any comments with regard to Chapter 4?

16. We have no comments in relation to chapter 4.

## Draft Guidance on Ancillary Service Providers

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

1. The BBFC's ability to revise this guidance, as stated in paragraph 8, should also be in the light of new data and evidence about how and where children are accessing pornography.
2. The proportionate approach outlined in paragraphs 4 and 5 should be informed by research into the sites and means by which young people continue to access pornographic content online. Details of our proposal for this are included in paragraph 4 of our response to the Consultation on age-verification arrangements.
3. We know from our research that viewing pornography can be extremely distressing for young people and can give unrealistic and problematic ideas about sexual relationships. It is therefore vital that the 'prompt timeframe for compliance', referenced in paragraph 7, is as short as is reasonably possible to reduce the number of young people that remain able to access the site, whether intentionally or accidentally.

### The impact of viewing pornography on young people

From our research with over 1,000 young people aged 11-16<sup>3</sup>:

- 27% of those who had seen pornography told us they felt shocked the first time they viewed it.
- 53% of boys and 39% of girls who had seen online pornography said they thought it was realistic.
- 44% of boys and 29% of girls who had seen online pornography said it had given them ideas about the types of sex they want to try out.

Here are some of the things young people have told us about viewing pornography:

*"It gives an unrealistic view of sex and our bodies, makes us self conscious and question why our bodies are not developed like what we see online."* (Female, 13)

<sup>2</sup> Information Commissioner's Office, 'Consultation: Children and GDPR guidance'. 21/12/17 – 28/2/18.

<sup>3</sup> Martellozzo, E., Monaghan, A., Adler, J.R., Davidson, J., Leyva, R. and Horvath, M.A.H. (2016) I wasn't sure it was normal to watch it. London: NSPCC

Draft Guidance on Online Pornography (Commercial Basis) Regulations 2017 and Draft Guidance on Ancillary Service Providers – Naturist Action Group’s Response.

Do you agree with the BBFC’s Approach as set out in Chapter 2?

1. In general, Naturist Action Group agrees with the approach the BBFC is taking in regards to Online Pornography (Commercial Basis) Regulations 2017 and Ancillary Service Providers, but we also believe the BBFC has a duty of care to the consumer, ensuring they are not misled by inappropriate titles and/or description of content under Regulation 5 of The Consumer Protection from Unfair Trading Regulations 2008 and paragraph 32 of The Digital Economy Act 2017.
2. The Naturist Action Group (<http://naturistactiongroup.org>) is an independent collective of naturists seeking the inclusion of naturism within British society. It is a not-for-profit organisation, limited by guarantee, and has no membership, but can number approximately 500 registered users for our website, almost 1,500 supporters on Facebook and roughly 4,000 followers on Twitter.
3. Section 15 (1) (d) of the Digital Economy Act 2017 defines the online content covered by the regulations as: “a video work in respect of which the video work authority has issued an 18 certificate, and it is reasonable to assume from its nature was produced solely or principally for the purposes of sexual arousal.” Sections 15 (1) (f) (i) and 15 (1) (g) (i) similarly describe the content covered.
4. The International Naturist Federation ([www.inffni.org](http://www.inffni.org)) defines naturism thus: “Naturism is a way of life in harmony with nature characterised by the practice of communal nudity with the intention of encouraging self-respect, respect for others and for the environment.”
5. From British Naturism’s website (<https://www.bn.org.uk/campaigning/index/>), it defines naturism as: “A philosophical belief in a natural, naked lifestyle’ characterised by respect; for oneself, for others and for the natural environment.” Our own definition is not too dissimilar from that used by British Naturism. All three organisations believe that naturism is the expression of non-sexual social nudity that has benefits, both psychological and physical, for human health.
6. The Oxford English Dictionary (<https://en.oxforddictionaries.com/definition>) defines the word *naturist* as: “A person who goes naked in designated areas; a nudist. (e.g.): ‘he is a dedicated naturist’” and for *nudist* it states: “A person who engages in the practice of going naked wherever possible.” Similarly, Chambers Dictionary defines Nudism as: “1. The practice of not wearing clothes, as a matter of principle; 2. *US Naturism*. Nudist, noun, someone who wears no clothes, as a matter of principle.” None of these definitions suggest that sexual activity is part of the lifestyle.
7. An online search using the term “naturists in porn” easily finds websites offering pornographic content with ‘naturist’ or ‘nudist’ in the title, thereby implying a link between the lifestyle and sex, and purely for the purpose of arousal (e.g.: <https://xhamster.com/videos/naturist-club-filed-with-a-friend-pt-1-8828101>; [https://www.xvideos.com/video11452787/nudist\\_bar\\_-\\_30s\\_france](https://www.xvideos.com/video11452787/nudist_bar_-_30s_france)). All too often with the online content the pornographer provides they give the impression that naturists, by their naked state are almost permanently aroused and desire sex. Not so. Naturists acknowledge the existence of sex, of course; naturism is a family-orientated lifestyle after all, but like so many things in life, it has its time and its place. The use of the ‘naturist’ tag by the online pornography industry therefore has detrimental consequences to the consumers’ understanding of what naturism (nudism) is and as a result they are being misled by the use of these terms in the title of the work and/or description used to entice the consumer into a transactional purchase.
8. While Naturist Action Group recognises that the primary purpose of the BBFC in this process is to ensure that online pornographic works with either an ‘18’ or ‘R18’ certificate and websites hosting these pornographic works are age restricted, we believe the BBFC has an unspecified duty to protect the consumer by ensuring they are not misled by incorrect terms in titles and/or descriptions.
9. Under **The Consumer Protection from Unfair Trading Regulations 2008 Part 2, Misleading Actions, Regulation 5** (<http://www.legislation.gov.uk/ukxi/2008/1277/regulation/5/made>): ‘a commercial practice is a

misleading action if it satisfies the conditions in either paragraph (2) or paragraph (3).’ Paragraph (2) (a) states a commercial practice would satisfy the conditions of the paragraph “if it contains false information and is therefore untruthful in relations to any of the matters in paragraph (4).”

10. Paragraph 4 (f) of Regulation 5 referenced above states that: “any statement or symbol relating to direct or indirect sponsorship or approval of the trader or the product.” As stated previously, it is our contention that statements made by the pornography industry describing naturism are false and misleading. No naturist organisation would sponsor or approve of a pornographic trader or their product, either directly or indirectly that links the naturist lifestyle with sexual activity via online video content, either by word or deed.
11. Paragraph (3) (a) of the 2008 regulations states a commercial practice would contravene it if “it concerns any marketing of a product ... which creates confusion with any products ... or other distinguishing marks of a competitor.” No reputable naturist organisation would consider themselves a competitor to that part of the sex industry these regulations are concerned with, however, we would contest that the terms naturism, naturist, nudism and nudist defines our ‘product’ as described above and would not endorse or condone how pornographers would like it to be portrayed. It is our contention that statements made in the title and/or description of the work amount to marketing material designed to attract the consumer to either view or purchase the video work allegedly containing naturist content.
12. We further submit that the BBFC should consider Paragraph 32 of **The Digital Economy Act 2017** which amends section 107 of The Copyright, Designs and Patents Act 1988 relating to the infringement of copyright. It substitutes the text for paragraphs 2A and 2B, making them more relevant to the new economy. The text for paragraph 2A is changed to: “A person (‘P’) who infringes copyright in a work by communicating the work to the public commits an offence if P (a) knows or has reason to believe that P is infringing copyright in the work and (i) intends to make a gain for P or another person.”
13. Video content ([https://www.xvideos.com/video9552899/nudist\\_colony\\_tour\\_-\\_naked\\_and\\_free](https://www.xvideos.com/video9552899/nudist_colony_tour_-_naked_and_free)) titled *Nudist Colony Tour* hosted by xvideos.com is a promotional work owned by Hideaway Nudist Resort, Oklahoma USA, and listed by the American Association for Nude Recreation (AANR) as a member for the Southwest region (<https://www.aanr-sw.org/index.html> — accessed 14 Apr 2018). In 2008, this association suspended a nudist resort for contravening its family-friendly policies (<http://ttt-suweb.newscyclecloud.com/news/2009/aug/22/pa-g-string-contest-brings-trouble-to-paradise-ar-83093/>). The resort later gave up its membership allowing it to pursue an adult-only business model. In the light of this, it is highly unlikely that permission to upload the video would have been given by Hideaway Nudist Resort, even if it had been sought.
14. Although the above example is from the USA, it demonstrates the blatant disregard for copyright law for any country by the online pornographic industry, the United Kingdom included.
15. Naturist Action Group recognises that these arguments may be outwith the scope of this consultation but feel that it is important that we bring to your attention through this submission the broader aspects of consumer protectionism implied in the Digital Economy Act 2017, and the Consumer Protection from Unfair Trading Regulations 2008. We feel that the BBFC is in an ideal place to inspect content as the designated authority under the Video Recordings Act 2010, to not only assign a certificate to the video and confirm the age-verification process as fit for purpose, but to also verify that the title and/or description are not potentially misleading consumers with inaccuracies and/or false vicarious endorsements.

Do you agree with the BBFC’s Age-verification Standards set out in Chapter 3?

*No Comment*

Do you have any comments regarding Chapter 4?

*No Comment*





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

<b>Summary</b>	<b>4</b>
<b>Recommendations</b>	<b>4</b>
<b>Age-verification Arrangements Response</b>	<b>6</b>
Do you agree with the BBFC's approach as set out in Chapter 2?	6
Age verification's inability to meet its own stated aims	6
Extreme pornography does not fit within the scope of the legislation's aims	8
Other material which should be out-of-scope	9
Section 21 and 23 assessments must include a proportionality test	10
Do you agree with the BBFC's age-verification standards set out in Chapter 3?	10
Age verification risks social exclusion	10
Privacy guidelines are non-binding	11
Choice of providers	12
Do you have any comments with regards to Chapter 4?	12
The regulatory gap omitting privacy in pornography-related age verification	12
Risks of age verification for pornographic content	13
Identity risks	14
Risks from logging of porn viewing	14
Everyday privacy risks for adults	14
Risks to teenagers' privacy	15
Trust in age verification tools and potential scams	15
Market related privacy risks	15
Potential enforceable privacy standards for pornography-related age verification	16
Duty to regulate privacy for age verification systems	17
<b>Ancillary Service Providers Response</b>	<b>19</b>
Do you agree with the BBFC's approach as set out in Chapter 2?	19
Notices to withdraw service risk causing significant and irrevocable damage	20
Notices to ancillary and payment service providers risk sidestepping due process	20
Ineffective notices under section 21 will lead to disproportionate use of website blocking orders	21
Do you agree with the classes of ancillary service provider set out in Chapter 3?	22
Issues raised by considering social media platforms as ancillary service providers	22
Extension of definition should require consultation	23
Effect of withdrawing services: legal uncertainty, and inconsistency	23
Appealing notices	23

# 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 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.<sup>1</sup> 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".<sup>2</sup>

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.<sup>3</sup> Peer-to-peer file sharing

---

<sup>1</sup> Ogas O. (2011). *A Billion Wicked Thoughts: What the Internet Tells us About Sexual Relationships*. London: Penguin.

<sup>2</sup> 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*.

<sup>3</sup> Department for Digital, Culture, Media & Sport. (2017). *Impact Assessment (IA)*.

networks, offline storage media, and cyberlocker services can 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”.<sup>4</sup>

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 further shows 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 impact on 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”.<sup>5</sup>

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

---

<sup>4</sup> 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*.

<sup>5</sup> <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 on 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”. 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 directly prescribed by legislation, with clear aims that blocking could reasonably be expected to achieve, should devolve responsibility to private companies, and should 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:



“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”.<sup>6</sup>

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 paper on the possession of extreme pornographic material — 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”.<sup>7</sup>

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

---

<sup>6</sup> Home Office. (2005). *Consultation: On the possession of extreme pornographic material.*

<sup>7</sup> Home Office. (2005). *Consultation: On the possession of extreme pornographic material.*

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.

**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.<sup>8</sup>

***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.*

---

<sup>8</sup> Department for Digital, Culture, Media & Sport. (2017). *Impact Assessment (IA)*.

## 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 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.<sup>9</sup>

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

---

<sup>9</sup> <https://www.theyworkforyou.com/lords/?id=2017-03-20b.64.0>

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,<sup>10</sup> as well as to teenagers attempting to bypass the restrictions. There is a great deal that could potentially go wrong.

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.<sup>11</sup>
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.

---

<sup>10</sup> 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.

<sup>11</sup> 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>

### 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').
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.<sup>12</sup> 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.

---

<sup>12</sup> 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

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.

#### 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.<sup>13</sup> 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

---

<sup>13</sup> <http://www.bbc.co.uk/news/technology-34044506>



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.

Another approach could be to base regulation on an official ICO Code of Conduct.<sup>14</sup> 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.

---

<sup>14</sup> “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/>

**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.*

## 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.<sup>15</sup> 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)

---

<sup>15</sup> Germany has an age verification regime, but this only applies to German users accessing sites hosted in Germany.

- 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)

#### 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 ancillary 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 ancillary service provider set out in Chapter 3?

### Issues raised by considering social media platforms as ancillary service providers

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.<sup>16</sup> 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.

---

<sup>16</sup> 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*.

**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 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 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.*

**Title:** Parent Zone Response to BBFC consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers

**Date:** Monday, 24 April 2018

### **1) Introduction**

Parent Zone specialises in providing support to parents and families grappling with the challenges that are caused or amplified by the digital age.

**Our mission is to make the internet work for families.** We represent parents on the executive board of the UK Council for Child Internet Safety and reach over 2million families a year through initiatives like [www.parentinfo.org](http://www.parentinfo.org) (our free newsfeed service for schools delivered in partnership with the CEOP command of the National Crime Agency), *Digital Parenting* magazine (in partnership with Vodafone), and *Be Internet Legends* (in partnership with Google), a pupil facing primary school initiative teaching children how to stay safe and have fun online.

Through our research, parent services and work with schools, we have an in depth understanding of the difficulties families and the professionals that surround them face as they navigate their way through and in online spaces.

Our response to this consultation focuses on the areas about which we have specific expertise. It does not address broader questions and concerns.

### **2) Do you agree with the BBFC's Approach as set out in Chapter 2?**

Parent Zone is broadly supportive of the approach. Parents rightly expect that the laws that apply in the offline world are also applied online. We frequently hear from parents who have been faced with the difficult task of explaining pornography to younger children who have come across it accidentally.

Whilst we recognise that a proportionate approach needs to be taken, we are concerned that not all sites and services distributing pornography will be dealt with equally. Parents are unlikely to understand that some pornography is still readily available through – for example – social media platforms or via smaller commercial providers. Clear communication to parents about what is and what is not going to be within scope will be essential if this approach is going to achieve the desired outcome. It will also be crucial to deal with non-compliant sites quickly in order to maintain parental confidence and to monitor which sites children are visiting. We would anticipate that older children will migrate to different sites and services and that new services will emerge. This is something that we would hope the regulator will proactively monitor.

### **3) Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?**

The standards set out in Chapter 3 appear sensible and practical. Our primary concern would be that due regard is given to how easy it is for a child to access or fake age verification. Low tech solutions, whilst attractive for data minimisation



purposes are also easy for children to 'borrow'. What '*cannot be reasonably known by another person, without theft of data or identification documents or readily predicted by another person*' needs to be interpreted in the context of family life. We further hope that proper regard is given to the inclusion of '*measures to reduce the potential for improper use, in particular by children, of a verified account*'. For example, we would want sites to log users out after sessions and not allow users store their user name and password for automatic completion.

END

## **PSHE Association response to the BBFC Digital Economy Act consultation April 2018**

### **Background**

1. The PSHE Association is the national body for personal, social, health and economic (PSHE) education in England, providing advice and support to a network of over 20,000 teachers and other professionals working in schools nationwide.
2. PSHE education is a non-statutory curriculum subject which covers the knowledge, skills and attributes all pupils need to develop in order to keep themselves healthy and safe and to prepare them for life and work in modern Britain. Evidence shows that well-delivered PSHE programmes have an impact on both academic attainment and non-academic outcomes for pupils, particularly the most vulnerable and disadvantaged<sup>1</sup>.
3. The PSHE Association works to ensure that all schools can provide every pupil with the knowledge, skills and attributes they need to keep themselves healthy and safe, and succeed personally, professionally and academically.
4. PSHE education includes relationships and sex education. High quality PSHE education includes learning to help young people navigate a world in which online pornography is prevalent. This will include specific learning about pornography, for example exploring differences between sex portrayed in pornography and most people's real sex lives, as well as implicit, supportive learning, for example, understanding consent, equality and the features of positive relationships.

### **Support for age verification of pornography**

5. The PSHE Association welcomes the introduction of the age verification requirement for pornographic websites in the Digital Economy Act and the BBFC's role as a regulator. Research indicates excessive use of pornography can affect young people's relationship satisfaction, sexual satisfaction, body satisfaction and increase sexual preoccupation<sup>2</sup>. We therefore consider youth access to pornography to be a public health issue. This requires a multi-modal response, including quality PSHE education covering a wide range of issues including relationships and sex, media literacy and gender equality.
6. Steps to reduce young people's ease of access to online pornography are a necessary part of this public health response for two key reasons:

---

<sup>1</sup> [Curriculum for Life: the case for statutory PSHE education](#) PSHE Association

<sup>2</sup> Peter J & Valkenburg PM (2008). Adolescents' exposure to sexually explicit internet material and sexual preoccupation: A three-wave panel study, *Media Psychology*

Peter J & Valkenburg PM (2009). Adolescent's exposure to sexually explicit internet material and sexual satisfaction: A longitudinal study. *Human Communication Research*

Vanderbosch L & Eggermont S (2014) Sexualization of adolescent boys: Media exposure and boys' internalization of appearance ideals, self-objectification, and body surveillance. *Men and Masculinities*

- i. Pornography is a poor, and potentially dangerous, sex educator. It should not be seen as a reliable source of information or inspiration for young people.
- ii. Age verification sends a clear message that there is social consensus that pornography is a product for adult consumers

### **Pornography as a poor sex educator**

7. As an education charity and the national body for PSHE education, we are primarily concerned about online pornography because it is a poor, and potentially dangerous, sex educator. It is natural for young people to be curious about sex but pornography should not be where young people develop their knowledge and understanding of sex, nor attitudes and behaviours towards sexual partners.
8. Pornography frequently provides unrealistic portrayals of sexual activity and sexual practices based on male dominance and, sometimes, aggression against women<sup>3</sup>. As researcher Rebecca Whisnant has written, 'Consumers of [mainstream] pornography routinely see women treated in ways that most people would neither accept for themselves nor accept for those they care about.' It also rarely presents sex alongside critical aspects of positive relationships, such as intimacy. This narrow and often distorted view of sex will not prepare young people to develop and maintain healthy sexual relationships. Despite this, a proportion of young people may get their first knowledge and experience of sex from watching pornography and, if this is not counterbalanced by high quality PSHE in schools, this may influence their relationships for the long term.
9. We want all young people to receive education about sex from high quality PSHE in schools, as a statutory entitlement. This is as well as, not instead of, information, advice and support from their parents or carers. There is strong evidence for the value of school based PSHE in supporting young people to have more positive and safe sexual relationships throughout their lives. The National Survey of Sexual Attitudes and Lifestyles (NATSAL)<sup>4</sup>, for example, found that adults who reported school lessons as their main source of sex education (vs. friends/other sources) were more likely to be 'sexually competent' at first sex, i.e. less likely to report first intercourse before age 16, more likely to report that at that time: a reliable method of contraception was used; that the timing felt right; that the decision to have sex was an autonomous one and that both partners were equally willing.

### **Age verification as a message**

10. Currently pornography is easily accessible by young people online. Their natural interest in sex can lead to them finding and accessing pornographic content in a few clicks. They may be inadvertently exposed to pornography in the course of internet browsing, or

---

<sup>3</sup> Klaassen MJ & Peter J (2014). Gender (in)equality in internet pornography: a content analysis of popular pornographic internet videos. *The Journal of Sex*

<sup>4</sup> Macdowall W, Jones KG, Tanton C, *et al* Associations between source of information about sex and sexual health outcomes in Britain: findings from the third National Survey of Sexual Attitudes and Lifestyles (Natsal-3) *BMJ Open* 2015;

actively sent links to pornographic websites by peers.<sup>5</sup> Age verification will introduce a boundary. This may not be insurmountable for some young people but it remains worthwhile. As well as reducing ease of access to pornography, age verification sends a clear societal message that pornography is a product for adults.

11. This message is important because it helps to set out a social norm. Societal norms have a real impact on how we behave. The smoking ban, for example, has taken a commonplace activity – indoor smoking in public places – and made it almost unimaginable.
12. High quality PSHE education is delivered within the prevailing social norms of the day. PSHE presents young people with the opportunity to explore social norms, to understand why they might exist, how they fit with their beliefs and values, and to challenge them where necessary. The current norm of near unrestricted access to pornography online is inimical to the interests of young people.
13. PSHE must take a non-judgemental approach, and teachers must recognise that young people in their class may access pornography, may enjoy it or may have conflicting feelings about it. Age verification will enable teachers to situate education within a broader social context with clear boundaries around pornography. It will enable teachers in schools to point to a clear social consensus and discuss it, explore the reasons why and help young people to navigate this complicated online media landscape.
14. We believe this is a proportionate and necessary response to a public health issue. We also believe this is what the majority of young people themselves want and expect to see from the adults around them.

---

<sup>5</sup> Martellozzo E, Monaghan A, Adler J, Davidson J, Leyva R and Horvath M (2017) *I wasn't sure it was normal to watch it*. Report for the NSCCC and the Office of the Children's Commissioner

# RESTRAINED ELEGANCE: FETISH PHOTOGRAPHY AND ROMANTIC BAREFOOT BONDAGE MAGAZINE

## Response to BBFC consultation on Age Verification

I have many concerns with the wording and intention both of the Digital Economies Act and the BBFC proposals for how they should be implemented. I have attempted to cover the major concerns here in brief.

### Privacy

The privacy protections in the act and the consultation appear wholly inadequate. We are speaking here of creating a nation-scale database of people's entirely **legal**, but also entirely **private**, viewing habits. Suicides in the aftermath of the Ashley Madison hack <http://www.bbc.co.uk/news/technology-34044506> and the concerns about subversion of electoral processes by data collected by Facebook and Cambridge Analytica should surely serve as stark warnings that this aspect of the regulations must be looked at again. This is especially true given that the business model of some of the providers implementing large-scale age verification solutions is based on advertising, and therefore relies heavily on correlating and tracking visitors as they navigate online to target those adverts. I believe most people have a reasonable expectation of privacy when they visit a legal adult entertainment website. How is that expectation to be met if a secondary service provider (the age verifier) is correlating their porn viewing habits with their other online activity in order to cover their costs and make a profit?

### Right To Appeal

Little mention is made in the proposals of rights of appeal. This procedure needs to be laid out in detail, with an independent appeals authority, and a light-weight system for quick response to prevent unwarranted censorship and the closure of businesses pending appeal.

Previous attempts at internet regulation in the UK included ATVOD deciding that a one-man-band operation was somehow operating a television on demand service in competition with Sky and the BBC. The appeals procedure was unfair in that the service was required to be taken down pending appeal, ensuring complete loss of customers so that even once a successful appeal was made a year later, the business in question had already collapsed. (The ATVOD procedure was so flawed that the organisation was wound up).

Given that the new regulations treat the digital equivalent of the local corner store on the same footing as Pornhub and Playboy, what will the appeals procedure be? What consideration will be given to allowing the continued existence of the disputed website pending appeal? What guarantees will be made on the independence of the appeals panel and the speed of the process?

### The Scale of the Operation

There are 1.8 billion websites in the world (<http://www.internetlivestats.com/total-number-of-websites/>) of which 200 million are claimed to be currently active. In principle, each of these must be at least visited by BBFC inspectors to ensure that they are either non-adult in nature, non-commercial (presumably including any advertising), or if they do contain some commercial adult material, hold them behind a compliant age verification wall.

No serious consideration seems to have been given as to how a small organisation like the BBFC will be able to apply these regulations in anything like an even-handed manner given the scale of what is proposed.

Will automated or semi-automated searches be used to locate potentially infringing websites? This immediately falls foul of the Scunthorpe Problem (named after automated blocking by AOL's profanity filter prevented people from sCUNThorpe from making accounts on AOL, [https://en.wikipedia.org/wiki/Scunthorpe\\_problem](https://en.wikipedia.org/wiki/Scunthorpe_problem) ).

The BBFC propose to start with sites which are “most frequently-visited, especially by children”, which seems at face value to be sensible. Unfortunately, on reflection, both halves of the sentence are problematic. It is hard to establish traffic levels robustly, and how on earth are the BBFC proposing to identify sites visited by children in an ethical manner? And **all** websites are available worldwide, unless blocked by national level firewalls.

All websites serve British customers and there is no reliable way of a small business in (say) Nevada choosing to disallow visitors from Britain. They can decline to admit customers into paid areas on the basis of credit card address details, but that's never been any sort of problem anyway. At worst they may need to disallow the tiny fraction of payments made by debit card rather than credit card. This may be an issue to sites in Germany where credit cards are less used, but in the English-speaking world, credit card payment is almost universal and age verification to access the paywalled area is already the de facto standard (and has been for two decades).

The problem is trailers and the free area. There is no way for the Nevada producer to show legal-in-the-USA preview material to US customers but require UK customers to age verify first. Indeed, age verification systems required for UK compliance may be illegal in other jurisdictions given the lack of privacy protections. How can a small business obey mutually contradictory regulations coming from different countries?

Geotagging methods are haphazard and unreliable at best, and are also immediately defeated by any form of redirection ranging from simply telnetting to a machine in Spain and popping up a window back on your local machine, through virtual private networks (often used for legitimate purposes such as logging into commercially-sensitive corporate intranets while an employee is off site) to freely-available tools like TOR.

How is a small business operator in Nevada meant to comply with local and UK regulations if they cannot adjudicate the country of origin of an incoming HTML request? Doing so is beyond the capabilities of Netflix and the BBC, so what hope does a Swedish webmaster or a part-time performer in Amsterdam have of complying?

And why should one small business in Nevada have to endure the commercial burden of obeying UK regulations and paying to age-verify his potential customers so they can view his previews when his neighbour, whose site the BBFC have decided does not qualify as “frequently visited” and therefore do not propose to inspect, does not? Both will very likely be doing their best to comply with their local regulations already, but one is suddenly landed with a disproportionate foreign regulatory burden and the other is not.

They cannot even choose to age-verify only potential customers coming from the UK, since there is no robust method of geo-tagging by IP address that is not trivially defeated by redirection.

What in fact is likely to happen is what happened with ATVOD- site operators will keep their heads down in order to try to avoid notice, the regulator will pick on a small fraction of

operators essentially at random, and impose regulatory burdens on them which are not suffered by their competitors, putting the unlucky few at a serious competitive disadvantage, likely putting them out of business pending appeal.

The largest players who can afford to handle the requirements of verification on an industrial scale will rub their hands together in glee at the hope of putting their competitors- the small, diverse, boutique adult producers we'd presumably like to encourage- out of business.

The BBFC document simply fails to appreciate that the scale of the problem- 200,000,000+ active websites in the world- is out of all proportion to anything the organisation has ever dealt with before.

For example, in 2016 the BBFC classified 1075 cinema films, 8201 videos and 74 music videos. That's of order of 30 classifications a day. Websites are currently being created at the rate of 1 per second- 86,400 a day.

To enforce the regulations in an even-handed manner, every single one of these really ought to be inspected. And revisited regularly to prevent change of use, since unlike cinema films which are static objects (a film is not re-edited on a daily basis) websites can and do change dynamically all the time. Otherwise unscrupulous operators can just register "[www.MySewingWebsite.com](http://www.MySewingWebsite.com)" and use it to distribute porn- and if the regulators do chance upon it, will just switch domains to "[www.OurHillwalkingWebsite.com](http://www.OurHillwalkingWebsite.com)".

Estimates vary, but as many as 4% of websites might include adult entertainment, and therefore need more than a cursory inspection.

How do the BBFC proposed to organise the inspection of websites in a consistent and fair manner? At the very least, thresholds should be placed to exclude micro-businesses from unwarranted burden on the basis of hypothetical risk. It's not clear what a good and robust set of metrics for those standards would be, but excluding businesses below a certain number of employees, a certain turnover threshold, or some metric based on unique visitors per day would be a start.

We need something more rigorous and even-handed than "most frequently-visited" as a criterion and the BBFC needs to set this out publicly and transparently.

### **Metrics And Proportionality**

The act and the BBFC document appear to treat it as a given that viewing human nudity and human procreation when under the age of 18 is inherently harmful. Studies in this area are limited, with small sample sizes, questionable methodologies and contradictory results.

What steps are being taken to survey the extent of the problem in an impartial and rigorous way? We need data on the current extent of the problem, then we need metrics to quantify the reduction in harm as the regulations are rolled out, in order that we can evaluate their effectiveness. What metrics are proposed?

Since the UK's proposed solution is the imposition of ISP-level censorship, financial censorship, and potentially large fines, hadn't we better ensure that our approach is actually working, and that the harm caused to freedom of speech and the chilling effect of

self-censorship on already marginalised sexual minorities like the LGBT community and consensual BDSM practitioners sharing best practices online is actually accompanied by a positive effect on the problem the regulations are seeking to tackle?

Indeed, what steps are being taken to monitor the negative consequences of the regulations on freedom of expression and the provision of educational material by sexual minorities? Educational material is often made widely available on sites which also generate their income by sales of adult entertainment. “How to tie safely” videos on bondage websites, for example, and safe sex advice on gay sites. What attempt has been made to assess the chilling effect of regulation on these sources of information? Will they need to be placed behind age verification walls? A highly retrograde step if so, surely?

In short- what metrics are to be used to assess success, and to assess predicted negative consequences? How will it be determined whether these regulations are disproportionate or not?

### **Accountability**

The BBFC annual report mentions that the organisation regularly conducts public consultations to ensure its guidelines stay up to date with public expectations. However, recent legal cases such as that of Michael Peacock ([https://en.wikipedia.org/wiki/R\\_v\\_Peacock](https://en.wikipedia.org/wiki/R_v_Peacock)) show that at least as far as obscenity goes, the public’s view is significantly different from that of the authorities.

Given that the BBFC is now to be given sweeping powers to block free speech in the UK on the basis of subjective determinations of what constitutes 18-rated material or 18-R material, there needs to be a much more wide-ranging, active, ongoing and **transparent** procedure to keep these regulations up to date. What is the BBFC proposing to do in this area?

Remember that the scale of the operation is MANY orders of magnitude greater than anything the BBFC has previous tackled. The potential impact on free speech is therefore also much more severe, and it seems doubtful that current consultation structures will be adequate for the scale of the new endeavor.

If the BBFC is going to become the arbiter of free speech in the UK, are they to come within the remit of laws such as those governing freedom of information requests?

### **Specificity of Rules**

In the past, the BBFC has issued broad guidelines on what is likely to be considered at each level of classification, but the final classification of any work has always been made after viewing by human beings at the BBFC.

Detailed guidelines as to precisely what can and cannot be shown have never been issued.

Unless the BBFC is to recruit tens of thousands of new staff, they are going to be unable to inspect any meaningful fraction of adult websites. Given the typical scale of releases in the adult industry (many producers release a new product every day) it will not be possible for the BBFC to act in any advisory role in a meaningful way either.

Producers are left to guess what is and isn’t acceptable for publication on any given distribution channel. The most critical point where this matters is in knowing what material



is acceptable to distribute outside the age verification wall, and what must be restricted to within the wall.

For example, here are two still frames, drawn from trailers whose contents are rather similar.



Given a copy of the BBFC guidelines, can one determine if it is acceptable for the producer of an adult entertainment product to show the above stills on their free area or for publicity on public platforms such as Twitter? Or for the trailers from whence they come?

One cannot.

I chose these two examples with care to illustrate a problem caused by the lack of specificity in guidelines. Both show an attractive actress being tied up, against the will of the character they are playing (but of course consensually and professionally in a safe working environment in reality).

The top still is from an American bondage producer, and would presumably be rated 18, or possibly 18R, or possibly characterised as extreme porn because the actress has all four limbs bound and is gagged... even though no actual sexual activity takes place, and as far as I know no nudity is featured either (I haven't purchased the full film, just watched the trailer).

The bottom still is from the movie RED, rated 12 by the BBFC.

Which rating would apply to the trailer for the American bondage film? Extreme porn (illegal and banned), 18, 18R or rated 12? Would publishing it be permissible for advertising, and for publication on a website in a free preview area outside the age verification area?

If not, why not, since the above clip for RED is freely available on YouTube, and in any case was drawn from a movie which was only rated 12?

More critically, how could any producer possibly follow the rules and only publish acceptable material on their free preview area and publicity, if the rules are not detailed enough that one cannot make this determination given the above two images and a copy of the rules?

Given that a producer must make this decision for EACH new release, on a daily basis, how can they possibly attempt to ensure that their adverts, trailers and free preview areas are compliant with the laws without extremely detailed, unambiguous guidelines?

It is not a solution to require that all advertising or previews or trailers be behind age verification walls. The cost of age-verifying a viewer will either be non-zero (for a reputable age verification company making its money from providing a service) or zero, but with a stiff cost to the end consumer in terms of loss of privacy and risk of exposure of intimate details.

The average ratio of customers to viewers in any industry is high. Typical sales of fetish videos are in the tens to hundreds of units; typical followings on Twitter are in the tens of thousands. If it costs £1 to verify the age of each of 10,000 viewers to sell to 100 customers at £10 a unit, all small producers will be put out of business- the cost of age verification will rapidly exceed their turnover, by a factor of 10. Or they must turn their potential customers over to the mercy of advertising-based age verification operators, a dubious and unappealing proposition at best.

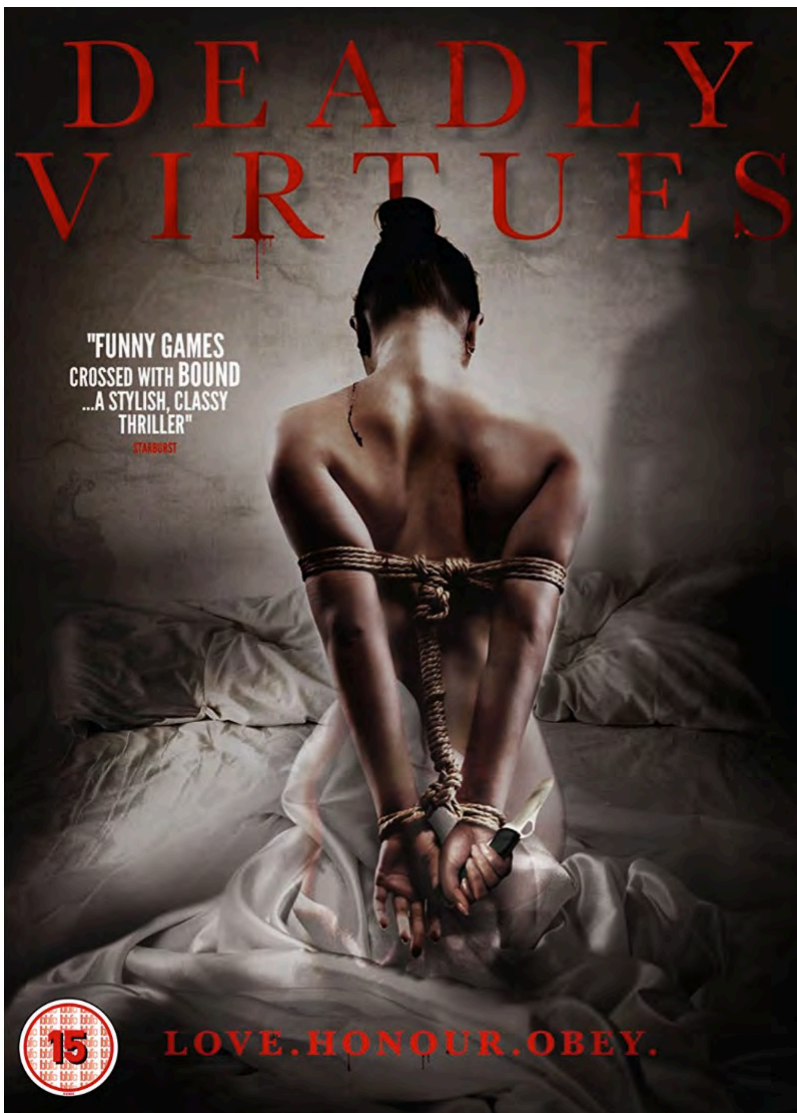


Society acknowledges this in mainstream films- we allow 12-rated trailers for 18-rated films, and sell 18-rated films in supermarkets with suggestive but allowable photographs on the cover.

To take a second example, the photograph above would be considered pretty extreme on a lot of BDSM websites- especially the knife held in the girl's hand, and what looks like a trail of blood on her shoulder.

The implication of violence, the blood, the (non-revealing, but clear) nudity... all would suggest an extreme porn image.

The producer of such an image might certainly consider keeping it behind an age verification wall, rather than putting it on the free area as a preview. And they might even self-censor, being unable to be sure whether or not it counts as extreme porn.



Actually, this image was on display at my local Tesco... at knee height.

It's the cover for a 15-rated movie, and was visible to passing toddlers.

As far as I know, there was no harm caused to anyone by its publication.

So if we are happy with this on the shelves at Tesco (which we should be), surely we should be happy with images like this on social media and as posters and previews for adult sites?

I defy anyone to classify the image according to BBFC guidelines and tell me whether or not it would be acceptable outside the age verification wall on an adult website, with reasoning that an impartial observer would be able to follow and verify.

## **The Difference Between Producers And Tube Sites**

Finally, I would just like to address the implicit idea that producers of adult entertainment are in any way targeting their products towards minors, as this seems to be an area of great misunderstanding.

Adult producers are also parents, carers, citizens, tax-payers and consumers. They have moral standards every bit as high - and occasionally of course as low- as everyone else's. From a moral point of view, few want minors to be consuming their wares, any more than the producers of "Deadly Virtues" want toddlers to watch their horror film. But, like the producers of "Deadly Virtues", they must showcase their wares in their shop windows in order to generate sales and make a living. "Deadly Virtues" did so in Tesco. Producers do so online on their websites in free areas and with trailers.

All reasonable producers would be willing to abide by sensible, consistent restrictions as to what they can display in their shop windows. They'd even do their best to do so country-by-country, despite the impossibility of verifying the geographical location of an incoming HTML request. (No such guidelines exist, certainly not for the UK). They keep the full versions of their products behind paywalls because that is how they make their money.

Payment for access to adult entertainment is overwhelmingly made by credit card, not debit card. Consumers are mostly savvy enough to know that all online purchases should be made via credit card, because of the greater consumer protection they provide. Existing paywalls are probably not perfect, but I would suggest that they already exclude almost all minors and could be tightened up if studies were to reveal that payment by minors using debit cards was actually a significant factor.

But note that minors would make extremely poor customers for adult producers. They have little disposable income, any payment methods they have are either illicit (stealing Dad's credit card) or of limited use online (debit cards), and they likely don't have the privacy at home to be able to consume adult entertainment. And since the vast majority of producers are reasonable human beings, the idea of kids watching their products is anathema.

The idea that producers are actually TRYING to sell to minors is far-fetched from both a moral and financial point of view. No producer has the slightest interest in minors viewing their material. They accept that some children may happen to view their preview material, as is the case for the extreme porn BDSM and blood image on the cover of Deadly Virtues and would be willing to work within a reasonable framework of restrictions on trailers, were any to be produced.

So how are kids going to view the full versions of these producers' adult entertainment products? What exactly is the problem here? Where does all this free porn come from?

- 1) By stealing Dad's credit card. Not likely to last long, and surely a parental issue not a governmental one. Age verification is of no help here, since if a card can be stolen, so can age verification credentials.
- 2) By getting access to material already legitimately purchased by an adult in the household. Again, a purely parental matter, and one which age verification online does not address.
- 3) By using their own debit card on the small number of sites which accept them. Possible, but are there any studies which indicate that this happens in significant numbers? Age verification would help here, but it is using a sledgehammer to crack a nut.

4) By viewing the material stolen and uploaded to a "Tube" site where it is made available for free to anyone.

This is the elephant in the room. Producers have been fighting an ongoing war against the tube sites for a decade or more, trying to stop copyright violation and piracy. Pirates post copies of a producer's material to tube sites without authorisation, giving away free what was previously only available behind a paywall.

THAT is how children access porn. All other channels are insignificant.

Perhaps if existing laws regarding copyright violation were used to prosecute those who operate and distribute stolen material from legitimate producers, tube sites would not be able to continue to steal traffic from paywalled sites by giving away their copyrighted material for free.

These sites have grown large on the backs of pirated material, so large that some of them are now in fact also legitimate producers. But their business model still revolves around advertising, selling visitor's eyeballs to advertisers.

It is they who have an incentive to display material to minors, because more visitors means more ad clicks which means more money. Unlike the original producer, their business model depends only on attracting more visits, not on convincing someone to pay for an adult entertainment product behind a paywall.

It is they who have an incentive to steal material, sucking in more visitors who previously would have had no option but to go behind the legitimate original producer's pay wall to view the products. They put cosmetic "complain and we'll take it down" measures in place so they can claim to be resisting piracy, but all adult entertainment producers know this is a sham. Videos get taken down on a complaint but are back up within hours. Many original producers are forced to hire specialist firms to try to combat the flood of piracy, and are losing the battle.

These sites are parasites on the legitimate industry of producing legal adult entertainment and it is they, not the original producers, who have created whatever problems might result from the free availability of adult entertainment online.

If one were to level the playing field by prosecuting the copyright infringement, removing all the stolen material from tube sites so it once again becomes available only behind existing pay walls, the problem of free porn would largely go away.

If one is serious about tackling minors viewing porn, prosecuting the pirates who make copyrighted material illegally available online would be a good start.

And being wary of allowing the most egregious example of a Tube site company built on piracy, MindGeek, to perform age verification and collect data on the private and intimate habits of a third of the UK population would probably be a wise second step.

## **CONCLUSION**

If we are going to insist on these ill-considered and draconian censorship measures to combat a problem whose existence is questionable, the least we can do is to come up with some reasonable and consistent guidelines for producers of legal adult entertainment to follow in order to know that they are within the law.

Furthermore, we must put in place swift and fair appeals procedures (to avoid putting legitimate small businesses out of business whilst enduring bureaucratic delays). We must insist upon transparent and wide-ranging public consultations on the standards, and produce rigorous, unambiguous guidelines for what is acceptable outside age verification walls and what has to be placed inside.

We must ensure the privacy of the estimated 20 million UK citizens who are likely to avail themselves of age verification systems. We must institute proper scientific studies into the harm caused to children by viewing different sorts of adult entertainment, and studies to assess any possible negative impacts on free speech and the chilling effects of the regulations on minority communities.

None of these concerns are adequately addressed by the recent BBFC proposals.

## **Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers**

Please find views on the draft Guidance from SWGfL

### ***Guidance on Age-Verification Arrangements***

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

Yes

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

Yes

Do you have any comments with regards to Chapter 4?

We foresee the creation of phishing websites that may emulate Age Verification appearance but purpose is simply to collect personal data (if individuals are familiar with sharing personal data to access content).

### ***Draft Guidance on Ancillary Service Providers***

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

Yes

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

Yes



# Consultation on BBFC Draft Guidance on Age-Verification Arrangements: Digital Economy Act - Part 3 Online Pornography

Response by Tara Beattie,\* Durham Law School

22 April 2018

## Do you agree with the BBFC's Approach as set out in Chapter 2 ("The BBFC'S Approach and Powers under Part 3 of the DEA")?

1. This submission raises a number of issues with the BBFC's proposed approach to assessing whether material is deemed "extreme pornography" under Part 3 of the Digital Economy Act 2017. This includes potentially falling foul of their legal obligations under the Act, and creating a situation of uncertainty for providers of online commercial pornography. A number of recommendations are made in the interest of avoiding these potential issues.

### *The importance of determining "extreme pornography" for the discharge of the BBFC's functions*

2. The BBFC will be responsible, in the first place, for identifying and notifying non-compliant providers of online commercial pornography under section 19 of the Digital Economy Act 2017 (DEA), as well as providing notice to payment-services, ancillary services providers, and internet service providers (section 21), requiring internet service providers to take further steps to prevent access to the offending material by persons in the UK (section 23); and for instituting civil proceedings for those who have had enforcement notices issued against them (section 19(11)).
3. Under section 14(1) DEA, a provider will be deemed non-compliant where they make pornographic material available on the internet in the UK, without securing that it is not normally accessible by those under 18. **The BBFC draft guidelines propose that one of the factors which it will take into account when deciding which services to investigate, for the purpose of prioritising protection of those aged under 18, is whether the service contains extreme pornographic material.**<sup>1</sup> This therefore requires the BBFC to assess whether material is deemed "extreme pornography" in the first place.<sup>2</sup>
4. In relation to sections 21 (notice to payment-service and ancillary service providers) and 23 (regulator power to require internet service providers to block access to material) of the DEA, **a provider will also be deemed 'non-compliant' where they make extreme pornography available on the internet to persons in the UK** (sections 21(1)(b) and 23(1)(b)), regardless of

---

\* Tara is a part-time tutor in Media Law, guest-lecturer in Law, Sex & Crime, and PhD candidate at Durham Law School. Her research focusses on extreme pornography regulations in England and Wales, is supported by an Arts and Humanities Research Council doctoral studentship award (Northern Bridge DTP). Prior to her studies, Tara worked as a project assistant at the Council of Europe's Equality and Human Dignity Department (Children's Rights). Website: <https://www.dur.ac.uk/law/staff/display/?id=15690>, Email: [tara.e.beattie@durham.ac.uk](mailto:tara.e.beattie@durham.ac.uk). The author would like to thank Kyle L Murray for his helpful comments on an earlier draft.

<sup>1</sup> BBFC, *Draft Guidance on Age-Verification Arrangements: Digital Economy Act - Part 3 Online Pornography* (March 2018) [2.5]

<sup>2</sup> See also *ibid*, [2.4]

whether the material is not normally accessible to those under the age of 18. The BBFC will accordingly be granted the powers mentioned in sections 21 and 23 not just in relation to those who fail to comply with section 14(1), but also those who provide extreme pornographic material online. Accordingly, the BBFC will also be required to assess whether material is deemed “extreme pornography” for these purposes.

5. It is therefore of utmost importance that the BBFC ensures a clear approach is taken when determining whether material shall be deemed to be “extreme pornography”.

### *Determining whether material is deemed “extreme pornography”*

6. Section 22 DEA 2017 determines that **the definition of “extreme” pornography is to be defined in accordance with sections 63(7) or (7A) of the Criminal Justice and Immigration Act 2008 (CJIA)**. The BBFC’s Draft Guidelines also acknowledge that extreme pornography is to be defined in accordance with the CJIA,<sup>3</sup> the relevant sections of which are provided in Annex 3.<sup>4</sup>
7. Section 63 Criminal Justice and Immigration Act 2008 defines “extreme” material in the following way:

*(7)An image falls within this subsection if it portrays, in an explicit and realistic way, any of the following—*

- (a) an act which threatens a person's life,*
- (b) an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals,*
- (c) an act which involves sexual interference with a human corpse, or*
- (d) a person performing an act of intercourse or oral sex with an animal (whether dead or alive),*

*and a reasonable person looking at the image would think that any such person or animal was real.*

*(7A)An image falls within this subsection if it portrays, in an explicit and realistic way, either of the following—*

- (a) an act which involves the non-consensual penetration of a person's vagina, anus or mouth by another with the other person's penis, or*
- (b) an act which involves the non-consensual sexual penetration of a person's vagina or anus by another with a part of the other person's body or anything else,*

*and a reasonable person looking at the image would think that the persons were real.*

Additionally, the materials must be considered to be “grossly offensive, disgusting or otherwise of an obscene character” (section 22(2)(b) DEA 2017; section 63(6)(b) CJIA 2008).

---

<sup>3</sup> *Draft Guidance on Age-Verification Arrangements: Digital Economy Act - Part 3 Online Pornography* (March 2018) [1.4]

<sup>4</sup> *Ibid*, 19-20 (‘Annex 3 - Definition of Extreme Pornographic Material’)

8. The BBFC's undertaking to determine extreme pornography in line with the CJIA's definition has been complemented with statements that they "will apply the standards [they] apply to pornography that is distributed offline", including "pornographic content [they] would refuse to classify".<sup>5</sup> **This could be suggestive of the view that material which the BBFC would refuse to classify as an R18, under its current guidelines for films and video works,<sup>6</sup> overlap fully, or sufficiently, with the definition of "extreme pornography" under the CJIA. To operate under this view would be incorrect.** Such an approach could also produce inconsistency and legal uncertainty - purporting to apply the CJIA standard of "extreme pornography", while in fact applying BBFC classification guidelines, would produce confusion, and unpredictability for providers in determining their obligations. It would also be contrary to the BBFC's legal obligations under the DEA (which, as stated above, require that the definition of "extreme" is limited to content described in sections 63(7) or (7A) CJ (section 22(2)(a) DEA))
9. For the sake of reference, the list of material considered "unacceptable" for classification by the BBFC is as follows:
- Material in breach of the criminal law, including material judged obscene under the current interpretation of the Obscene Publications Act 1959.
  - Material likely to encourage an interest in sexually abusive activity, which may include adults role-playing as non-adults.
  - The portrayal of sexual activity which involves real or apparent lack of consent. Any form of physical restraint which prevents participants from indicating a withdrawal of consent.
  - The infliction of pain or acts which may cause lasting physical harm, whether real or (in a sexual context) simulated.
  - Penetration by an object associated with violence or likely to cause physical harm
  - Sexual threats, humiliation or abuse which do not form part of a clearly consenting role-playing game. Strong physical or verbal abuse even if consensual, is unlikely to be acceptable.<sup>7</sup>

### *General observations*

10. The following draws out a general, overarching distinction between the CJIA definition of "extreme pornography", and material deemed unacceptable for R18 classification, and provides recommendations for avoiding unnecessary conflict between both.
11. As noted, the BBFC will not classify material which conflicts with the criminal law.<sup>8</sup> In particular, focus has been placed upon the relationship between the upper-acceptable limits of R18 classifications, and the criminal offence of publishing an obscene article under

---

<sup>5</sup> Cited in Damien Gayle, 'UK to censor online videos of 'non-conventional' sex acts' (23 November 2016, *Guardian*) <https://www.theguardian.com/technology/2016/nov/23/censor-non-conventional-sex-acts-online-internet-pornography>

<sup>6</sup> BBFC, *Guidelines* (2014). Available at: [http://www.bbfco.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014\\_0.pdf](http://www.bbfco.uk/sites/default/files/attachments/BBFC%20Classification%20Guidelines%202014_0.pdf)

<sup>7</sup> *Ibid*, 24

<sup>8</sup> *Ibid*, 3

the Obscene Publications Act 1959 (OPA).<sup>9</sup> This would be an unacceptable standard to maintain when determining whether material is considered to be “extreme pornography” under the CJIA definition:

12. For while it is generally thought to be the case that all material defined under the CJIA as “extreme” would also fall under the OPA definition of “obscenity”, the reverse does not hold true. Materials classified by the CJIA as “extreme” are subject to more restrictive requirements; foremost, they must fall under one of the listed activities in sections 63(7) and (7A), and be “explicit and realistic”. Caution must therefore be made so that the lower threshold of ‘obscenity’ under the OPA is not merely used to define “extreme pornography”. Therefore, and in order to be consistent with the CJIA definition of “extreme pornography”, **it is recommended that there be explicit acknowledgement of the need to depart from BBFC film/video work guidelines, and of OPA standards, when determining whether material is to be considered “extreme”, for the purpose of enforcing the Digital Economy Act.**
13. Regarding the practicalities of aligning definitions: in the past, the BBFC have encountered difficulties in aligning their standards, used for the purpose of R18 classification, and the contemporary practices of law enforcement agencies in relation to obscenity law. This is a matter which has been subject to judicial review,<sup>10</sup> and which resulted in the amendment of BBFC guidelines in 2000. Such amendment took place after extensive consultation with the relevant law enforcement agencies, and in light of the findings of a Home Office Consultation.<sup>11</sup> Since then, and according to Murray Perkins,<sup>12</sup> the BBFC has held numerous review sessions with the Metropolitan Police Service in order to ensure that the current prosecutorial practice for obscenity is reflected in the BBFC’s classificatory work.<sup>13</sup> Continued consultation and cooperation is crucial if the BBFC is to ensure that the standards it applies in R18 classifications mirrors the criminal law standards of obscenity.
14. Moreover, as the BBFC begins its work in determining what is deemed “extreme pornography” under the CJIA definition, there is again potential for conflict in understanding between the BBFC and current criminal law enforcement practice. Thus, **to ensure consistency in the standards used for determining “extreme pornography”, similar cooperation between the BBFC and those responsible for enforcing the criminal offence of extreme pornography possession under the CJIA 2008 is urged.**

### *Specific distinctions*

---

<sup>9</sup> *Ibid*, 24

<sup>10</sup> See *R v Video Appeals Committee of the BBFC, ex p BBFC* (2000) EMLR 850

<sup>11</sup> Home Office, *Consultancy Paper on the Regulation of R18 Videos* (September 2000)

<sup>12</sup> The BBFC’s ‘Head of the DEA’

<sup>13</sup> Murray Perkins, ‘Pornography, Policing and Censorship’ in Paul Johnson and Derek Dalton (eds), *Policing Sex* (Routledge 2012) 85-99, 93

15. The following draws out more specific distinctions between the CJIA definition of “extreme pornography”, and material deemed unacceptable for R18 classification; and provides recommendation for the purpose of avoiding unnecessary conflict between both.

16. *BBFC Guidelines (unacceptable material) - Material (including dialogue) likely to encourage an interest in sexually abusive activity which may include adults role-playing as non-adults (see above):*

- Such material is unlikely to fall under the CJIA definition of “extreme pornography”, unless the abuse involves violence significant enough to be considered “an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals”.
- While role-playing as non-adults may be considered to involve “non-consensual penetration” under section 63(7A) of the CJIA, it is questionable whether such would be considered “realistic” and, in particular, “explicit”. The Home Office Consultation on Extreme Pornography suggests that “realistic” depictions of activity would be those which “appear to be real and are convincing”, while an “explicit” depiction covers “activity which can be clearly seen and is not hidden, disguised or implied”.<sup>14</sup> On the basis of these definitions, adults role-playing as children is arguably neither a realistic nor explicit depiction of non-consensual sex. Furthermore, sexual activities falling short of non-consensual sexual *penetration* would not fall under the remit of the CJIA (section 63(7A)).

17. *BBFC Guidelines (unacceptable material) - The portrayal of sexual activity which involves real or apparent lack of consent:*

- Some such activity could fall under 63(7A) of the CJIA. It is to be noted, however, that section 63(7A) extends only to non-consensual penetration of the vagina, anus or mouth by a penis, or non-consensual penetration of the vagina or anus, by anything else. In contrast, the BBFC’s standard is much more extensive, seemingly including any non-consensual sexual activity.
- Moreover, there is a distinction between the BBFC’s requirement of a “real or apparent” lack of consent, and the CJIA’s requirement for there to be a “real or realistic” depiction of non-consensual penetration. It is noteworthy that the word “apparent” was removed and replaced instead with “realistic” during the passage of the Criminal Justice and Immigration Bill.<sup>15</sup>
- While the BBFC Guidelines further include “any form of physical restraint which prevents participants from indicating a withdrawal of consent”, it is unclear that removing the ability of a participant to withdraw consent would be considered “non-consensual” under the CJIA; and/or such may be considered an insufficiently “explicit” depiction of non-consensual penetration.

18. *BBFC Guidelines (unacceptable material) - The infliction of pain or acts which may cause lasting physical harm, whether real or (in a sexual context) simulated:*

---

<sup>14</sup> See Home Office, *Consultation: On the Possession of Extreme Pornographic Material* (August 2005) [38]. Available at: [http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/30\\_08\\_05\\_porn\\_doc.pdf](http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/30_08_05_porn_doc.pdf)

<sup>15</sup> See Criminal Justice and Immigration Bill Part 6, section 64(6). Available at: <https://publications.parliament.uk/pa/cm200607/cmbills/130/07130.43-46.html>

- Some such material may fall under section 63(7)(b) CJIA - an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals. There are two significant distinctions, however: the level of harm required, and the area of the body upon which harm must be inflicted.
- While the CJIA requires “serious injury” to be caused, the BBFC guidelines refer only to “the infliction of pain or acts which may cause lasting physical harm”.
- Additionally, infliction of injury is limited, in the case of “extreme pornography”, to three areas on the body. The BBFC guidelines *vis-à-vis* infliction of injury extend to any part of the body.
- Thus, while spanking which results in significant swelling, redness or bruising to the buttocks is usually considered unsuitable for BBFC classification,<sup>16</sup> these materials would fail both on grounds of the threshold of injury inflicted, and on the ground that the buttocks is not an area of the body listed under section 63(7)(b)). Injuries to areas of the body other than the anus, breasts or genitals would have to be deemed so severe that they could be considered life-threatening, under section 63(7)(a) of the CJIA.
- With regard to injury-infliction, the BBFC’s inclusion of “simulated” violence sits uneasily with the current understanding and use of section 63(7)(b) CJIA. As stated, the CJIA uses the relatively higher threshold of “realistic” depictions. Moreover, CPS guidelines on the CJIA now make clear that “it will generally not be in the public interest to prosecute serious injury cases unless there is some aggravating factor present”, including, *inter alia*, “[w]hether there is clear and credible evidence of the exploitation of those depicted in the images”.<sup>17</sup> This suggests a particularly high threshold for serious injury cases, overall.

19. *BBFC Guidelines (unacceptable material) - Penetration by an object associated with violence or likely to cause physical harm:*

- Some such material would be likely to fall under section 63(7)(b) CJIA, subject to the requirement that the penetration is explicit and realistic.
- There is an issue, however, surrounding the definition of an object “likely to cause physical harm”, particularly in relation to acts of fisting (the insertion of the hand into the anus or rectum). While the BBFC have frequently demanded cuts to scenes of fisting,<sup>18</sup> the CPS have now made clear that, for the purposes of the CJIA, “[i]t is likely to be difficult to prove that cases of ‘fisting’ involve images that show activity that is likely to result in serious injury”.<sup>19</sup>

20. *BBFC Guidelines (unacceptable material) - Sexual threats, humiliation or abuse which do not form part of a clearly consenting role-playing game:*

---

<sup>16</sup> See e.g. BBFC, *Releases: DEBBIE DOES SPANKING 2 [Cuts Substituted]* (22 May 2005). Available at: <http://www.bbfc.co.uk/releases/debbie-does-spanking-2-2005-0>

<sup>17</sup> Crown Prosecution Service, *Legal Guidance: Extreme Pornography*. Available at: <https://www.cps.gov.uk/legal-guidance/extreme-pornography>

<sup>18</sup> See e.g. BBFC, *Releases: KILLERGRAM - ALL GIRL ANNIHILATION [Some Cuts Substituted]* (18 March 2008) Available at: <http://www.bbfc.co.uk/releases/killergram-all-girl-annihilation-1970-0>

<sup>19</sup> Crown Prosecution Service, *Legal Guidance: Extreme Pornography*. Available at: <https://www.cps.gov.uk/legal-guidance/extreme-pornography>

- Some such material may fall under several of the listed “extreme” activities under the CJIA: for example, forcing an individual to engage in sexual activity through threats with deadly weapons could be considered a life-threatening act under section 63(7)(a). Further, material which depicts an individual being forced to engage in sexual acts with an animal (as covered by section 63(d) CJIA) could conceivably be classified as “humiliation”. Meanwhile, sexual abuse, if laced with physical violence, could be considered an act which risks serious injury (under section 63(7)(b) CJIA).
  - However, much humiliation, and all abuse which does not reach a high threshold of physical violence would be excluded. “Strong (...) verbal abuse”,<sup>20</sup> in particular, would be excluded.
  - The BBFC threshold of materials which “do not form part of a clearly consenting role-playing game” seems to fall foul of the CJIA standards of “realistic” depictions of non-consent: where it is “not clear” whether what is being depicted is consented-to, it does not, logically, follow that there is therefore a “realistic” depiction of *non*-consent.
21. Finally, the use of several bodily fluids in sexual activity (including urine, excrement, blood and vomit) are regularly considered unacceptable by the BBFC. In particular, and most controversially, submissions depicting “female ejaculation” have commonly required cuts, on the basis that these are considered by the BBFC to depict, or appear to depict, urination.<sup>21</sup> It is clear that this material would be highly unlikely to be considered “extreme pornography” under the CJIA.
22. In light of the above, and in the interest of clarity, **it is recommended that the BBFC establish guidelines for materials that are considered “extreme” pornography, for the purposes of enforcing the Digital Economy Act 2017. These should mirror CPS legal guidance, and other related guidelines and standards, of the current understanding of “extreme pornography” under sections 63(7) and (7A) of the CJIA 2008.**

### *Conclusions and recommendations*

23. There are a number of significant distinctions between the BBFC standard of material that is unacceptable for classification, and the CJIA standard of “extreme pornography”. For the purpose of enforcement under Part 3 of the DEA, following the definition as set out by sections 63(7) and (7A) of the CJIA is required by law (section 22 DEA). It is also preferable to do so accurately, from the perspective of preserving consistency and legal certainty.
24. **While a comprehensive overhaul of the area, which reconsiders and synchronises the varying standards of obscenity, ‘extreme pornography’, and non-classifiable material, would be ideal, it is accepted that this lies beyond the remit of the BBFC and of this consultation. At a minimum, therefore, the following recommendations are made:**

---

<sup>20</sup> BBFC, *Guidelines* (2014) 24

<sup>21</sup> See e.g. BBFC, *Releases: MORE OF WHAT WOMEN WANT* (2001) Available at: <http://www.bbfcc.co.uk/releases/more-what-women-want-2001>

- That it be explicitly and formally acknowledged that there is a need to depart from BBFC film/video work guidelines, and of obscenity standards under the Obscene Publications Act 1959, for the purpose of determining whether material is to be considered “extreme” under the Digital Economy Act 2017 ([12], above).
- That specific guidelines for material which the BBFC considers “extreme” under the Digital Economy Act are established. This should mirror legal guidance on the current understanding of “extreme pornography” under the Criminal Justice and Immigration Act 2008 ([22], above).
- That ongoing cooperation between the BBFC and law enforcement agencies is established, in order to ensure consistent, cohesive standards are used when determining “extreme pornography” under the Digital Economy Act 2017 ([14], above).



## UNDER AGE SALES LTD/AGE CHECK CERTIFICATION SCHEME - ORGANISATION

Dear BBFC,

Thank you for providing us with the opportunity to comment on your draft guidance on age verification arrangements under Part 3 of the Digital Economy Act 2017.

We are a social enterprise that specialises in support to providers of age restricted goods and services. We provide accredited training, point-of-sale materials and mystery shopping services. We are also appointed as the auditing body for the UK's Proof of Age Standards Scheme (PASS) which is endorsed by the Home Office, Chartered Trading Standards Institute, National Police Chiefs Council and the Security Industry Authority. Our compliance and audit team consists of fully qualified trading standards professionals. We are not a provider of online age verification services or proof-of-age cards or systems, making us uniquely placed to provide an independent and impartial view on age verification arrangements.

Please find enclosed our confidentiality statement, but we are content for you to publish any of our response and we intend to put our response on our website at [www.underagesales.co.uk](http://www.underagesales.co.uk).

### General Observations

As a general observation, we are supportive of both guidance documents that you have released for consultation. We feel that they strike the right balance for determining the types of arrangements for making pornographic material available that BBFC will treat as complying with section 14(1) of the Digital Economy Act 2017.

In placing the guidance before Parliament, we strongly recommend that BBFC make reference to the guidance being drafted in accordance with the Government's [Regulator's Code](#).

Broadly, we think that these guidance documents have been prepared in accordance with the provisions of the Regulator's Code, so being able to claim conformity to it will be relatively straightforward. It will assist BBFC with the credibility it needs to demonstrate that its approach to regulation is in accordance with the government's wider policy of ensuring that regulators carry out their activities in a way that supports those you regulate to comply and grow.

In having regard to the Regulator's Code, we urge you to embrace the principle of **earned recognition** as set out in paragraph 3.4 of the Code:

3.4 Regulators, in making their assessment of risk, should recognise the compliance record of those they regulate, including using earned recognition approaches and should consider all available and relevant data on compliance, including evidence of relevant external verification.

The principle of earned recognition will provide BBFC with a method to prioritise resources to tackling non-compliance by providers of online services, whilst leaving broadly compliant providers to largely self-regulate their activity. An example of earned recognition would be compliance with the new **PAS 1296:2018 Code of Practice for Online Age Verification** published by the British Standards Institute and Digital Policy Alliance. In our view, to earn recognition through compliance with PAS 1296:2018, claims of conformity will need to be externally verified by an independent third party scheme.

As the existing appointed Audit Body for the UK's Proof-of-Age Standards Scheme (PASS), I am pleased to be able to advise you that we are currently exploring extending our scope to provide an independent third party certification scheme for claims of conformity under PAS 1296:2018. Our approach will be in accordance with the guidance issued by the International Standards Organisation (ISO 17067) providing a full independent certification process with appropriate impartiality and quality controls. In due course, our intention would be to work with UKAS, BSI and the DPA to establish PAS 1296:2018 (or a further iteration of it) as a new area of assessment, which would enable us to bring our proposed certification scheme within formal accreditation under ISO 17065:2012. This process can take upwards of two years to complete.

However, in the meantime, we plan to establish the certification scheme in readiness for future UKAS accreditation but as an 'other party' validation scheme under s.9.3.3 of PASS 1296:2018. More information about our proposed scheme will shortly be available on [www.accscheme.co.uk](http://www.accscheme.co.uk) - but we plan to develop this in cooperation with the industry stakeholders and BBFC as the regulator.

It would be our intention that a certificate of conformity provided by us to an age check service providers would state:

"Age check services provided by [identification of the claimant] in accordance with PAS 1296, are Age Check Certification Scheme (ACCS) validated."

In our view, a certificate of conformity provided by the Age Check Certification Scheme, ought to be sufficient evidence of earned recognition for BBFC. We would urge you to include this possibility within your guidance for businesses. Of course, it is open to others to come forward with their own third party certification schemes and we would not seek exclusivity. However, we believe that we are uniquely placed as the existing independent third party provider of audit services to the Proof-of-Age Standards Scheme.

To gain your confidence in our approach to certification and in accordance with the guidance under ISO 17067, we would offer BBFC as the regulator a seat on the formal Impartiality Committee that will be established to oversee the scheme. We will remain independent of the age check services industry.

We recognise the timescales for bringing the provisions of Part 3 of the Digital Economy Act into force and, with this in mind, we intend to open the certification scheme to applications from early adopters in May 2018. We would anticipate, therefore, being able to issue certificates of conformity during this year and in advance of Part 3 coming into force.

We would be willing to discuss this all with you in more detail.

## Guidance on Age-Verification Arrangements

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

Yes, we agree with the approach that you suggest. However, in section 2.5 we recommend that a factor that you ought to take into account is the principle of **earned recognition** as set out above in addition to the other factors already listed.

We are concerned that the guidance does not provide for BBFC to take urgent action where the circumstances would warrant it. We would strongly urge you to review the case of R v Glen Adaway [2004] EWCA Crim 2831 before establishing your enforcement policy. The guidance, as currently written, only envisages actions against what you might describe as online pornographic providers that have as an intention to comply, but fall short - thus requiring BBFC's intervention. The guidance, as currently written, may unduly fetter your discretion to act with urgency to deal with a scenario where the provider is established with no intention of compliance and simply to make a quick return and move on - this could have BBFC running round in circles hamstrung by your own guidance.

An example of this would be a provider that decides to set up a website, specifically targeted at school children, offering (let's say) 'teacher porn' in return for payment. This is set up, sweeps across social media (using 'click bait' approaches), has no age verification in place, is able to make a significant sum of money within days or weeks and is then shut down.

Applying your guidance to this scenario, you would not have the opportunity to take urgent action to cause the removal of such a service. We think that will unduly fetter your discretion as applied by the Adaway case.

We recommend that you retain a default authority under your guidance where you can take urgent action to deal with a circumstance where an online pornography provider has established themselves to **deliberately** target their service to children. In such circumstances, we would expect an accelerated range of enforcement actions to address that situation.

Of course, we hope that it would never arise, but to produce guidance on the basis that it would never arise would, in our view, be short-sighted.

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

Yes, we agree with the standards in Chapter 3. As set out earlier in our response, we believe that your guidance should make overt reference to the principle of **earned recognition** in accordance with the provisions of the Regulator's Code. Chapter 3 would seem to be the appropriate place to do that.

Do you have any comments with regards to Chapter 4?

None.

**Draft Guidance on Ancillary Service Providers**

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

Whilst noting that the list of potential ancillary service providers is not exhaustive, we would like to establish whether or not the Age Check Certification Scheme would or could be considered an ancillary service provider under s.21(5) of the Act. If it were, then the powers of direction for BBFC could be incompatible with the sovereign control of certification decisions that certification schemes must have under the provisions of ISO 17065. We would like to consider that more with you.

Firstly, in practice, we do not believe that this would be a problem in reality. If BBFC were to write to us (formally or informally) drawing a non-conformance of a certified provider to our attention, we would certainly act on that in accordance with the rules of the certification scheme.

Our issue, on protection of impartiality of the certification scheme, would be if BBFC were to direct the certification scheme to withdraw its services to the non-compliant provider exercising your powers under s.21 of the Act.

As such, we feel that your guidance, if indeed a certification scheme is regarded as an ancillary service provider, then specific provision should be made for BBFC notifications of non-conformance being made to the relevant certification scheme.

Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

Yes, we do agree with this.

I trust that our response helps you to further develop your guidance. We are, of course, happy to clarify any of the points that we have raised. We would also be keen to speak with you about the establishment of an Age Check Certification Scheme.

Best Regards

Tony

**Tony Allen**

Chartered Trading Standards Practitioner

Specialist Emeritus Advisor | Under Age Sales Ltd

[www.underagesales.co.uk](http://www.underagesales.co.uk)

Broadstone Mill | Broadstone Road | Stockport | SK5 7DL | 0345 257 0018 | 07802 978749

Registered in England | 07357348 | VAT Registered GB 996 2087 72

## DEA Consultation – Guidance on Age-Verification – BBFC

We welcome the appointment of the BBFC and the opportunity to comment on the draft guidance.

### Comments:

#### 1. Introduction:

**Sections 1.1 – 1.6** Although much is made of the process of AV and prevention of access by children this needs to be balanced against the fact that those who are over 18 need to have an environment that allows them easy access to Adult Content.

We welcome the powers that the BBFC is proposing with regard to Payment Service Providers (PSP) withdrawing Merchant ID's and also ISP's making websites go dark, these sanctions have sufficient bite to make the regulation effective. However, such sanctions are potentially damaging if wrongly applied, we would hope that the BBFC would share with stakeholders the format of the notices including those to take websites off line and withdrawal of merchant id's for consideration. Also, although it is clear from the guidance how sanctions might be imposed however little or nothing is said of the process of reversing the process or appealing against the process. VeriMe as a provider of a robust methodology of AV will be seeking to work with websites that have problems to make those websites compliant and there needs to be a clear and transparent process of reversal. The sanctions of making a website dark or removing the ability to process payment cards are legally a very strong power to be able to exert therefore checks and balances need to be in place.

**Section 1.7** relating to good practice, it is VeriMe's belief that this needs to be fleshed out in greater detail as we are getting feedback from website owners who believe they are doing something that is going to be considered "robust" when in fact it is not.

**Section 1.11 – 1.12** VeriMe welcome the fact that there is going to be an Annual Report and assessment to the effectiveness of the regulation. We would ask that this report be public and transparent and include stakeholder input, this allows for adaption and change based on performance and feedback.

**Section 1.13** VeriMe has some concerns with regard to this section and references it to ATVOD regulation and the loss of appeals that occurred with that regulation, the latter part of this section reads like a contractual obligation yet there is no contractual relationship between the 2 parties. (BBFC will not want to receive the mainstream criticism that ATVOD received by ATVOD for the quality of some of it's decisions). See references attached.

#### 2. The BBFC's Approach and Powers under Part 3 of the DEA

We are presuming the use of the phrase “Extreme Pornography” is referencing the definition from the Criminal Justice and Immigration Act

<https://www.legislation.gov.uk/ukpga/2008/4/section/63>

This definition is welcomed as reasonable and also reflects the position of the PSP’s under the Card Scheme rules.

**Section 2.1** Commercial Basis needs further clarification/definition.

**Section 2.2/2.3** welcomed.

**Section 2.4** the definition of services and the approach with regard to what is and is not included needs clarification and expansion. Similarly, having defined extreme pornography as being present will the website owner be given the chance to remove such content, will there be a process to provide intelligence to the BBFC either by whistle-blower and/or commercial competitors.

**Section 2.6** It has come to the attention of VeriMe that there is still considerable misunderstanding from the Card processing industry as to how this will affect them and that they have not prepared sufficiently for its implementation. The use of preliminary notices is welcomed and guidance on time frames that will be allowed would be welcomed as well as making these notices issued publicly available so that the website owners can be assisted to become compliant.

**Section 2.9** VeriMe welcomes the clarity on the use of Enforcement action however we would welcome expansion on how exactly the power of civil proceedings might be used and work, what is envisaged and under what circumstances.

### **3. Age Verification Standards**

**Sections 1 – 8** are welcomed however VeriMe feels these could be referenced against the PAS 1296.

**Section 3.9 – 3.10** The data industry is going through major change with the GDPR requirements and referencing the requirements of that legislation is welcomed. VeriMe are concerned about the swapping of data and credentials and how the robustness of methodology might fall short if such swaps take place. Care and Caution and guidance from the regulator would be welcomed, privacy notices on websites can clarify the use of the data but the regulator needs to determine what is good practice.

**Section 3.12** The definition of responsibility is welcomed however is it always going to be easy to find or engage with the “person that makes material available”? VeriMe assumes that all measures possible to make contact with said person will be taken. Can the BBFC reveal what measures it is envisaging in making contact with the responsible person i.e. email to [webmaster@website.com](mailto:webmaster@website.com) etc.....



#### **4. Data Protection and ICO**

**Section 4.1 – 4.2** are welcomed VeriMe specialises in the use of Mobile Phone to verify age and as such data is kept to the absolute minimum.

**Section 4.3** is welcomed save as to the fact that sufficient data needs to be kept to allow:

1. Customer Service – for example “why did you take £1 from my credit card and then refund it back to me”
2. Regulatory Audit: for example, “why did you let this person on this website on this day”

It is VeriMe’s opinion that confusion has occurred in the market place when the anonymisation of data has been mistook for “I am not required to keep records for the purpose of audit”

Section 4.1 – this hints at, without clarifying, what might be reasonable in the swapping of AV credentials as previously discussed in 3.9 – 3.10 clarification from either the ICO or BBFC is welcomed.

#### **Annex 1 & 2 & 3 Definition of Pornographic Material and Extreme Pornographic Material**

This would seem to be sufficient however a reference to the Obscene Publications Act might be helpful. Although our understanding is that very few if any prosecutions still take place it was an act that moved with societies mores.

There is some concern from VeriMe that the BBFC will be drawn into grading of material and drawing a line on what does and does not constitute extreme material, that would be detrimental to the process and what is trying to be achieved. It could become very time consuming for the BBFC and resource dependent. What is being proposed will be a huge task in itself, there should not be the distraction of taking on unnecessary responsibilities.

## Guidance on Ancillary Service Providers

This guidance is well constructed and welcomed.

A general point VeriMe would like to see the guidance future proofed to include such developing technologies as Crypto-Currencies, Phone payment/Near Field Billing, Virtual Wallets. The ability to widen the guidance to other forms of payment and media should be encompassed.

**Section 1.10** As previously stated, any reporting will need stakeholder input and transparency.

**Section 2.9** As previously stated the definition of the process of moving towards sanction is welcomed however clarity is needed with regard to appeal and reversal.

**Section 2.11** is welcomed especially the reference to search engine results and we believe that is how most children are arriving at the pornographic material. However, VeriMe questions how these goals might be achieved quickly and effectively in practice, perhaps the BBFC could spell out how this will work in the real world.

**Section 2.16** VeriMe would welcome an example as to what might be published and an indication of how frequently information will be updated.

**Section 3.3** VeriMe welcome this section however some indication of how the BBFC would seek to find the relevant parties and inform them would be helpful VeriMe can see this becoming a potential mammoth task and a resource hog/distraction.

In general, if a website is being looked at by the BBFC and considered compliant or non-compliant then VeriMe believes there are possible problems with such assessments as they represent a moving target. For example, will the BBFC be going into the sections of the website behind the paywall to look at material, if so are they going to pay or ask permission to enter?

Some websites are absolutely huge in terms of the amount of content contained. VeriMe can envisage circumstances where a website is attempting to be compliant and reacting to notices of inappropriate material from consumers and providers but could fall foul of an assessment. There would seem to be a need for an alternative "must try harder" type of notice where the website owner is trying to be compliant but falling short. It is VeriMe's opinion that this case should be considered differently to a website owner who is completely gung-ho and defiant of the regulations.

In conclusion this a good draft guidance, however not without problems and pitfalls that the regulator should avoid falling into. In an age where device convergence is more and more prevalent there is a necessity to clear up some anomalies like the VOD and AVMS legislation and definitions. The DEA offers a good opportunity for clarification with a unified approach across all platforms and media.

VeriMe would welcome a form of digital certification or license for being a compliant website if we could show this to clients/banks/advertising channels and get a clean bill of health this would be extremely useful, VeriMe don't think the current proposal/draft facilitates this.

We feel that this legislation has been a long time coming and it is over 2 years since initial meetings with the DCMS, all efforts should no be made to expedite this project to one of action, if there is anything VeriMe can do to facilitate this then please let us assist.

**References:**

<https://en.wikipedia.org/wiki/ATVOD>

<https://www.broadbandtvnews.com/2015/07/22/vice-wins-appeal-on-uk-vod-requirements/>

## **Yoti Consultation Response: Age-Verification Arrangement & Draft Guidance on Ancillary Service Providers**

### 1. Age-Verification Arrangements Comments

Yoti supports the recommendation that adult content providers should offer consumers a choice of suppliers and mechanisms to confirm age in a privacy preserving way to ensure a degree of consumer choice given the sensitive nature of verifying age to use adult content sites. We recommend a minimum of two suppliers and two approaches for a consumer.

The research that the BBFC undertakes should be published on the BBFC website to ensure that the public and industry can understand the BBFC rationale for deciding when certain AV methods are deemed compliant and others are not deemed compliant. Regulatory transparency improves consumer trust.

Central to the guidance, is the 'proportionate approach' to assess whether an AV arrangement complies with the provisions that pornographic material 'is not normally accessible' by those under 18 (Chapter 2). In our view, approaches must not be easily tricked or circumvented at low cost or with little investment of time by children. We believe Yoti's biometrics based method is both easy to use and robust, so less easily circumvented by both younger and older children.

In terms of the 'Age-verification Standards', Chapter 3, the guidance outlines that there will be 'effective and robust age-verification arrangements to ensure that the material is not normally accessible to those under 18'. Given the widespread availability of chat rooms and social media, we believe there will be instant sharing of any weak or vulnerable methods. Areas that the regulator will need to keep a close eye on in case of widespread abuse include:

- It is easy to obtain stolen credit card details [via online forums](#) and the same details could then easily be widely shared.
- Children may attempt to borrow username / passwords published online to circumvent the controls if just a username and password is sufficient to re-enter a site. Where there are no device limit thresholds this is more open to abuse.
- Adult operators should check that only one person can be logged in concurrently on one of their web sites or use a username and password in rapid succession. Clearly companies will need to use at least hashed usernames and passwords to carry out this check in an automated way that does not compromise privacy or security.
- Age verification suppliers must not allow multiple tokens to be linked to one username and password, where several people share the same username and password on an age-verification supplier website.

## 2) Principles

We commend the approach of the BBFC to adopt ‘a principle-based approach not normally accessible to under 18s... when assessing new age-verification arrangements’ and that it ‘shall maintain a dialogue with stakeholders’. It will be important for the BBFC to demonstrate that these principles are based on science and evidence, not perception or swayed by cultural bias.

One approach could be to devise criteria and a scoring matrix by which the solutions are assessed on an annual or bi-annual basis, with headings such as security, data minimisation, effectiveness, ease of spoofing and with optimal and minimal thresholds for success.

Publicly available Frequently Asked Questions will engender more trust in the BBFC approach and enable age verification providers, relying parties and the general public to understand the BBFC’s stance in a time efficient manner.

Notably, the recently published PAS 1296 Age Checking is not mentioned in the guidance. The PAS 1296 is agnostic of age band and of technology. It would be useful to signpost this document to relying parties, new age verification providers and interested parties in other jurisdictions.

## 3. Privacy

Key stakeholders are rightly concerned about the potential privacy impact the Digital Economy Act will have on consumers of pornography who are aged 18 or over. There is a fear that the new law will mean it is more likely that consumers’ pornographic consumption history will become public in the event of a data breach. There is concern that the use of user name and password solutions make this much more likely because of the ability of websites to track use against a user name (which potentially has personal data such as credit cards details logged against it). Ideally only an 18 plus attribute or token will be shared between the Age Verification Provider and the Adult site.

Therefore, our view is that the BBFC should stress more strongly the requirement on websites and age verification providers to take a data minimisation approach and to adopt strong security. Paragraph 7, Chapter 3 of the Guidance on Age Verification Arrangements uses the verb ‘recommends’ to suggest data minimisation standards. Our view is that the verb should be ‘**mandates**’ or similar. Yoti allows only an anonymous 18+ attribute to be shared with adult content sites.

Yoti verifies the user is genuine, but no other personal identity details are shared with the adult content provider, making it safer and more private than using a paper ID document, and limiting risk of personal identity exposure.

Neither Yoti nor the adult website accepting Yoti will have access to any information about the individual - except that they are over 18. Yoti is built with privacy by design:

- Yoti only keeps a copy of the ID document for up to 7 days after a user has registered while the account is proven genuine. The document image is then deleted.
- Once created ID details have been verified, Yoti does not see any personal details.
- Yoti doesn't see any of the information being shared between a business and customers, and can not track people's personal activity.

[For demonstration see <https://yoti-online-age-check.herokuapp.com/>]

Furthermore, we suggest that the BBFC spells out the criteria by which it will assess age-verification arrangements. There should be clearly defined criteria that age-verification arrangements must promote security, data minimisation and are not easy to circumvent. Paragraph 11, Chapter 3 of the Guidance on Age Verification Arrangements can perhaps be amended accordingly.

The BBFC should commit to reviewing the most popular age-verification solutions annually to ensure continued compliance to the above key criteria. Yoti would welcome a robust review of all age verification systems.

Like many other interested parties, we do believe that adult material on social media sites should be reviewed by the BBFC, given that they are clearly commercial platforms and there is a high volume of pornographic content on leading social media sites like Facebook and Twitter.

## 5. Accessibility

Increasingly in the UK both politicians and industry influencers are saying that the internet should not be the Wild West. Proof of age is required for a wide set of goods and services, and the Government is looking at further sectors such as corrosive liquids.\*

Yoti's solution allows people with identity documents [over 150 countries](#) - passports, national identity card and driving licenses to set up a Yoti to prove their age or identity. Hence foreign visitors to the UK (estimated at [4 million](#) per month) would not be excluded from verifying their age.

The standards of proof of age for goods sold online should, where practical, keep up with the standards expected in the offline world. In the UK there is no government identity card

scheme. So whilst providing age should be accessible to all; there is a tranche of the UK population who are not able to prove their age or identity. There is vastly different provision in Scotland, where all young people are issued with a proof of age, to the rest of England and Wales. We would support measures to democratise the provision of anchor identity documents across the UK. An unintended consequence otherwise could be that a adult householder may not in future have the documentary proof required to be able to access adult content or buy bleach for their bathroom...

## Summary

In conclusion, here at Yoti we are confident that our approach meets the requirements of the BBFC and consumers, in terms of providing a data minimised, privacy preserving approach. An adult can set up their Yoti in under 5 minutes linked to their Government issued identity document, free of charge. People take a selfie, complete a quick video test to prove they're a real person, and scan their passport or driving licence using their phone. Yoti verifies the selfie and ensures it matches the photo ID, verifies the integrity of the ID document and then creates a secure digital identity.

Then they can prove anonymously, by just sharing their over 18 token, that they are over the age of 18. They also have the freedom to use their Yoti in a wide range of contexts to prove their age or identity - for instance on nights out, in supermarkets, peer to peer on classified and online dating sites, logging into websites and to manage their passwords. Yoti uses 256 bit encryption to secure data. It puts individuals in control by giving them the only key to their Yoti.

Yoti supports the stance of child protection organisations, that the Digital Economy Act is designed to protect children from stumbling across age inappropriate content. [73%](#) of parents were concerned about their children accessing inappropriate material online (*Growing Up Digital report, The Children's Commissioner, January 2017*). Crucially, Yoti offers free age checks to all adult content sites regulated by the BBFC and complying with the UK's Digital Economy Act 2017.

\*Age Restricted goods and services in the UK include: ([https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/299373/13-537-code-of-practice-age-restricted-products.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299373/13-537-code-of-practice-age-restricted-products.pdf))

Aerosol spray, Air weapons and imitation firearms, Alcohol, Butane & Cigarette Lighter Refill, Cinema films, Crossbows, Caps, cracker snaps, party poppers, Fireworks, Gambling, Liqueur confectionery, National Lottery tickets, Petrol, Pets, Knives and Offensive Weapons, Scrap metal, Solvents, Sunbeds, Tattooing, Tobacco products, Video Works and Video Games.

## ANONYMOUS ORGANISATION #1

### **Feedback on BBFC consultation on draft guidance regarding age-verification arrangements**

Below is the feedback supplied by our client as of 6th April 2018:

While we applaud the intention of protecting children from inadvertent exposure to pornography, we think the proposals as drafted will cause significant harm to UK consumers, as described in detail below.

Unless these problems are rectified in a revised proposal, we suggest that the law will not receive the widescale support of the UK public which would be required for it to succeed.

### **Potential for criminality and fraud**

Internet users have long been advised, both by “fraud-aware” campaigns and the police, to be careful in sharing personal information on the Internet because of the risk of financial and/or ID or other fraud. Online blackmail where users are enticed to share personal identifying information along with inappropriate photos is also increasingly a problem (<http://www.bbc.co.uk/news/magazine-37735369>).

Currently, a consumer visiting an adult site that asks for “personal information” such as mobile phone, credit card, driving license or passport (for example), would be rightly concerned.

The guidance for establishing age verification arrangements for users now reverses the years-long advice, and instead anyone viewing adult sites is likely to be presented with a request for personal information. It will not be possible for the consumer to determine if the request is:

- a) A valid request in order to ascertain if the user is 18+ and allow them to view the pornography or
- b) A scam or fraud, e.g., intended to obtain personal information for purposes of ID theft, fraud, blackmail, unauthorised credit/mobile charges

Furthermore, given that there is no guidance on exactly what is considered a legitimate age verification exercise, there is no way for the consumer to understand whether what they are being asked for is legitimate, proportional or valid.

Such scams do not even need to be perpetrated by or with the awareness of the site owner since adult sites are already being widely hacked in order to distribute malware. Future hacks against adult sites will likely use legitimate looking “age verification” forms/pages as a vector for fraudulent/criminal activities.



Given that there are an estimated 5 million adult sites likely to fall under this legislation, and that many of these sites are operated by foreign actors with little regard for computer security, data privacy, customer protection etc. then this will be a huge concern for consumers visiting such sites.

The ICO will not have any ability to police this potential for consumer harm.

*The guidance, as currently envisaged, has potential to cause great harm to the 30 million individuals who are estimated to view pornography in the UK. The consultation period should be expanded and the ambit of those being consulted should be extended to specifically solicit feedback from those involved in protecting consumers from internet fraud, including the police, anti-fraud organisations and computer security experts.*

### **Lack of regulation of third party Age Verification Services and the inability of the ICO to police them**

Given that Age Verification Providers will not be regulated or subject to any form of approval, as mentioned above, there is no way to determine a legitimate age verification service from an illegitimate one, either by consumers or pornography providers.

Even if the Age Verification Provider is offering a “legitimate” service, many (all?) of those services currently proposing to offer such a solution to UK consumers are based overseas, often with obscure or hidden ownership.

Even supposing that the ICO had jurisdiction and made a determination against one of these services in the event of a hack or mis-use of consumer data, there would be no way to practically enforce any remedy or penalties against those responsible who are outside UK jurisdiction. The requirement for the provider to nominate an EU representative for GDPR purposes (even if followed) would not change this.

For this reason, there is also little incentive for these services to be incorporated or otherwise based in the UK since it would be a higher risk to operate such a service from within the UK than if it were based overseas. Legitimate UK businesses would therefore be discriminated against.

*The proposal should ensure that non-UK services are not afforded commercial/legal/operational advantages over UK based services. The ability of the ICO to effectively regulate non-UK actors must be considered as part of this.*

### **Risk to consumer of unauthorised or fraudulent charges**

Two methods of verification likely to be popular would be:

1. Requesting a PIN code or similar by text to an 18+ registered phone
2. Use of a credit card, in order to verify user is 18+

Both put the user at risk of unauthorised transactions such as credit card charges or premium rate text messages as part of the “verification” process (or subsequent to it). The guidance does not mention whether such a charge to a user is an acceptable part of an age verification process. Is there a limit to such a charge? Can the charge be repeated? Again, this puts the consumer at risk of harm/fraud unless, at the very least, the charges (including any repeat charges) are explained to users clearly and ambiguously before the start of the process.

*The Age Verification Regulator needs to provide guidance on the risk of unauthorised / excessive credit card or text message charges to prevent consumer harm.*

### **Potential discrimination against consumers by third party Age Verification Services**

There is no requirement that Age Verification Providers do not discriminate.

If a user does not have a credit card, an 18+ registered contract phone, a driving licence or a passport, it is highly unlikely an age verification provider will be able to verify that they are 18+. This differs considerably from the “offline” world where a user is largely not required to present any personal information in order to access 18+ services.

*A requirement that any Age Verification Provider does not discriminate against those without a credit card, a contract 18+ phone or lacking a driving license or passport is essential. At a minimum, the Age Verification Regulator should propose a verification method that is non-discriminatory and private (available to all UK adults without exception).*

### **Consumers (and children) will be driven to more harmful services**

A consumer who chooses not to, or is unable to, go through an age verification process will still have millions of pornographic sites to choose from, one click away via a Google search.

It is expected that the most popular sites, which generally offer content that is legal and not extreme, that act responsibly, for example by removing revenge porn, and that cooperate with UK authorities, will implement Age Verification.

Those sites which do not implement Age Verification are less likely to have proper oversight, are more likely to have inappropriate content, and will benefit from increased consumer usage.

The BBFC's approach as outlined in chapter two of the Guidance on Age-Verification Arrangements will actually cause this harm by specifically targeting the most popular sites.

An expectation set out in previous official documentation that "approximately 50" ISP blocks/year may be ordered (as part of impact assessment on ISPs) will make close to zero dent in the millions of sites offering pornography on a commercial basis given that a Google search for "porn site" returns over 100 million results.

The focus should be resolutely on those sites which cause most harm to children, not those that are most popular with adults.

*Consumers who choose not to age verify or are unable to age verify (perhaps because they are not over 18), will be driven to access sites which are more likely to expose them to harmful or illegal pornography. Change is needed to ensure that this natural outcome of the current proposal is avoided. A **primary focus** on "harmful" (e.g. abusive, extreme, criminal, unauthorised e.g. revenge porn) content first and foremost should be considered, (rather than service popularity, which would lead to the perverse outcome described). A **secondary focus** on those sites which are likely to provide inadvertent exposure to pornography (such as showing for inappropriate/innocent search terms, easy to stumble upon innocently, advertising in places which may be shown to minors, not correctly describing or protecting adult content) should be a secondary objective.*

### **Transparency of choice of enforcement actions**

Given the number of sites offering pornography on a commercial basis, many of whom will likely choose not to comply with this legislation, it is clear, as acknowledged in the guidance issued by the Secretary of State, that an approach is needed to prioritise which sites to target. The entire web simply cannot be covered.

The targeting criteria should be openly published, it should be measurable and it should be transparent. Without this, there will be a lack of clarity about which sites are targeted and the process it will be open to political, media and potentially corrupt influence.

For example, a weighted scoring system could be used to rank sites by priority. This could be based on objective criteria such as:

- Level of extreme content
- Availability to minors without any splash/warnings
- Advertising inappropriately (email spam/search)
- Etc

*The only factors for targeting of enforcement actions should be based on objective measures that quantify the harm being caused to minors by access to the material. This should ensure that the process is not subject to political, media or potentially corrupt influence.*

### **Lack of information about the Appeals process**

There is no information on the Appeals Process. The Secretary of State, according to guidance issued, must be satisfied as to the “arrangements” for appeals but without public comment or provision of such details it is impossible to be sure that any proposal is fit for purpose.

*Full details on the appeals process are needed.*

## ANONYMOUS ORGANISATION #2

23<sup>rd</sup> April 2018

Re: Guidance of Age Verification Arrangements, Digital Economy Act – Part 3 Online Pornography.

To whom it may concern,

Herewith please find the comments and response from [redacted] in relation to the public consultation issued as outlined above.

We are of the opinion that in general the guidance is well thought out and that it is clearly documented what the objectives of the DEA are.

It is good to see that “The primary purpose of this Part is the protection of children from pornographic content online” and that the definition of “not normally accessible” is clearly highlighted in section 2 of the introduction.

That said, there are areas which should be addressed and those are in turn detailed below:

### **Introduction**

#### Comment 1

Para 7: *“This guidance also outlines good practice in relation to age-verification to encourage consumer choice and the use of mechanisms which confirm age, rather than identity”*

Response(s): It is pleasing to see that merchants will be encouraged to use more than one supplier to reduce claims of a monopoly.

Will there be any kind of move towards enforcement of those items currently described as good practice?

### **Section 2**

#### Comment 1

Para 1: *“The method by which an internet connection or access can be obtained is irrelevant.”*

Response(s): This should be clarified as to whether the merchant/AV provider is expected to provide location on mobile devices and/or use of a VPN or other kind of traffic routing method.

#### Comment 2

Para 4: *“deciding which services that provide online pornographic material on a commercial basis it will investigate”*

*“assessing whether an age-verification arrangement complies”*

Response(s): How will the decision be made as to who will be investigated and in which order?

How will the merchant and/or AV provider know whether the 'arrangement' complies – the AV provider may well be whitelisted but there is risk for incorrect implementation, how will this be dealt with?

Comment 3

Para 9: *"Once an enforcement notice....."*

Response(s): Will a non-compliant merchant be provided details of compliant merchants they can work with and/or details of any professional/trade body with whom they can engage?

**Section 3**

Comment 1

Para 2: *"These solutions draw from numerous datasets including credit card, passport, driving licence and mobile phone age-verification"*

Response(s): This is a leading statement and could infer that only these methods are acceptable. How does the regulator intend to ensure equality with other, already acceptable methods, and those which may be developed once the DEA becomes enforceable?

The regulator should give consideration to the wording of this statement to avoid any misinterpretation.

Comment 2

Para 3: *"the BBFC will adopt a principle based approach when assessing new age verification...."*

Response(s): Will AV providers and merchants be provided with the features and factors which will be assessed and part of this approach?

Comment 3

Para 4: *"good practice in relation to age-verification to encourage consumer choice...."*

Response(s): Will a gateway offering more than one method therefore be deemed as good practice, OR should a merchant be using more than one gateway?

Comment 4

Para 6c: *"accepting age verification through the use of online payment methods..."*

Response(s): How does the regulator intend to deal with Pre-paid cards and the use of Crypto Currency (Pornhub now accepting Verge coin) – should we assume these will be banned as acceptable methods of age verification (although some Crypto coins do perform full KYC/Age Verification)

Comment 5

Para 9: *"and requesting more data than is necessary to confirm age, for example, physical location information."*

Response(s): As the DEA is to protect UK consumers from access to inappropriate content and the expectation is for merchants to only apply these checks to UK viewers. How is the merchant expected to ascertain whether a check needs to be performed if they are not able to determine a user's physical location?

#### Comment 6

Para 11: *"The BBFC will report the results of these assessments on its website."*

Response(s): What is the difference between this list of certified AV providers and the proposed accreditation of Trade Body members?

### **Section 4**

#### Comment 1

Para 3 a-f: *"age-verification systems must be designed with data protection in mind.....not retained for longer than is necessary to achieve the purposes for which it was originally collected"*

Response(s): When implementing a system which does not hold any personal data the question of enforcement comes up. How is a law enforceable if there is no way to prove/disprove the alleged breach. The purpose of verification is very short-lived, if not instantaneous, how the purpose of proving compliance with the legislation continues until the relationship with that consumer ends. Therefore, will the regulator:

- a) Expect a zero audit trail within both merchant and AV provider environment? OR
- b) Expect a pseudo/partially anonymized audit trail which shows a verification took place but has no ability to actually trace it to an individual to prove "Mr X was verified using 'X' information against 'X' provider", OR
- c) Allow the AV provider to hold a full trail which cannot in anyway be linked to an individual merchant? OR
- d) All the AV provider to hold a full audit trail as long as it is fully encrypted and in the event of a breach cannot be used for any inappropriate activity? OR

#### Comment 2

Para 4 d & e: *"retaining data for longer than is necessary" and "a requirement to provide, and any subsequent retention of, physical location information"*

Response(s): As outlined earlier, the definition of 'necessary' needs clarification, also how should the merchant ascertain whether they need to verify a consumer if they do not collect location information.

### **Annex 4**

#### Comment 1

Section 19: *"the BBFC agrees that it should inform the commissioner where concerns arise during its assessment of the age-verification effectiveness that the arrangement does not comply with data protection legislation."*

Response(s): Will the AV provider also be informed that this notification has taken place?

**General comments**

It is the opinion of \_\_\_\_\_ that the PAS 1296 should form the basis upon which age-verification systems should be developed and assessed.

Although the guidance refers to the AV provider/merchant minimizing the risk of verified credential sharing either deliberately or by fraudulent means it is not a requirement and is purely a best practice guidance, it also does not make any reference to the minimization of risk of an acceptable method of verification being used to spoof systems more than once (e.g. sharing of a driving licence to set up multiple accounts). It is in our opinion that this is a significant flaw in the legislation at present.

We look forward to working with the BBFC and DCMS to provide cost effective and appropriate solutions to the online pornography industry to meet the requirements of this act.



## ALEXANDER AGIUS

Subject: Privacy

Dear consultation team,

Given the recent revelations by Facebook, and the terrible reputation for safe storage of private data this move is very bad for the public, data breaches of millions of people's data is a cost not worth the perceived benefit (which in my opinion will not be achieved by this requirement).

The fact is if parents are allowing children to watch pornography they are abusing their children and the British government should take direct action against child abusers.

Instead (as is typical of the government's response to many problems like knife, gun and drug crime) the government thinks that some regulation will magic away the problem.

Fact is many sites operate outside the UK and will not care what the law in the UK (after all what can you do?). Sure you can block these sites but as we've seen with the blocking of piracy sites these blocks are very easy for users to get around (a simple Google search will show this to be the case).

The problem is the lack of education in schools and neglectful abuse some parents show.

The further concern is why stop at porn? Why not violence? After all a child can easily go onto a site like LiveLeak and watch actual people dying. The slippery slope is the rule (not a facility) when it comes to government action (for a prime example of that look at gun control laws in the UK).

My name and response does not need to be confidential.

Sincerely,

Alexander Agius

NIGEL AINSCOE

Subject: Call for public comment on AV guidelines

Dear consultation team,

As someone who works in IT and specifically, data security, I am horrified at the current proposals for age verification.

Whilst I understand the case for trying to protect children from inappropriate exposure to online content, I feel that creating a market for online verification is a disaster waiting to happen.

The sensitivity of such information would make it an obvious target, not only for casual hackers, but also for nation state actors who would have a strong interest in data like this for blackmail purposes.

In addition, the private sector has proven itself unreliable at best in securing personal data. Without stringent privacy provision this regulation is unlikely to turn out well. Least of all for the BBFCs reputation.

My name and response does not need to be confidential.

Sincerely,

Nigel Ainscoe



FILIPESCU MIRCEA ALEXANDRU

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,

Filipescu Mircea Alexandru

ANT ALLAN PH.D.

Subject: Age verification (AV)

Dear consultation team,

I am writing to you as a private citizen, but my comments draw on eighteen years as an analyst with the world's largest research & advisory firm, working in the area of security & risk management.

AV must respect personal privacy.

Recent events underscore the need for robust regulation and oversight to ensure that private companies as well as public organizations are reliable custodians of our personal data.

Better still, any firm providing online services should be prohibited from collecting and retaining personal data if it has no need to do so.

It is quite feasible to architect AV in a way which doesn't expose any personal data (even date of birth) to the website using the third-party AV service and doesn't require the AV service to keep any information about who visited that website.

It should be a regulatory requirement for any company offering AV services to use such a privacy-respecting architecture.

My name and response does not need to be confidential.

Sincerely,

Ant Allan Ph.D.



## LUKE ASHBY

Subject: Age Verified - Prove it.

Dear consultation team,

AV tools may create a sensitive record of the public's porn watching habits.

The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

Also how does one know if the ID being used is of the person it belongs to. Just because someone has access to the ID it does not mean they are themselves old enough to view.

My name and response does not need to be confidential.

Sincerely,  
Luke Ashby

## STEVE ASHFORD

Subject: Age verification

Dear consultation team,

Privacy must be protected in any technology that's introduced for internet age verification. Unless protected, personal information is open to identity theft.

My name and response does not need to be confidential.

Sincerely,  
Steve Ashford

**BRIAN ASTBURY**

Subject: The Digital Economy Act

Dear Consultation team,

I am most concerned about the sloppy way that this Act is being written.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is outrageous. Private companies will disregard user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

Please take this seriously. This is NOT about access to Porn sites - it is about misuse of our data.

My name and response does not need to be confidential.

Sincerely,

Brian Astbury

## REG BAILEY

Dear David

Following our brief conversation this morning, I am following up with this email to say that I have read and considered the draft Guidance on Age Verification and am delighted to see that this guidance is very much in the right direction of travel in terms of protecting consumers, especially children and other vulnerable people, from the normalising impact of unfettered access to pornography. I declare an interest in that I am a long term supporter of an effective Age Verification system as a means of helping in the formation of Children and young people in becoming emotionally resilient citizens.

The age verification process is very much “principles led” which is helpful in terms of adapting to very fast changing technologies, and is a proportionate response to the issue. I am pleased to see that the annexes give clear descriptors of how to define extreme pornography, and also the definitions of R18 are spelt out for clarity too.

Overall I cannot but see this as a common sense approach to child protection, and in this respect I am fully in favour and supportive of this guidance.

I hope this is helpful.

Warm Regards

Reg

Reg Bailey CBE  
(Former Independent Reviewer for the Government of the Commercialisation and Sexualisation of Childhood.)

## DAVID BAIN

Subject: Age verification

Dear consultation team,

The proposed legislation has inadequate data safeguards. Given the value of personal data in today's electronic age, there are bound to be leaks or access attempts: only absolute, guaranteed security is enough. The proposed approach does not have that.

My name and response does not need to be confidential.

Sincerely,  
David Bain



## TIM BANNISTER

Subject: Age verification consultation

Dear consultation team,

Online access to sexual images, videos etc is a sensitive matter. Information about age verification could easily reveal someone's sexuality, and potentially other sensitive personal data too.

I believe that effective labelling of content is more valuable than having services verify that the person accessing the service is over 18. With good labelling, parents should be in a position to manage their children's access to nudity and other sexual content. It might also be helpful to be able to label text content; although the BBFC does not look after text content, there will certainly be sexual text content online that parents feel is not appropriate for their children.

Crucially, advertising **MUST** be limited so that UK advertisers are not showing inappropriate adverts to young people in the UK. Where unlabelled adverts are served to all viewers without checks, the most effective measures will be those that restrict income from the services being advertised.

UK pornographic websites should involve performers who are over 18 and (in the UK) viewers who are over 18. It will be difficult to be precise about the definition of "in the UK" for various reasons. Where a web service could reasonably assume that a potential customer is in the UK, I understand the value of making checks on that customer's age. This is equivalent to what might happen at a cinema (whether showing pornographic films or other films with an 18 certificate).

I have industry experience of federated identity systems in a different context: UK academia and online access to academic resources. There, the systems in place make it difficult for service providers to track visitors. The default check might be along the lines of "is this person a member of your institution". Age checks for pornographic websites need to be at least as mindful of privacy concerns. It is important that there be a genuine market for age verification services, so that people who doubt the good intentions of one provider are free to choose from a range of others.

I recommend that the BBFC and ICO work together to transpose relevant requirements from GDPR into industry-specific regulations. These can and should stay in place even once the UK leaves the EU.

My name and response does not need to be confidential.

Sincerely,  
Tim Bannister

TOM BARKER

Subject: Privacy Must be Integral to Age Verification Tools

Dear consultation team,

Requirements for pornographic websites to verify UK users are over 18 will come into effect soon, and the BBFC is in charge of issuing guidance for how age verification (AV) tools must operate. Ensuring children and young people are protected, educated and given parental care is vital, however we have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Tom Barker

## ELIZABETH BATHORY

Subject: AV tools

Dear consultation team,

Requirements for pornographic websites to verify UK users are over 18 will come into effect soon, and the BBFC is in charge of issuing guidance for how age verification (AV) tools must operate. Ensuring children and young people are protected, educated and given parental care is vital, however we have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

My name and response does not need to be confidential.

Sincerely,

Elizabeth Bathory

## TIMOTHY BATES

Subject: Confidence in privacy: An opportunity for AV

Dear consultation team,

Given a policy of age verification, protecting users from exploitation by or abuse of this policy is essential. It also creates an opportunity for the UK to lead in private verification and reputation technology.

My request is that whatever system is used

1. Separates verification from identity. websites should receive a token indicating that page requests are from a verified viewer, but nothing more.

\* This can be implemented with public key methods among others.

2. This verified identity should be portable for the user: An open-source implementation and API (programming interface) would allow the technology to be used for verifying claims without disclosing personal information in an extensible fashion. Such a system could become a global standard for privately verifying information from interests or memberships, to citizenship.

I hope that the consultation team takes this opportunity not just to implement the government's will that viewer of certain sites be adults, but to do so in a way that

1. Preserves and enhances privacy

2. Does not give websites (often of very dubious backgrounds) personally identifying information, such as emails, addresses, passport #s or other sensitive information.

My name and response does not need to be confidential.

Sincerely,

Timothy Bates

## ALUN BEARD

Subject: Age Verification

Dear consultation team,

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy legislation and meaningful penalties for breaches or violations.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Alun Beard

BRIAN BEESLEY

Subject: Age Verification Privacy

Dear consultation team,

I am seriously concerned about privacy issues which the proposed Age Verification mechanisms may raise.

At present there is a gap where neither BBFC nor ICO is responsible for overseeing users' privacy. In the light of recent scandals it is clear that private companies are not fit to take on this responsibility.

Unless and until responsibility for privacy is assigned, mandatory age verification should not be allowed to come into force.

In my opinion age verification is acceptable only if no data is stored permanently anywhere except as a securely encrypted certificate on the subject's own computer / tablet / smart phone, and if all communication over the network is encrypted using a secure mechanism with a key length of at least 16384 bits.

At the very least the age verification mechanism must not, for any reason whatsoever, expose any personal information to any third party, whether or not in an encrypted form and even if for statistical purposes only.

My name and response does not need to be confidential.

Sincerely,  
Brian Beesley

ROBERT BELDINGFORD

Subject: Response to age verification consultation

Dear consultation team,

I feel that extremely strong privacy tools need to be included with any age verification app/software/coding. After the recent facebook scandal concerning Cambridge Analytica with millions of peoples sensitive personal data being stolen and used in ways to manipulate world events, it is of paramount importance that privacy of data names, addresss, age, habits etc is protected.

My name and response does not need to be confidential.

Sincerely,  
Robert Beldingford

ALEX BELL

Subject: Dangerous measure

Dear consultation team,

An ill thought out measure will put countless people at risk of fraud and/or blackmail

My name and response does not need to be confidential.

Sincerely,  
Alex Bell

KELLY BELMONT

Subject: Age Verification

Dear consultation team,

My name and response does not need to be confidential.

You cannot police the world. Parental screening tools for PC have been around for decades. If parents want to control what their children's access, it's as simple as keeping PCs in multiperson rooms, such as living rooms. You really are not going to get any porn going there.

This is down to parental guidance, not making everyone else have to give over sensitive information lest children access sites they should not.

Why should adults, wanting to access adult content, have to give over extremely sensitive information because of a group of under-aged users?

Teenagers used to access pornography before the internet. It was passed-around copies of Razzle and Playboy. Will adults have to give over ID to buy these magazines from newsagents now, just in case a person under 18 manages to buy a copy?

The fact of the matter is that the government, the BBFC, and ICO cannot keep our information safe. You can apologise all you want when a breach happens, but it's no good when our information has been stolen.

All these steps to stop children accessing places they should not be is ridiculous. The onus should be on the parents to parent. If every Sky box has a parental code to do regulate the channels their children can see, PCs can too. Children do not need smart phones, if access in this manner is the concern. Again, try putting some of the weight on parents to actually parent.

Here's another point: not all "children" (anyone under the age of 18)) are trying to look at pornography.

This doesn't even touch upon the fact that information is cash. We've had too many instances of personal information being sold to third parties. Even our medical records are being sold to third parties without our consent, but for us to allow a tribunal access, that's a £130 administration fee. This is through the NHS.

You could always impose fines on those who lie about their age to access sites? The sites offer access in good faith. That's kind of like punishing a shopkeeper for being robbed.

The irony here is that I'm not a user of pornography. It just isn't my thing. However, I don't want other people who thoroughly enjoy it to be limited in their access to it. It provides a lot of people with a glimmer of joy to an otherwise miserable day. Don't make it harder to get legally with this enhanced age verification garbage.

Sincerely,  
Kelly Belmont



## MARTIN BENNETT

Subject: Stupid idea.

Dear consultation team,

Just 2 reasons why the age verification proposals are stupid.

No organisations can guarantee that documentation supplied for age verification will not be mislaid or misused.

Pornography does not just exist on web sites run by responsible law abiding organisations. It is hosted on rogue web sites. It is distributed via social media, email and other communication tools. There will be plenty of opportunities for people to avoid and bypass age verification and yet still access pornography.

My name and response does not need to be confidential.

Sincerely,

Martin Bennett

## PETER BENSON

Subject:

Dear consultation team,

I am afraid that handing age verification over to private companies is a recipe for big business to be able to use peoples internet habits against them.

I most definately do not want a Cambridge Analytica wannabe to be able to effectively blackmail me by threatening to reveal my internet browsing.

My name and response does not need to be confidential.

Sincerely,

Peter Benson

## SIMON BERESFORD

Subject:

Dear consultation team,

I am totally against this incredibly stupid age verification legislation. LEAVE THE INTERNET ALONE!! Get rid of the Snoopers Charter. Do what you can to bring back Net Neutrality and tell the USA off for FOSTA-SESTA (which I consider an act of war as it affects all internet using English speakers, not just Americans).

Politicians should NEVER interfere with the INTERNET!!!

Instead of this nonsense, encourage parents to parent their children. If a teenager wants to watch porn what is to stop them from borrowing their parents credit card details? And if somebody is searching for porn they're probably old enough to watch it. They just need teaching that porn is not real. Parents need to stop being squeamish and teach their kids the birds and the bees at about age 8.

No form of age verification is fool proof and you are making British Citizens more at risk of identity theft and blackmail if they have to give their credit card or passport details to porn websites!

My name and response does not need to be confidential.  
Sincerely,  
Simon Beresford

## CHRIS BIDMEAD

Subject: Opposition to age verification in DEAct

Dear consultation team,

Protection of children and young people on the Internet is important but no government regulation can substitute for educated parental care.

In particular, reliance on age verification (AV) to achieve this, particularly when implemented with arbitrary, poorly appraised technology, is exactly the sort of "solution" guaranteed to create more problems than it solves, especially but not exclusively in the area of personal privacy.

I have been an IT journalist for over 35 years and I am very wary of the introduction of ill-thought-through legislation by politicians who understand neither the field of knowledge nor, apparently, the problem.

My name and response does not need to be confidential.

Yours,

Chris Bidmead

## COLIN BIRKS

Subject:

Dear consultation team,

I am concerned about the potential breach of privacy in the proposed AV tools. The information to be gathered is highly sensitive and, in the light of the Cambridge Analytica scandal, I am far from convinced that it will be handled in conditions of adequate security. Privacy must be integral to this information gathering exercise.

My name and response does not need to be confidential.

Sincerely,  
Colin Birks

## BENJAMIN BLACK

Subject: Age Verification

Dear consultation team,

I am appalled by the proposal to create a database, managed by private companies, which will contain the sensitive viewing habits of the UK population. This is 'bad regulation' which will backfire as people have no confidence in their privacy being respected online. If there is a data breach (think Cambridge Analytica), the consequences could be dire to many individuals, their relationships, their reputations and their wellbeing, not to mention being used as a potential blackmailing tool. For example, what happens to the 18 year old who is curious about his sexuality, watches gay porn and then is outed in a privacy breach to his friends and family, or the woman who has a particular fetish which her husband does not know about and would not approve of? Such a breach would be catastrophic to people's personal lives.

Who will ensure privacy here? There is no level of confidence in this process as neither the BBFC, nor the ICO have considered who will oversee this. Surely there is a better way of educating children effectively and keeping them safe online through parental controls rather than storing data.

My name and response does not need to be confidential.

Sincerely,  
Benjamin Black

SIMON BLACKBURN

Subject: age verification

Dear consultation team,

The issue of age verification not only creates censorship of the internet, who judges what is adult content as it is a some what flexible term depending on peoples points of view?

It also means giving our personal information to 3rd parties with the Cambridge Analytica fiasco this is open to abuse

My name and response does not need to be confidential.

Sincerely,

Simon Blackburn

## About Pandora Blake and Myles Jackman

This evidence is submitted jointly by Pandora Blake and Myles Jackman. Pandora Blake is an independent scholar and multi award-winning feminist pornographer, whose ethical porn site was unsuccessfully censored in 2015 by ATVOD under the AVMS Regulations 2014, and reinstated in 2016 after a successful appeal to Ofcom.

Myles Jackman is a lawyer specialising in obscenity law, who obtained Not Guilty verdicts in two landmark obscenity trials in 2012, Rv Walsh and Rv Peacock. The same year, he was awarded the Law Society's Junior Lawyer of the Year Excellence Award.

Both have significant concerns around the impact of obscenity law on sexual minorities, and are active campaigners for civil liberties and sexual freedom.

# Guidance on Age-Verification Arrangements

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

### Child protection

The Guidance repeatedly refers to the child protection aims of age verification. However there is no credible research base showing that exposure to pornography is harmful to children. Both the evidence gathered by the expert panel for DCMS<sup>1</sup> in November 2015, and Ofcom's own overview of the potential impact of R18 material<sup>2</sup> from May 2005, show that there is no robust evidence to prove that young people are harmed by encountering sexual images. In fact Ofcom's review shows that data from Denmark, Japan and the USA links greater access to pornography to positive outcomes, including lower rates of sexual violence, higher reporting of sex crimes, and lower rates of STI transmission and teenage pregnancy.

Age verification won't stop under 18s from looking at porn anyway: young people are digital natives, and internet-literate teenagers - like everyone else - will be able to obviate age checks via VPNs, TOR and proxies if they are determined to do so. This risks driving under 18s into the dark web, which carries far higher child protection risks - a risk noted in the DCMS Impact Assessment.

These measures therefore can only possibly seek prevent young children from accidentally encountering porn. However, this is not a problem that exists. The claim that increasing numbers of young children are accidentally encountering porn online, and are distressed by it, is not supported by the evidence.<sup>3</sup> Studies fail to differentiate between younger and older children, grouping 9 year olds with 16-17 year olds over the age of consent to have sexual intercourse in order to generate misleading and overblown statistics. The 2011 EU Kids Online study shows that children are far more likely to encounter sexual imagery offline than online, and that "overall, most children have not experienced sexual images online and, even of those who have, most say they were not bothered or upset by them".<sup>4</sup>

---

1

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/500701/Report\\_of\\_DCMS\\_Expert\\_Panel\\_\\_Autumn\\_2015\\_FINAL\\_.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500701/Report_of_DCMS_Expert_Panel__Autumn_2015_FINAL_.pdf)

<sup>2</sup> <http://stakeholders.ofcom.org.uk/binaries/research/radio-research/r18.pdf>

<sup>3</sup> <https://bishtraining.com/does-porn-harm-young-people>

<sup>4</sup> [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20\(2009-11\)/EUKidsOnlineIIReports/Final%20report.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf)

Ranum's Law states that "You cannot solve social problems with software". Young people deserve our protection and support, but there is no evidence that age verification will do anything to keep children safe. Meanwhile, the Government are reducing funding for sex education, schools, libraries and youth clubs, indicating that they are more interested in blocking access to pornography and controlling the Internet than in truly helping young people.

Age verification is a distraction from the real issues. To truly protect young people, compulsory sex education, provided by independent experts rather than untrained teachers, needs to be funded and supported by the government.

## The scope of the legislation

Paragraph 2.1 limits the scope of the BBFC's jurisdiction to websites making pornographic material "on a commercial basis". Under the current Commercial Basis regulations, all websites hosting over-18 stills, images or audio are expected to comply with age verification if they "make or receive" any payment in connection with making pornographic materials available; regardless of whether they make any profit, or even any income at all from doing so. This creates an unfeasibly large scope for age verification which is impossible for the BBFC to uphold.

As David Austen has noted, it is unrealistic for the BBFC to classify and notify millions of websites each year, especially since he only anticipates taking on "one or two extra people"<sup>5</sup>. It is therefore ludicrous to imagine that the BBFC might be able to assess more than the tiniest fraction of websites, which are created at the rate of 1 per second and often updated daily. A proportionate approach as mentioned in paragraphs 2.3-5 is therefore the only possible way forward; however section 2 fails to explain how the BBFC will choose which websites to examine in a fair and even-handed manner.

## Out-dated classification guidelines

The BBFC's own R-18 classification guidelines rely on the Obscene Publications Act (OPA) 1959, via the Crown Prosecution Services' guidance<sup>6</sup>. As Myles Jackman is well aware, this Guidance is not up to date with UK case law. In *R v Peacock* 2012, Jackman represented a client who was unsuccessfully prosecuted under the OPA for distributing DVDs representing gay whipping, urolagnia and fisting. The jury returned a unanimous verdict of Not Guilty. Yet six years later, the CPS website still lists "sodomasochistic

---

<sup>5</sup>

[https://hansard.parliament.uk/Commons/2016-10-11/debates/5da6f418-b687-41aa-9418-449cf52d598e/DigitalEconomyBill\(SecondSitting\)](https://hansard.parliament.uk/Commons/2016-10-11/debates/5da6f418-b687-41aa-9418-449cf52d598e/DigitalEconomyBill(SecondSitting))

<sup>6</sup> <https://www.cps.gov.uk/legal-guidance/obscene-publications>

material which goes beyond trifling and transient infliction of injury, torture with instruments, activities involving perversion or degradation (such as drinking urine, or urination)” and “fisting” as types of activity which may be suitable for prosecution, and the BBFC still refuse to classify such activity as R-18.

Not only does this discrepancy reveal the neglect of the CPS in staying up to date with UK case law, it also indicates the widening gulf between the BBFC’s understanding of obscenity, and public opinion.

If even the BBFC and CPS cannot reliably stay abreast of UK obscenity law, it is unrealistic to expect site owners and members of the public to know whether material they publish would be classified 18 or R18, and therefore whether they are required to put it behind age checks or not. Before expecting site owners to comply with age verification, the BBFC must engage in a review of their classification guidelines to bring them up to date with UK case law, and provide clear guidance for site owners about what material can and can’t be published outside age checks.

“Frequently visited”

2.5 implies that the BBFC will assess which services are “most frequently visited, particularly by children”. What data is the BBFC planning to base this assessment on? Determining how many children visit a given website has significant ethical implications. Since the BBFC is committed to transparency, they must publish details of how they will be obtaining this data, and a list which sites they deem to be “frequently visited”.

Extreme pornographic material

2.5 refers to “extreme pornographic material”, referencing the Criminal Justice and Immigration Act (CJIA) 2008. Under the current regulations, sites publishing this material will be subject to penalties including unilateral web blocking at ISP level, even if the material is confined behind age checks. Yet the CJIA 2008 refers to a crime of possession, not of publication.

Crimes of publication are covered by the Obscene Publications Act (OPA) 1959.

Extending crimes of publication beyond the scope of the OPA is beyond the remit of age verification, and outside the jurisdiction of the BBFC.

It is inappropriate for the BBFC to misuse the powers vested in them for the purposes of implementing age verification to extend the reach of the CJIA, and impose new, more severe penalties (ie web blocking) for crimes of publication. The BBFC’s role is to enforce age verification, not to censor what kinds of content can be published or viewed by consenting age-verified adults.



Indecent images of children

The BBFC also propose to find sites containing “indecent images of children” non-compliant (2.5). Investigating images of child abuse is the purview of the Police and Internet Watch Foundation, as per the Protection of Children Act 1978 and the Criminal Justice Act 1988. Given the BBFC’s limited resources, it is overstepping their authority, and a waste of taxpayer’s money, for the BBFC to attempt to duplicate the efforts of the Police and IWF.

## Right of Appeal

Under ATVOD’s jurisdiction, websites were targeted in a scatter-gun and discriminatory manner, with a disproportionate emphasis on websites providing fetish material depicting female domination. Although the AVMS 2014 ostensibly limited scope to “On Demand Programme Services” such as Amazon Prime Video and BBC iPlayer, ATVOD targeted tiny one-woman clip stores hosted on US services such as Clips4Sale.com as ODPS.

Pandora Blake’s website Dreams of Spanking was one such. After appealing to Ofcom, it was determined that this website was not an ODPS and should not have been targeted by ATVOD. However, the requirement to take the website offline for ten months while the appeal was being considered meant that their (previously successful) business was effectively destroyed despite successful appeal, due to the loss of traffic and SEO incurred during the downtime. No financial compensation or redress was offered for the ongoing loss of employment and income.

ATVOD’s activities were sufficiently indefensible that the organisation was disbanded while Ofcom were considering Blake’s appeal. Nonetheless the BBFC is now emerging as another regulator who is able to exercise comparable levels of discretion when considering which websites to assess. It is paramount that the BBFC avoid the discriminatory and stigmatising approach taken by ATVOD.

Section 2.8 refers to the right of a person notified to “make representations” to the BBFC - however it puts the BBFC under no obligation to take these representations into account. Given the ambiguities of the 18 and R-18 classifications, and the BBFC’s lack of personnel and resources to handle the size of the task ahead of them, a robust appeals process must be in place, with serious consideration given to considering representations made by notified persons.

Annex 4.16 is insufficient to inform site owners of the process for appeal. Who will the Independent Appeals Panel be? How will they be selected? The BBFC need to produce fair and transparent guidelines for appeal to an independent organisation, which do not cause

unreasonable loss of income by requiring a website to be taken offline while the appeal is being considered.

Section 2.16 notes that the BBFC will publish details of actions taken and the outcome of appeals on their website. When ATVOD published their determinations, the legal names of pornographic website owners were frequently posted, with no respect for the individual's privacy or chosen pseudonym. The BBFC must take privacy into account and redact the names of site owners when making these publications.

## Sanctions and disproportionality

The UN Special Rapporteur for Freedom of Expression, Frank La Rue, has criticised default internet filters and web blocking, and found that in the case of child protection online, no additional measures were necessary:

“While the protection of children from inappropriate content may constitute a legitimate aim, the availability of software filters that parents and school authorities can use to control access to certain content renders action by the Government such as blocking less necessary, and difficult to justify.”<sup>7</sup>

This applies directly to the BBFC's powers to notify ISPs to block non-compliant websites. This power will lead to the effective creation of a new UK-wide firewall, and massively compromise the digital liberties and freedom of speech of UK citizens. Once in place, these new powers of web blocking can be misused by future Governments to suppress other forms of speech which they do not like. Currently the only other countries imposing this sort of blanket internet restriction on its citizens are China, Saudi Arabia and Iran.

The BBFC's powers to block non-compliant websites combine with the chilling effect, the personal and social harms of mandatory age verification on small websites and their users, and the impact on independent sex workers, to constitute a real and serious threat to free expression. This is a human rights issue.

Given the weak evidence for the purported benefits of age verification and the manifold harms that will result, age verification represents a disproportionate impact on free expression and personal privacy.

---

<sup>7</sup> [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

## Impact on low-traffic websites

Imposing compulsory age verification on low-traffic and niche content providers will cause businesses to close, and significantly impinge freedom of expression.

### Financial impact

Installing age verification tools will carry a significant cost to sites who undertake it. Sites will have a choice of age verification services which charge the site owner a fee (either per age check or per month), or free services paid for by advertising, which carry a less quantifiable cost of compromised privacy and security. Regardless, site owners will bear the labour costs of setting up the technology. Large, for-profit pornographic websites are more able to bear these combined costs than smaller, low-traffic or amateur websites. These regulations will therefore discriminate against small businesses and amateur pornography creators unless the latter are exempt from complying with age verification.

Many adults post home-made explicit images on sex blogs which they share with small audiences of likeminded readers online. They might receive at most a few pounds per year from hosting adverts, but not enough to cover the costs for age verification.

Similarly, many small porn sites such as that owned by Pandora Blake are in the same situation: producing pornographic material for the joy of it rather than to make money, with their material viewed by a tiny, niche audience. These sites advertise via publicly visible free previews and trailers.

In the last month at time of writing, Pandora Blake's site Dreams of Spanking has received 2000 unique visitors per day, and has processed less than one new sale per day. This represents a sales conversion rate of less than 1:1000. While Pandora's website is significantly less active now than it was prior to ATVOD's unjustified disruption of its business, such figures are not unusual for niche pornographic websites. Even with an error margin of several orders of magnitude, if a website with such a conversion rate is required to age verify all site visitors, it will instantly go out of business.

### Lack of technical resources

Small pornographic websites are often built on pre-made website templates, owned by one or two individuals who usually have other jobs, who lack the IT skills or the resources to set up age verification.

There are very few IT freelancers who provide technical services to amateur pornographic websites: these freelancers are likely to find themselves swamped with

requests to install age verification, leaving even site owners who are eager to comply in the lurch. Site owners should not be discriminated against because they lack access to timely IT support.

### Social benefits of online sexuality communities

Online communities where people share their sexual fantasies, memories, questions and desires play a valuable social role. Sexuality is a core theme of many people's lives, and many individuals benefit from the opportunity to discuss these personal topics under a pseudonym within likeminded communities online. These conversations contribute to improved mental and emotional wellbeing, the health and longevity of romantic partnerships, and bring joy and fulfilment to many people, without causing harm to anyone.

Obliging these amateur site owners to require age verification of their visitors will stifle free expression. It will also increase the social stigma around talking and writing about sex, causing manifold indirect social harms.

Adults who talk about sex online are understandably concerned to protect their privacy. Many post using pseudonyms, and keep their online activities private and separate from their work and family lives. Given the inadequate privacy protections proposed by the draft Guidance (see replies re Chapters 3 and 4 below), it is unreasonable to force such sites to refuse access to anyone reluctant to risk their personal privacy by submitting their details to a third party age verifier.

There are many valid social reasons why people might wish to keep their legal activities private. Restricting access to online pornography would increase the amount of social stigma associated with it. Mandatory age verification has the effect of stigmatising consensual adult sex, fostering ignorance about sex among young people, and increasing the taboo appeal of pornographic material.

Enforcing age verification on community sites devoted to sexual expression will therefore not only impose impossible financial burdens on the site owners, it will also discriminate against users who value privacy and will be unwilling to use age verification.

When small websites inevitably find that many of their viewers are unwilling to trust their sensitive data to an age verification tool, the loss of traffic will dissuade amateur erotica creators from continuing to run their sites. This will inhibit free speech and the healthy diversity and inclusivity of adult media online.

## Impact on diversity and freedom of expression

Consenting adults have the right to sexual expression. Erotica and pornography are declarations of humanity, and are the backbone of free speech. In his 2001 report the UN Special Rapporteur for Freedom of Expression stated that "the right to freedom of expression includes expression of views and opinions that offend, shock or disturb".<sup>8</sup> His report also noted that restrictions on access to information can have a "chilling effect", whereby individuals restrict their own activities in anticipation of being forced to comply, often over-estimating and censoring themselves far more effectively than if it were left to government enforcement.

Many critics condemn mainstream pornography for presenting an unhealthy, unrealistic or even harmful view of sex. To counter any harms caused by this trend, what is needed are more amateur content creators creating homegrown, consensual pornographic content, which expresses their authentic sexual selves freely and without shame. It is precisely these sites that will disappear if they are forced to comply with age verification, while the larger, mainstream, commercial sites have the funds and resources to survive.

Lifestyle sex bloggers and content creators who post within tight-knit, low traffic communities, and spend more money maintaining their websites than they make, should not have their freedom of expression constrained by expensive and unnecessary age checks.

We have already seen many UK sites pre-emptively self-censoring in entirely unnecessary ways since the Digital Economy Act passed last year - for instance by needlessly deleting certain words and phrases from their websites. It is a good start that the BBFC are intending to take a proportionate response, but more clarity is needed to avoid a chilling effect where people self-censor out of fear of getting in trouble.

## Proposals

The BBFC must protect freedom of expression by providing clarity and reassurance. They should:

- Explicitly state that amateur, low-traffic sites will not be expected to comply.
- Set a minimum number of visitors per day, below which the site is considered to be too small to comply.
- Set a minimum turnover per annum, below which sites are considered to be non-commercial in nature. For instance, Italy set a €100 000 per year minimum for

---

<sup>8</sup> [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

sites to be expected to comply, when implementing the AVMS 2014.

Any, or all, of these measures would create needed transparency, reduce the chilling effect, and ensure that the BBFC's approach to enforcement was truly proportionate.

## Impact on independent sex workers

For similar reasons to those outlined above, age verification will have devastating consequences for sex workers who advertise online. It will decrease their options, freedom and independence, and making it harder for them to choose clients and work in safety.

Consenting adult sex workers advertising their services are publishing pornographic material for the primary purpose of advertising, not arousal. A sex worker might post an explicit advert, but not attract any clients nor receive any payment or benefit in association with making the material available. This material therefore falls outside both the definition of "pornographic material", and the definition of "commercial basis".

Despite this, many sex workers are eager to avoid attracting unwanted attention from the regulator, and fear that they must somehow comply with age verification while knowing it will decimate their independent means of making a living.

Sex workers must not be prevented from posting their own advertising, screening and vetting their own clients, and choosing what services they offer. Clients are understandably concerned to protect their privacy, and are easily daunted by requirements to reveal their identity. If sex workers are obliged to lock their adverts behind age verification tools, it will deter most clients from viewing their sites. The consequences will be that sex workers who cannot advertise independently will instead be obliged to go back to working for exploitative bosses, or on the street, because they cannot effectively attract clients online. This will put them at greater risk of violence, exploitation and abuse.

The BBFC must not endanger vulnerable people by forcing sex workers to hide their adverts behind age checks. The Guidance must explicitly state that sex workers who advertise services online are not considered to be making pornographic material available on a commercial basis, and will not be expected to comply with age verification. This will provide clarity to sex workers, and will enable them to continue to work in the safest way available.

## Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?

### Privacy “recommendations” are unenforceable

Sections 3.7 and 3.8 describe how the BBFC “recommends” good practice and consumer choice. In section 3.1 the BBFC use forceful language requiring that pornography providers “*must*” adopt effective and robust age verification arrangements. By contrast, the minimal and weakly-expressed “recommendations” in Chapter 3 that age verification providers “should” protect user privacy are wholly inadequate. If the BBFC can “actively assess individual age verification arrangements to test their effectiveness and robustness”, why can they not also assess them to test their privacy and security?

3.7 proposes “good practice” for age verification solutions; this is non-binding. Data protection and minimisation standards must be an enforceable regulatory requirement, rather than mere recommendations which the BBFC are not empowered to enforce.

The BBFC should publish comprehensive technical privacy and security guidance which age verification providers are required to comply with. Age verification producers which do not meet these privacy standards should not be considered compliant.

### Risk of social exclusion

The BBFC state in section 1.6 and 3.4 that they are interested in confirming “age, rather than identity”. However the means of verifying age mentioned in 3.2 include credit card, passport, driving licence and mobile phone - all of which are linked to identity.

Not every adult over 18 has the necessary documentation to verify their age. They might not have the financial security to maintain a credit card or pass a credit check; they might have unstable housing circumstances preventing them from giving proof of address.

Passports and driving licenses might be financially inaccessible to those with disabilities, those who lack citizenship or live in poverty.

Transgender individuals, particularly trans women, are more at risk of violence or murder than any other group. Survivors of domestic abuse, queer and transgender people are all entitled to sexual expression, but would put themselves in danger by connecting their online activity with their legal name. Marginalised adults must not be prevented from accessing legal material online in a way that perpetuates existing inequalities.

## Collection and retention of data

The recommendation that age verification solutions provide “ease of use” (3.7) for end users is welcomed. However the BBFC seem to misunderstand how this might be achieved.

Once a user has been verified by an AV service, they will prefer to not have to re-submit documents on subsequent visits, which might take place on the same day. Sites will want to offer their users a streamlined browsing experience by letting them age verify using systems they have already used, rather than having to re-submit identifying materials each time. An AV tool which offers a “single sign on” approach across multiple sites will have a significant market advantage. This can only be achieved if the AV provider keeps records about which websites have been visited by which verified individuals.

It is demeaning to expect records to be kept about what we do with our genitals, and what we think about while we do it. Furthermore such record-keeping creates an extraordinary privacy risk, which could result in databases of people’s sexual preferences and porn browsing history - linked to logins or email addresses - being leaked or hacked.

## Conflict of interest

Some age verification providers have a vested interest in collecting these datasets. MindGeek is the biggest porn company in the world, and the means by which a lot of under 18s access porn. They reportedly own approximately 90% of the free adult “tube” sites on the internet such as Pornhub, YouPorn and RedTube. Their “tube” sites make money by allowing users to upload pirated (stolen) content made by producers like Pandora Blake, and then monetising it via advertising; the resulting content is free to the end user.

Using profit earned via pirated content, MindGeek have bought porn brands such as Brazzers and Digital Playground, and thereby established their monopoly both on production, and on distribution. Now, age verification will allow them to also become the gatekeepers of porn via their age verification system AgeID.

AgeID will inevitably have broad take-up amongst members of the UK populace, as it will be the only age verification solution providing access to popular free tube sites such as Pornhub. Digital Media Director David Cooke informed delegates at the age verification technology demo organised by the Adult Provider Network in 2016 that MindGeek anticipate 20 to 25 million adults in the UK will use Age ID “within the first month”. That’s 39% of the UK population.



This poses a massive conflict of interest. Advertising is MindGeek's main source of revenue, and they have a direct profit motive to retain and monetise data on what people like to look at. MindGeek intend to offer AgeID as a federated AV solution for other site owners to use - which will allow them to create vast, lucrative databases of users' porn browsing habits, not only on their own websites, but on sites outside their network.

MindGeek have a terrible record on keeping sensitive data secure. Pornhub recently suffered a year long malvertising attack.<sup>9</sup> In 2012 a YouPorn data breach revealed the email addresses, usernames and passwords of a million porn viewers.<sup>10</sup> The same year hackers romped through Digital Playground, leaking 73,000 user details and numbers, expiry dates and security codes for 40,000 credit cards;<sup>11</sup> "the Digital Playground site was so riddled with security holes that it acted as a irresistible target". Chat logs and login details for 800 000 Brazzers subscribers were leaked in 2016.<sup>12</sup> MindGeek has suffered breach after breach after breach.

The Digital Economy Act creates a market for age verification technology which is completely unregulated. With no compulsory privacy safeguards required for compliance, the BBFC is expecting the market to magically protect user privacy. But that's not how the market works. Advertising-funded companies such as MindGeek have no incentive to minimise data transmission or retention, and a proven track record of security failures.

AgeID will give MindGeek access to a unique new seam of profitable data: information about what porn sites AgeID users log into across the world wide web. MindGeek may not see user IDs, but they will ask for email addresses and passwords to provide ease of use; data that they have repeatedly compromised in the past. AgeID therefore creates the very real risk of a database of the sexual preferences and porn browsing history of 25 million people, linked to their identifying credentials, being leaked or hacked.

To avoid this, the BBFC Guidance must place robust privacy and security requirements on age verification providers. A "conflict of interest" clause preventing pornography or advertising-based companies that stand to profit from collecting porn browsing data from operating AV tools would also be sensible.

---

<sup>9</sup> <https://www.theinquirer.net/inquirer/news/3018894/pornhub-hack-hackers-hijacked-ads-with-malware-in-year-long-attack>

<sup>10</sup> [https://www.pcworld.com/article/250532/youporn\\_data\\_breach\\_exposes\\_1\\_million\\_user\\_logins.html](https://www.pcworld.com/article/250532/youporn_data_breach_exposes_1_million_user_logins.html)

<sup>11</sup> [https://www.theregister.co.uk/2012/03/12/smut\\_site\\_hacked/](https://www.theregister.co.uk/2012/03/12/smut_site_hacked/)

<sup>12</sup> <https://www.cnbc.com/2016/09/07/alleged-data-breach-exposes-almost-800k-brazzers-porn-site-users.html>

## Risks associated with data breaches

Sexual information is private for a reason. Data relating to “an individual’s sex life or sexual orientation” is rightly granted special treatment by the forthcoming Data Protection Act 2018. Many people have secrets to keep, and the consequences of privacy breach can be catastrophic.

The data breach of extramarital affair dating site Ashley Madison<sup>13</sup> is a sobering example. The site failed to keep user data secure, resulting in a breach that led to scandal for politicians and CEOs, blackmail, identity fraud, and suicides.

The Ashley Madison data breach is a clear warning of what can happen when people’s sex lives are leaked into the public domain. Far more people view online pornography than were registered with Ashley Madison, and so the potential scale of harm is substantially larger. If age verification solutions are not forced to protect user privacy, there is a genuine risk of widespread loss of life.

An international porn database would be a tempting target for hackers seeking to cause scandal and reveal the porn habits and emails of politicians and public figures. There exists a market for lurid sexual exposés, and the British tabloid press have a proven track record in ruining lives to sell newspapers.

But it’s not only public figures who stand to suffer in the event of a large-scale porn data breach. The most marginalised members of society have even more to fear. The kind of sex people like to have, and fantasise about having, can have extraordinarily high stakes for those at risk of homophobia and transphobia. LGBTQ people who are not out to their families stand to lose their homes and their relationships. In the case of young or vulnerable people living with parents or guardians, being outed poses a very real risk to their survival.

Consensual adult sexuality encompasses a huge range of legal activities, and yet many sexual subcultures continue to be vilified in the UK. People who are outed as queer, trans or enthusiasts of BDSM risk being publicly shamed, bullied and mocked, including by the press, losing their job or facing threats and violence. There are no UK laws protecting the rights of people into BDSM from discrimination, and if they are revealed, our consensual and private sexual activities can get us fired. For many of us, privacy is not a luxury but a matter of survival. At present there is no discussion of these risks by the BBFC, the DCMS or the ICO. If they are to be taken seriously as regulator, the BBFC must show that they understand these risks and are working hard to mitigate them.

---

<sup>13</sup> <https://digitalguardian.com/blog/timeline-ashley-madison-hack>

## Lack of redress

The BBFC claim in section 1.13 that they do not accept liability for any loss or damage. If a database of people's private sexual preferences linked to identifying markers is leaked or hacked, no means of redress are available. Once out, the cat cannot go back in the bag.

Financial redress is poor consolation for those who have lost loved ones to suicide, but the BBFC may be held financially accountable if their failure to protect privacy leads to loss of life.

## Do you have any comments with regards to Chapter 4?

Age verification for online porn creates a new technical space with unique privacy and security needs, and requires new privacy and security standards uniquely tailored to these circumstances. However Chapters 3 and 4 describe no mandatory privacy standard which age verification software must comply with. The basic legal minimums enshrined in the General Data Protection Regulations (GDPR) are insufficient to ensure the privacy of people using age verification.

Throughout the Guidance, the BBFC defer privacy concerns to the ICO, creating a tremendous regulatory gap which fails to hold age verification providers to account for protecting users' privacy.

### Insufficient security standards

It's a really bad idea to habituate the British populace into bad security patterns, such as giving random websites permission to see their social media details, phone number and credit card details.<sup>14</sup> Habituating UK internet users to surrendering personal information to gain access to adult content will have lasting implications for cybersecurity. Fraudulent websites will inevitably spring up worldwide urging UK users to submit identifying details, which can then be used for the purposes of identity theft and credit card fraud.

### PCI-DSS

In the case of credit card fraud and identity theft, banks will underwrite losses and compensate victims. Data breaches involving payment card information therefore carry significantly less risk than data breaches involving private sexual information. Nonetheless, credit card information is protected much more effectively via a robust compulsory security standard: the Payment Card Industry Data Security Standard (PCI-DSS).

This defines robust requirements for firewalls, encryption, access controls, what data is visible (both to the user and to the vendor), and personnel background checks. Since age verification data is substantially more sensitive, and data breaches of age verification datasets carry greater risk, data security standards around age verification should be equal to, or greater than, the security standards around credit card transactions.

---

<sup>14</sup> <https://medium.com/@alecmuffett/a-sequence-of-spankingly-bad-ideas-483cecf4ba89>

## PAS 1296

The only standard which exists to protect data collected during age verification is BSI PAS 1296. This is insufficient to protect user data: it says little about security requirements or data protection requirements, and provides no strong enforcement for AV solutions to protect user privacy.

Even the PAS is a voluntary specification; neither the BBFC nor the ICO are going to enforce it. Without mandatory privacy protections, there will be little incentive for age verification providers to comply with the recommendations of the PAS.

## Data protection

GDPR provides a certain baseline privacy standard. However, Facebook is a good example of how easily an online company can persuade users to share their data - and the Cambridge Analytica scandal reveals the risks of trusting private companies to respect the conditions on which data is shared.

An AV provider interested in collecting sensitive data while complying with GDPR may create enticing user experiences; one can easily imagine PornHub asking users something like, "Do you want us to provide you with personalised porn recommendations?"

Compliant data re-use might be achieved by requiring impatient users to blindly accept a Terms of Service or Privacy Policy document before they were allowed to use the service they were trying to access. Once a user is invested in a service and habituated to using it, they are incentivized to accept new terms of service even if they would not have consented to them originally.

Data protection law is simply not designed to govern situations where the user is forced to agree to the use of highly intrusive tools against themselves.

## The need for robust security standards

Users cannot be expected to take it on faith that age verification providers will be trustworthy - either that they will have good security goals, or that they will be capable of meeting them. Companies may claim that they are interested in protecting user privacy, but regulatory oversight is required to ensure that they do.

Good security practice consists of baking security into the protocols. If age verification providers can't collect or retain sensitive user browsing data because the protocols prevent them from doing so, this would be best practice.

There are a number of ways to build protocols that achieve this. Here are just a few:

Blinding: replace durable, transparent names (of e.g. users or websites) with short-lived, opaque identifiers.

Minimum data: the transaction does not require any more data to be transferred than is absolutely necessary.

Separation of authority: avoid aggregation; each authority only sees the minimum amount of data.

Least privilege: grant exactly the amount of privilege (permission to do something) required for the transaction, and no more. Every privilege granted opens more surface for attack.

In the case of AgeID, the system fails to employ any of these basic security protocols. User data is not blinded; AgeID can connect an age verification transaction to an email address and password. Website data does not seem to be blinded either; MindGeek *could* if they wanted access or retain the list of websites that a given user has accessed via AgeID, and we merely have to take it on trust when they say they won't. As a content provider and an AV provider, MindGeek does not have separation of authority; the same company will own your Pornhub, Digital Playground and Brazzers account details, which might well contain your credit card details and other information, and your AgeID account.

## Conclusion

The unique risks of age verification are largely outside the scope of GDPR. Given the high stakes involved, and the lack of potential for redress, the Government have a responsibility to *prevent* data breaches, rather than simply waiting for the ICO to “highlight compliance concerns” once they have already occurred.

To avoid catastrophic data breaches, a new privacy and data security standard must be created which fulfils the unique needs of age verification, and plugs the gap left between the BBFC and the ICO. The BBFC should call upon the Government to establish mandatory privacy and security standards in legislation, similar to PCI-DSS, which age verification providers must comply with. This would require a body - either the BBFC or another organisation - empowered to regulate age verification providers and ensure compliance with these standards.

## NICHOLAS BOND

Subject: Age Verification Guidelines

Dear consultation team,

While I have no inherent objection to preventing minors from accessing unsuitable material, such as pornography, the current proposal to require individual websites to adhere to an Age Verification system is unacceptable.

There should be no requirement for websites to retain any personally identifying information. Sex, sexuality and pornography are highly sensitive topics. Setting up a system whereby insecure websites must collect the personal information of all its' users for 'age verification' purposes will result in creating a trove of potential blackmail material that will become a huge target for those with malicious intent.

Further, as it stands, the operators of the websites have no requirement to protect the personal information you are proposing to force them to collect.

Beyond the issue of requiring websites to censor themselves, tech savvy individuals will always be able to find a way around such a broad-brush approach, by using unregulated websites, VPNs based in other unregulated countries, or TOR / darkweb browsers.

If there is no solution other than Age Verification, then it should be run through a highly secure, anonymized, central system, so that individuals are not identifiable to the websites. Something similar to a blockchain system, where users only need to register in one central location, and can then use their individual code to verify their age, and the website will have to download the entire blockchain to cross-verify the user.

My name and response does not need to be confidential.

Sincerely,  
Nicholas Bond

## CAMILLO BOSCHETTI

Subject:

Dear consultation team,

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible. My name and response does not need to be confidential.

Sincerely,  
Camillo Boschetti

## PAUL BOWDEN

Subject: Privacy concerns

Dear consultation team,

My name and response does not need to be confidential.

I am very much opposed to any organisation, private or public knowing what I view legally on the internet.

There have been far too many breaches of data in recent memory for me to be comfortable for anyone collecting my adult preferences.

In addition this is very much a nanny state over reaction and I do not concur that any of the plans being put into place will actually help alleviate the issue.

I also object to the amount of public money which will be spent on this exercise and feel the funds would be better utilised funding our police force to combat sexual exploitation instead of unfairly demonising legal sex work and producers in the UK.

Sincerely,  
Paul Bowden

## LORNA BOWMAN

Subject: Storing Data in Risky

Dear consultation team,

I'm very concerned about the lack of privacy required for organisations to implement the new age verification rules. The age verification process is fine, but I don't believe that any information from that process should be retained by the organisations beyond the requirement to verify. To hold that information for any length of time makes the information (i.e. people's identity) vulnerable to theft as a very basic risk. Much more frightening though is that if that information is held alongside data concerning people's online footprint - and therefore it is also vulnerable to hacking, selling as we've seen recently, or inappropriate reuse.

Please take the time to make clear what information MAY and MAY NOT be held, and for how long. Also what is an appropriate duration for any permitted storage, and what the penalties for leaking data will be - and how this will be enforced. To not store the data protects both individuals AND the companies who won't be hacked for data they don't have!

My name and response does not need to be confidential.

Sincerely,  
Lorna Bowman



DAVID BOYDON

Subject: Age Verification privacy

Dear consultation team,

My name and response does not need to be confidential.

If the government is going to go down the route of age verification and will place the standards of this with yourselves the BBFC then the government and yourselves should enact in law strong regulations for the data collected from the AV systems, to be protected as strongly as possible by both technology, encryption, secure storage of the data etc and by regulations with strong laws / rules for miss use of this data and to protect peoples privacy.

I also see no way that any of this can be inforced or controled for web sites overseas, as these would be covered by the laws of the country where the server is sited, unless you are consulting industry in other countries looking to get some details to shape the AV system based on there laws.

German operates an AV system but it only covers the sites in German that their government think need some type of AV because the content is of a stronger nature, but sites outside Germany are free for people to go to if they want to.

Sincerely,  
David Boydon

## REBECCA BRADSHAW

Subject:

Dear consultation team,

Come on!

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Rebecca Bradshaw

## SUE BROCK

Subject: Privacy

Dear consultation team,

I am very concerned that in requiring adults to provide proof of age before accessing pornography on line will leave them exposed to companies and so on who may obtain their details? If proof of age goes ahead then I feel that there should be very strong privacy arrangements to ensure that adults viewing legal pornography are protected and their privacy maintained. The Cambridge Analytica scandal shows how easily this could happen.

Thank you.

My name and response does not need to be confidential.

Sincerely,  
Sue Brock

CHRIS BROWN

Subject: Privacy concerns

Dear consultation team,

I have concerns about the proposed age verification plans. The information of people whose data would be collected could be extremely sensitive and yet privacy seems to have been a secondary concern, rather than a primary concept. I also fear that the plans seem to be largely reliant on one company (mindgeek) providing the verification service as well as the burden of the new regulations would fall hardest on smaller independent companies.

My name and response does not need to be confidential.

Sincerely,  
Chris Brown

FERGUS BROWN

Subject: Maintain privacy for AV

Dear consultation team,

With the recent privacy scandal of Cambridge Analytica, it is clear that companies cannot be trusted with our data and strong privacy regulation must be put in place. Private records of viewing habits must be kept private.

My name and response does not need to be confidential.

Sincerely,  
Fergus Brown

## JOLYON BROWN

Subject: Age Verification - public comment

Dear consultation team,

For your public consultation on age verification for pornographic websites, I would like to register grave concerns about how this will operate.

The existing proposal does not safeguard privacy and in light of the Cambridge Analytica incident I urge a rethink.

The age verification process could easily be used to record individual habits for accessing porn. The inevitable breach of this data would be catastrophic for the public.

There must be a set of strict privacy guidelines for companies enacting age verification. Recent headlines show that without them private companies will simply not safeguard this privacy and there will be an eventual leak or hack which will lead to this data being made available.

Please make privacy a central plank of this requirement to have private companies enact age verification.

My name and response does not need to be confidential.

Sincerely,  
Jolyon Brown

## RICHARD BROWN

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Richard Brown

## CALUM BROUGH

Subject: Age verification

Dear consultation team,

This age verification stuff is laughable. You're expecting people to entrust their personal information to an industry that has historically used such age verification techniques for Identity theft. The law is also practically unenforceable

My name and response does not need to be confidential.

Sincerely,

Calum Brough

## MARK BYRNE

Subject: Privacy

Dear consultation team,

I am very concerned that there appears to be no privacy requirements built in to the Age Verification process that you are nominally in charge of. I do not wish data about my internet viewing habits to be collected by private companies with no control over what they do with this information whatsoever.

My name and response does not need to be confidential.

Sincerely,

Mark Byrne

## STAWBS CAMPBELL

Subject: Re: strong privacy is a must for age verification technology

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,

strawbs Campbell

MICHAEL CARRITHERS

Subject: Re: age verification tech

Dear consultation team,

As we have learned recently, giving our personal information to private companies is the road to disaster. They cannot be trusted because there are no substantial restraints or tests on how they use our personal data.

Protecting minors from harmful content is important, but giving our personal information to private companies is not the way to do it.

My name and response does not need to be confidential.

Sincerely,  
Michael Carrithers

BERNARD CARNEY

Subject: AV Tools

Dear consultation team,

Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines. It is in the BBFC's interest to make sure AV tools protect the public's privacy.

My name and response does not need to be confidential.

Sincerely,  
Bernard Carney

## MATTHEW CHAMBERLAIN

Subject: 'Digital Economy Act' Consultation

Dear Sir/Madam,

In regards to the 'Digital Economy Act', I am in agreement with many elements of the act outlined in chapters 2, 3 and 4. With regards to chapter 3 concerning age verification of adult content I understand the importance of keeping children safe online, however I am concerned about how age verification is going to be implemented. I feel that there needs to be consideration towards the safety of adults who access adult websites or applications regarding their personal and financial details. I am concerned ID security could be put at risk by the storage of ID, particularly in the form of passport image uploads and I would also like to stress that Credit Card checks should not be considered as not all adults possess Credit Cards as you may be fully aware. I am also concerned about the possibility of payments to adult sites being described as an adult product on bank statements as this would infringe upon customer privacy which I strongly believe should be respected.

I hope my concerns will be considered in your response to this consultation.

Yours Faithfully,

Matthew Chamberlain.

## NEAL CHAMPION

Subject: Concerns over age verification tools

Dear consultation team,

I am extremely concerned about the intended age verification (AV) requirement which the BBFC will be in charge of overseeing. While I understand the concerns over people under 18 accessing pornography, the creation of a huge dataset of highly sensitive personal data is an enormous risk.

I would like to make the following points:

- between the BBFC and the ICO, it is not obvious who is responsible for privacy in this area
- almost every week, one reads about data breaches from private companies
- it's difficult to imagine data more sensitive than that about individuals personal viewing of pornography
- this is a poisoned chalice for the BBFC, who will be scapegoated when the inevitable breach occurs

My name and response does not need to be confidential.

Sincerely,  
Neal Champion

CHRIS CHEETHAM

Subject:

Dear consultation team,

My name and response does not need to be confidential.

This is in response to your consultation on the issue of age verification for pornographic websites.

I have no problem with the argument that children and young people need to be protected from pornography on the internet.

However, I have great concern over the issue of age verification and how it is carried out. My first concern is that many parents who do not understand technology will rely too heavily on the existence of a government approved age verification system to keep their children safe. This would be a great failure as the system works imperfectly for films and there is no reason to believe it will work any better for the internet.

Secondly there must be concerns that any system which collects data on the viewing habits of people on the internet would be open to breaches of security, either from within companies or by outside agents. Given that what has happened with other companies with a strong interest in security the idea of such a breach is not fanciful.

Frankly bland assurances from companies and public bodies are not worth the paper they are printed on. It is essential that the systems put in place are robust and regard user security and privacy as the just as important as the issue of age verification. The privacy guidelines must be strict and enforced as the slipshod approach of companies like Facebook shows that companies can and do pay lip service to privacy issues when it is not legally enforced.

Finally, I would hope that government experience of recent scandals such as the "Windrush generation" would convince government and public bodies that policies need to be viewed in the round and that unintended consequences may be more serious than imagined. Any breach of security leading to the release of private viewing habits would I am sure be another public relations disaster for the Government who would quickly shift the blame to the BBFC and the Information Commissioner. Your self interest may well lie in making public privacy a key aspect of any proposal.

Sincerely,  
Chris Cheetham



## CHRIS CLAY

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Chris Clay

## GRAHAM COBB

Subject: Age verification providers must not be permitted to hold records of sites/companies/content visited

Dear consultation team,

Age verification for access to porn has the possibility to generate massive amounts of personal data which could not be more sensitive.

Previous data breaches such as TalkTalk, Ashley Madison, Equifax and even Cambridge Analytica would pale in comparison to any leak of personal sexual habits and interests on the majority of UK families.

And, for anyone in the public eye such as politicians or celebrities, the data would have extremely high value either for exposure or for blackmail. The value would be so high that an insider will always be found to provide the data.

The regulatory environment needs to be watertight, with no possibility of finger-pointing between regulators or regulatory requirements lost "in the cracks". It would be a disaster if the BBFC, ICO and the government do not create a seamless, powerful and effective regulatory environment.

When the first breach occurs, and the public realise the impact on their families, it is the BBFC who will get the blame. It is critical that any approved AV tools must have extremely powerful and effective privacy regulation addressing not only storage and external threats, but insider attacks and, of course, completely disallowing any commercial use or communication of any AV-related data.

My name and response does not need to be confidential.

Sincerely,  
Graham Cobb

## PAUL CODD

Subject: Privacy protection shouldn't be an afterthought

Dear consultation team,

Privacy protections should be in front and centre in any Age Verification scheme. The government cannot abandon its duty to protect its citizens. Unfortunately it seems that privacy has been completely forgotten or sidelined in the way the AV scheme has been conceived.

Nobody should be at any risk of having their sensitive personal documents such as passport intercepted, hacked, leaked, or stolen.

Most important of all nobody should be at any risk of having their identity linked to their internet use, porn or otherwise.

My name and response does not need to be confidential.

Sincerely,  
Paul Codd

## NATHAN COLLINS

Subject: Age verification by private companies

Dear consultation team,

In order for private companies to be able to verify a person's age they will need to be able to access private personal information. It is essential for privacy and security reasons that this information is not stored by private companies, nor should they be permitted to use this information for marketing or profiling purposes.

If the Government is going to issue requirements for private companies to verify users' age, the Government should take responsibility for ensuring that this information is used only for the intended purpose.

My name and response does not need to be confidential.

Sincerely,  
Nathan Collins

MAL COLMAN

Subject: Strong Privacy

Dear consultation team,

The Cambridge Analytica scandal over personal data and how it is collected reminds us how important privacy is.

With Age Verification technology collecting data in huge amounts any breach could be catastrophic for individuals wishing to remain private.

Companies in the private sector are capable of disregarding user privacy as witnessed recently. Such breaches of data occurring again following a regulatory gap with no guidelines is unconscionable. Please make sure AV tools protect the public's privacy.

My name and response does not need to be confidential.

Sincerely,  
Mal Colman

STEVE CONNOR

Subject: Age verification concerns

Dear consultation team,

I understand the concerns about under 18s being exposed to porn on the internet, but the idea of providing proof of age by means of passport, driving license or credit card details is a mistake.

I'm nearly 65. I don't have a passport or a driving license and I'm certainly not going to get a credit card just to access certain websites.

Then of course there is the issue of these details being obtained by third parties which has been happening in the past and continues to do so.

These issues need to be addressed before any action is taken.

My name and response does not need to be confidential.

Sincerely,  
Steve Connor

JOHN COSSHAM

Subject: Vetting porn consumers.

Dear consultation team,

I use pornography sometimes and want to continue to be able to do that. I do not have a passport or driving licence, and my money is in a building society account with a passbook. So as far as I can tell, your plans to 'verify' my age, who I am, inside leg measurement etc isn't going to work for me, and I might have to resort to a work-around such as Tor, or some other not-very wholesome approach to view the 'pretty ladies' that I sometimes like to do.

I'd much rather vulnerable people were protected by having parental controls, and what the industry already does which is to block images etc such as bestiality, 'at source' rather than at the consumer end.

I feel that if you make access to pornography difficult, people may resort to image-sharing platforms which are not controlled by the porn sites' obligations to vet users.

I urge you to look again at how we keep vulnerable people 'safe' and away from 'corrupting' images.

My name and response does not need to be confidential.

Sincerely,

John Cossham, age 51

JAMIE COURTNELL

Subject:

Dear consultation team,

This is a flawed and frankly reckless system. It should not be up to the websites to self-regulate the age of it's visitors, instead this should be the onus of parents and guardians.

I strongly urge you to reconsider and revisit the problem with a fresh, modern perspective.

My name and response does not need to be confidential.

Sincerely,  
Jamie Courtnell

JACOB COX

Subject: Age Verification

Dear consultation team,

It is vital that there are clear, strict guidelines in place to retain our privacy online. We cannot leave collection of personal data up to the whims of the market.

Whilst young people must be protected, everyone has a right to privacy online, so the public need government reassurance that our data will be kept safe.

My name and response does not need to be confidential.

Sincerely,  
Jacob Cox

## ANDREW CROWTHER

Subject:

Dear consultation team,

Ensuring children and young people are protected, educated and given parental care is vital, however we have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Andrew Crowther

## MATT CUMMINS

Subject: Privacy with regards to Age Verification technology implementation

Dear consultation team,

Given the many recent data breach scandals, chief among them the Cambridge Analytica fiasco, it is imperative that if age verification technology is to be implemented in order to view adult material in the UK, privacy must be of utmost importance in its design.

Trusting private companies to responsibly handle the kind of documents that could meaningfully verify a user's age is at best reckless. This could effectively create a series of unregulated data caches containing highly embarrassing information linked directly to law abiding UK citizens, and the inevitable data breaches that -will- eventually occur could prove absolutely catastrophic to some people in sensitive positions.

Please strongly consider the ramifications of not implementing this technology in a considered, thoughtful and secure manner when making your decision. The citizens of the UK deserve at least that much.

My name and response does not need to be confidential.

Sincerely,  
Matt Cummins

## GEOFFREY CURL

Subject: Age Verification and Privacy.

Dear consultation team,

It is in the BBFC's interest to make sure Age Verification tools protect the public's privacy. However, between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee.

Age Verification tools will potentially create a record of the public's private habits. The consequences of a breach would be catastrophic for millions of UK citizens. In light of the Cambridge Analytica scandal, it can be seen that private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

My name and response does not need to be confidential.

Sincerely,  
Geoffrey Curl

KAMIL DABROWSKI

Subject: Age verification consultation

Dear consultation team,

It is a crucial matter to consider the full process and potential side effects of implementing any technology, especially so when it comes to the national level. Doubly so when it comes to controlling Internet traffic.

Questions the type of:

- who is responsible for keeping secure the private details of visitors
- what standards must the AV solutions meet regarding security and quality
- how can one remove their pornographic site history from the site database, if at all
- what will be the penalties for negligence or failing to fulfill the above requirements
- what results similar efforts had in the past
- how will that change the behavior of site visitors, i.e. what will be the side effects

and many more must be given proper consideration.

Please take time considering those issues. I'd suggest seeking independent third-party technical consultation if possible.

I want my name and response to be public.

Sincerely,

Kamil Dabrowski



ALAN DAY

Subject: Strong privacy is a must for age verification tech!

Dear consultation team,

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens, this is liable to be a target for infiltration of the database, privacy must be a priority but also the data needs to be anonymized because the government has a very poor record on data protections.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy, neither the BBFC, ICO or any other government body can be trusted in regards to this.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines, however neither UK private companies can be trusted let alone overseas private companies.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible, both should be held accountable and where a breach of information does occur then adequate compensation is required, not the usual government response where some lowly civil servant takes the fall and the government says that it will learn from the mistakes, this is only being done as the government wants to censor the internet and to control what people view online, it has nothing at all to do with protecting children, it is just the start of bigger things to come, the UK is fast catching up with the like of China and Russia in the censoring of the internet.

My name and response does not need to be confidential.

Sincerely,  
Alan Day

STEPHEN DICKINSON

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Stephen Dickinson

## PHILIP DIXON-PHILLIPS

Subject: Give in to these requests

Dear consultation team,

I sign this petition as I believe in the sentiments expressed in it, so please act accordingly instead of dismissing points raised and riding rough-shod over us?

My name and response does not need to be confidential.

Sincerely,

Philip Dixon-Phillips

## BERNARD DOHERTY

Subject: DEAct

Dear consultation team,

Recent failures to control the unwanted exploitation of personal data held by companies have been distressing enough. In those case, the relevant companies can be held accountable. At the moment, the UK government is about to insist that various online companies hold excessive data about individual users without establishing any secure standard about how that information is to be held.

It is apparent that the legislation was issued by people with little comprehension of the practical difficulties they were creating or the dangers for the future. I hope that your team will insist on adequate safeguards to protect the privacy of users of all online services, including providers of pornography.

My name and response does not need to be confidential.

Sincerely,

Bernard Doherty

## JONATHAN DORE

Subject:

Dear consultation team,

It's very worrying to see the proposal to introduce compulsory identifying information as a requirement for viewing legal material on the internet. If this principle is conceded, what is to stop its application elsewhere, for instance to expressions of certain political, scientific, or religious views?

If identifying information exists, someone, somewhere will be recording it, and the apparatus for future exploitation of that information will have been put in place. That return to a pre-20th-century view of restricted and bureaucratically overseen personal liberty is unacceptable in a modern democracy.

My name and response does not need to be confidential.

Sincerely,  
Jonathan Dore

## MARTIN FARROW

Subject: Age Verification

Dear consultation team,

Ashley Madison. The age verification system should be designed with unassailable privacy to avoid an Ashley Madison event.

The human rights act grants individuals the right to privacy therefore a Government enforced age verification system if not subject to very strict controls and remedies, seems likely to me to almost certainly to compromise an individuals human rights.

The BBFC should consider a trapdoor mechanism for one time verification followed by anonymous access (in much the the manner as our voting sytem works). This would mean verifying, then destroying the verification data and granting the user an access token - so that there will be no way of linking a users access to their identity which to my mind is the key human rights issue.

Cambridge Analytica shows how data can be misused and it seems to me that if not securely and legally protected, a persons completely legal private viewing habits could be used to force compliance to an assumed public moral code - again a breach of human rights.

My name and response does not need to be confidential.

Sincerely,  
Martin Farrow

JOE FEELY

Subject:

Dear consultation team,

I don't watch porn, but I do care about peoples right to privacy and the right to not have their personal information misused.

Age verification (AV) as a requirement comes with many risks, which could be reduced if peoples data is protected. Achieving this protection is very difficult. Unless there are stringent requirements on such entities that are tasked with providing such protection, there will be less effort to achieving it.

The laws requiring AV do not require such protections. This clearly needs to be fixed before applying such laws, or the more sure way to protect users data is to not require AV.

Aside form the above which is fraught with technical difficulty, younger people would very quickly find ways around it.

My name and response does not need to be confidential.

Sincerely,

Joe Feely

WILLIAM FENNELL

Subject: Age verification

Dear consultation team,

In the light of the recent Cambridge Analytics scandal, I am very concerned that the Digital Economy Act does not make clear the level of confidentiality required for the information that will be collected. While much of the publicity relates to keeping under-18s off porn sites, there are other areas where a digital ID will be required. Having seen what can be done with non-sensitive information, I am very concerned that the Age verification (AV) procedures and tools should have high standards of security and privacy enshrined in law. Some of the context in which this information is collected may be very sensitive as far as the "customer" is concerned, and the verification medium (e.g. passport number) sensitive in itself from the point of view of protecting against fraudulent use of ones personal details.

The BBFC should be insisting on the highest levels of privacy and security for the AV tools.

The gap between the BBFC's and the ICO's remit in terms of privacy needs to be plugged, otherwise unscrupulous operators will plunder private information.

This is even more important now that the Cambridge Analytica affair has shown how much data can be used.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

Also, it is not just in porn and other matters that AV will become used. We can expect to see it being used on ordinary retail websites to check on the purchase of alcohol, knives and other items that are age restricted.

Do not let slapdash and careless drafting allow a coach and horses to be driven through the privacy and security we are trying to ensure.

My name and response does not need to be confidential.

Sincerely,

William Fennell

STEPHEN FLAHERTY

Subject: Age Verification for Adult Sites

Dear consultation team,

I am writing in response to the proposal for Age Verification to be built into Adult Sites.

Firstly, I think this is a bad idea. It won't do what it is meant to do - children, most of whom are more 'tech savvy' than their parents will be able to circumvent it with the use of proxies, VPNs, IP masking tools and no doubt other methods. However, more important than its inefficiency is that it presents a serious risk to those who go through the AV process. They will be forced to hand over documents such as driving licenses and passports to companies who have been given no guidelines or standards on how to store and use said data. The risk of a security breach and subsequent ID Theft is considerable. Or other abuse of data.

If the government is determined to go on this Fool's Errand then, at the very least, safeguards for the security and privacy of the AV Data must be built in.

My name and response does not need to be confidential.

Sincerely,

Stephen Flaherty

## DR JOÃO FLORÊNCIO

Subject: Consultation on porn sites age verification

Dear consultation team,

Requirements for pornographic websites to verify UK users are over 18 will come into effect soon, and the BBFC is in charge of issuing guidance for how age verification (AV) tools must operate. Ensuring children and young people are protected, educated and given parental care is vital, however I have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

This is all the more concerning given the news that the company MindGeek—owner of most porn tube sites and several porn production studios, as well as a secretive company with unclear business activities and suspected of money laundering and tax avoidance/evasion—may be contracted to provide AV systems in the UK under the new act of Parliament.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. This is all the more concerning given our unclear understanding of the aims, scope and business carried out by MindGeek. In that context, there is no excuse why the Government should not be prioritising privacy for AV technology.

The reasons for that are that AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens and their right to privacy.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

I urge you to take my concerns on board and devise a way to ensure that the providers of AV systems will comply with their duty of protecting the privacy of users by keeping their data confidential. not sharing it with third-parties, now using it for any other purposes other than AV.

My name and response does not need to be confidential.

Yours sincerely,

Dr João Florêncio

Lecturer in History of Modern and Contemporary Art and Visual Culture  
University of Exeter

## ROWENA FOOTE

Subject: Privacy protection must be integral to Age Verification tools

Dear consultation team,

Under current proposals no organisation has been assigned to oversee the privacy of those who use adult websites. In addition, the Government has made no plans to issue strict privacy guidelines to internet companies for the protection of privacy to be built into AV technology.

Given that the private internet companies are being tasked by the Government with devising AV tools for adult websites and given the appalling example of Facebook collecting billions of private records in its interaction with Cambridge Analytica, there must be **STRICT STATUTORY REGULATION TO PROTECT USERS' PRIVACY, INCLUDING THE CREATION OF A STATUTORY BODY TO ENFORCE THE PRIVACY GUIDELINES.**

If the BBFC fail to ensure that the Government takes these steps, then - when the inevitable serious breach of privacy takes place - the public will, rightly, blame both the Government and the BBFC.

My name and response does not need to be confidential.

Yours sincerely,  
Rowena Foote

## GEORGE FORRESTER

Subject: Age verification (AV) tools

Dear consultation team,

Age Verification tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

George Forrester



## BEN FOUNTAIN

Subject: Age classification on websites

Dear consultation team,

The concept of AV on websites is contentious, with many regulatory and technical challenges.

Introducing such controls would result in a reduction in privacy for those adults who wish to view such perfectly legal material. Any technical method that provides sufficient assurance also provides sufficient impact to privacy that it is a matter of concern.

Whether the government is aware or not, the UK is not a leading hosting location for websites. That is the entire point of the internet as a transport method. Given the woeful enforcement of existing regulations, this will just be another series of websites that would operate from the grey fringes of the internet. The impact this will have on the police ability to enforce the commonly accepted legal controls around child exploration will only be reduced as a result of this action.

Rather than further dabbling with citizens privacy, the government would be well advised to engage in the wider debate, and consider whether to establish a .xxx.uk domain, in order to facilitate better blocking technologies.

My name and response does not need to be confidential.

Sincerely,  
Ben Fountain

PETER FOX

Subject:

Dear consultation team,

I would like to bring to your attention the issues of using age verification.

While I respect the intentions of this bill I've yet to see an evidence age verification will be effective in performing the task.

As a teenager I was frequently able to bypass "safety" lock outs in a number of ways, from being able to bypass the pin codes to view adult TV on freeview or through using a debit card to buy games online while under age. These skills luckily helped me to go on to earn a degree and masters in Computer Science but I've also seen the otherside where this has gone towards helping other become cyber criminals.

The system proposed seems to rely on centrally stored data which will be fine for the average person but those who have more specific fetishes will likely not want their name attached to what they view. This will likely lead to a bigger dark web of content that the government cannot control, with more people learning how to access it and use it securely. This might be even more damaging if more of our young people go down this path.

We need to have systems in place to guarantee the privacy of online users. A central copy of this data is a gold mine to criminal elements who would use it for extortion. We have seen time and again that breaches can and will occur.

I would recommend that the BBFC takes more time in implementing these steps to ensure that a system with assurances is produced which holds the correct people to account in the event of a breach.

My name and response does not need to be confidential.

Sincerely,  
Peter Fox

NICK FREWIN

Subject:

Dear consultation team,

I strongly believe there should be strict government guidelines on privacy for the AV tools, especially in light of recent scandals such as Cambridge Analytica.

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

Nick Frewin

## MARCUS FREWIN-RIDLEY

Subject: Age Verification

Dear consultation team,

I am deeply concerned about the plans to bring in mandatory age verification for adult materials. Everything points to this policy being unworkable and damaging. Small business such as my own will be adversely affected by having to pay for this, especially if we are forced to use a solution created by our competitor Mindgeek, who have every interest in hobbling and profiting from their competition, particularly through data farming and mobilisation as they already do. This must be made impossible by the wording of the legislation, if it must go through, and it must be made clear who exactly is affected, for with the current wording it seems sex blogs and sexual health advice videos are as affected as hardcore sites. This must not turn into FOSTA/SESTA like situation in the states, under which huge amounts of business are treated as under the same umbrella forcing people into poverty and dangerous underground work.

Campaigning by Pandora / Blake, Myles Jackman, and ORG has shown this policy to be unnecessary and damaging, but if it really must go through, there is so much more that needs to be done. To summarise:

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

Marcus Frewin-Ridley

## EMMA FROST

Subject: Strong privacy is a must for age verification tech

Dear consultation team,

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Emma Frost

## JENNIFER GARNETT

Subject: Age verification

Dear consultation team,

Many people are concerned about the changes to take place, what it means for porn producers and viewers. As a parent, I feel measures are adequate enough as they are. As an adult I am concerned about privacy, data safety, fraud and incomes of those in the industry.

My name and response does not need to be confidential.

Sincerely,  
Jennifer Garnett

## TIM GERSHON

Subject: Privacy and age verification

Dear consultation team,

I am pleased that there is a consultation on the important issue of age verification. There is a clear public interest in preventing under age individuals from accessing inappropriate material on the internet. This is matched, in my view, but the necessity to ensure that this is done in a way that does not compromise each individuals right to privacy. Given recent events in the news, in particular those concerning Cambridge Analytica and Facebook, it is all too easy to imagine how some unscrupulous companies might take advantage of access to age verification data if they are able to obtain it. Therefore, the BBFC and the government must make strong privacy a central requirement of any technology used to restrict or enable access to material on the internet.

My name and response does not need to be confidential.

Sincerely,

Tim Gershon

## TOM GILLESPIE

Subject: Privacy rights

Dear consultation team,

I need proper privacy rights if I am required to verify my age on certain web sites.

What guarantee can you give that makes the use of my details illegal if used by any other agency.

Since we have been reading about Cambridge Analitacal harvesting people's data ,what assurances would you put in place to reassure me that the same will not happen to me if I use the internet.

T. Gillespie

My name and response does not need to be confidential.

Sincerely,

Tom Gillespie

## BARRY GRAHAM

Subject: AV Tools

Dear consultation team,

The entire process is a joke, but if it does happen and looks likely then in light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

My name and response does not need to be confidential.

Sincerely,

Barry Graham

## CHRISTIE GRINHAM

Subject: Age verification creates a dangerous pretence for ID verification

Dear consultation team,

Age verification for pornographic websites presents a dangerous pretence to general ID verification to use the internet. People should be able to access the open internet without being identified or tracked. Children's access to the internet should be the responsibility of their parent or guardian, I realise not all have the technical knowledge to achieve this, the money should be spent on creating this knowledge instead. This will also make a more technically knowledgeable population which is desirable for the future.

My name and response does not need to be confidential.

Sincerely,

Christie Grinham

AMY GUNN

Subject:

Dear consultation team,

I am writing in response to the proposed Age Verification laws.

My views, however ineloquently worded, are strongly opposed to this legislation going forward.

Adults should be allowed to access pornography without surrendering their personal, financial and sexual details which makes them vulnerable to breach of privacy and public shaming.

Gathering data based on which porn websites users visit will be information begging to be hacked.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

Placing age verification tools (such as AgeID) in the hands of companies like MindGeek mean that the biggest supplier of mainstream pornography has more access to users porn watching habits. This gives even more power to companies perpetuating a standard of sexual behaviour that should not be the norm - or how teens and adults understand how to have sex.

Mediating access to porn based on age should be done through sex ed in schools and proper education for parents - not by holding the sexual habits of consenting adults hostage to private companies.

My name and response does not need to be confidential.

Sincerely,  
Amy Gunn



CALLUM HALL

Subject: Privacy for AV is a must

Dear consultation team,

Pornography is part of my life. I'm not embarrassed about that. If there were to be a leak, I would not be ashamed that it came out that I watched porn.

HOWEVER, I would be worried about the exposition of my sexual orientation, kinks and viewing habits. This is information which should be given the highest possible regard and be considered as sensitive or more than bank details and other information which has the potential to ruin lives.

I implore you to take the security of AV age identification seriously, as the consequences of a leak could be devastating to millions of UK citizens who were doing nothing wrong.

My name and response does not need to be confidential.

Sincerely,  
Callum Hall

## RICHARD HARRIS

Subject: Age verification

Dear consultation team,

Indiscriminate requirements for age testing for porn graphic site puts vulnerable people at risk. Almost every major site has been hacked at some point. Of each site has a record of who uses it, this puts people at risk all over country and when they travel.

I am strongly opposed to the concept and the proposed implementation of it.

My name and response does not need to be confidential.

Sincerely,  
Richard Harris

## ANDREW HARRISON

Subject:

Dear consultation team,

While I understand and agree with the government's intentions to limit the access of minors to pornographic material, I feel that merely requiring age verification to be implemented independently by individual sites poses significant privacy problems.

In the wake of the recent Cambridge Analytica scandal, providing private information to purveyors of pornography makes me feel fairly uncomfortable. I would much prefer for the BBFC to consider this issue further with the intention of finding a safer implementation, so as to protect the privacy of UK citizens.

My name and response does not need to be confidential.

Sincerely,  
Andrew Harrison

## PHIL HEMBURY

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Phil Hembury

IAIN HENDERSON

Subject: Privacy and Age Verification

Dear consultation team,

My name and response does not need to be confidential.

The Facebook scandal that will continue to unfold should make it clear that privacy is of critical importance. This must be taken into account in the deployment of age verification technologies.

Sincerely,  
Iain Henderson

MARK HERRIGES

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Mark Herriges

DAVID HICKS

Subject: DEA and privacy

Dear consultation team,

My name and response does not need to be confidential.

As has recently been illustrated by the Cambridge Analytics actions in employing personal data for political ends, it is entirely inappropriate that private companies should be responsible for personal data, some of it very sensitive, gathered for the purposes of the DEA.

It is clear that the BBFC have neither the resources nor the powers necessary to regulate the use and security of information so gathered, and that the proposed Age Verification system will be both intrusive and, as currently proposed, dangerously insecure.

In view of the lack of any clear powers vested in the BBFC and ICO to enforce privacy of user data, however gathered, it is imperative that strict and punitive legislation prevents the misuse or exchange of that data.

Sincerely,  
David Hicks

CHRIS HILLIARD

Subject: My Privacy

Dear consultation team,

We have seen, in the past, what exploitation of sexuality has done to minorities and people in power before.

I live in Wilmslow. The town where Alan Turing ended up being forced by the state to take hormones that lead to depression and death.

We also live in a time where teachers like Lucy Meadows are hounded to death and suicide by organisations due to them being transgender.

Nicholas Goddard was forced to resign from teaching adults at university after he was found to have acted in some pornography films.

The Ashley Madison breach lead to many people who were again, not committing illegal acts, having their private lives intruded upon in a huge way.

Those consequences, in this time, provide a stark reminder that while something isn't illegal, when private activities become public, a lot of damage can be done.

We have now seen how organisations target internet data to use against a population. We have seen how easy it is for a corporation to take data and use it for nefarious and arguably undemocratic purposes. We have seen in the past week that other states have infiltrated numerous computer systems.

The privacy of millions of members of public, their private masturbatory urges, fantasies, and more. That is what is on the line. Material that while not illegal, could be used to devastate someone's life.

The guidelines you put in place with regards to the age verification tools are likely to become the beginnings of a template for other bodies around the world. They need to be bulletproof. They need to guarantee the privacy of members of the public, restrict the flow of history sharing, and put in strong guidelines for security and restriction of the data.

I implore you to consider just how large a job this is, and the consequences of what will happen if breaches are made. How many lives will be devastated once personal fantasies are made public on the front of a newspaper. And do all you can to prevent that from occurring.

My name and response does not need to be confidential.

Sincerely,  
chris hilliard

ROBERT HOOPER

Subject: Proposed new Universal Application for allowing Adult access to Adult Material.

Dear consultation team,

The proposed new Application should be Universal and like other information transmitted online, the information carried must only be statistically culled from traffic that is, in itself, totally anonymous.

Breaches of law remain breaches ONLY within that single Country, thus no other 'responsible Governing source' need ever know about 'foreign breaches' occurring elsewhere.

Perhaps Governments might persuade website providers to restrict 'Adult Material of the most offensive nature' to contain such material strictly within that Country's availability limits. "Regular (legal) Adult Material" can be transmitted worldwide without restriction other than what local laws apply in each sovereign Country.

My name and response does not need to be confidential.

Sincerely,

Robert Hooper

# THE BARONESS HOWE OF IDLICOTE CBE

Dear David

## Response to the BBFC DEA Consultation

Thank you for your email of 26 March regarding the consultation the BBFC is undertaking on the two documents related to the implementation of age verification under the Digital Economy Act 2017 (DEA). Please find my comments below:

### Guidance on Age-verification Arrangements

#### Section 1: Introduction

Paragraph 2 – I think it would be helpful to give more background on who is expected to comply with the Regulations, as I set out in my letter to Lord Ashton of Hyde. I sent you a copy of that letter.

Paragraph 7 – I suggest that “met with the” should read “met the”

#### Section 2: The BBFC’s Approach

Paragraph 5 – I was surprised to read that the BBFC is deciding to prioritise services that “contain potentially indecent images of children” as during the debates in the House of Lords, Ministers made clear that this was the responsibility of the Internet Watch Foundation. I welcome the BBFC’s approach as I have made very clear my concerns about the shortfall in the scope of Part 3 of the DEA, but I question whether:

a) there is potential for conflict between the two organisations. For instance, at Report Stage of the Digital Economy Bill in the House of Lords, the Minister said, “*I do not think that I said anywhere in my remarks that we were extending the remit of the IWF, because it covers non-photographic child sexual abuse images hosted in the UK, and we are not going to extend that—but we will continue to work with the IWF to strengthen the response to child sexual abuse material. **We do not want to open up the scope of the line between the BBFC and the IWF.***” (emphasis added) Report Stage, 20 March 2017, col 39-40, <https://hansard.parliament.uk/pdf/lords/2017-03-20>; and

b) whether there is the legal scope for this action given the drafting of the Act. As Annex 1 and 3 of the Guidance documents set out, the BBFC can act against pornographic material that is 18, R18 and extreme pornographic material. Material that falls within section 1 of the Protection of Children Act 1978 (photographs and pseudo-photographs) and under section 62 of the Coroners and Justice Act 2009 (animated child sexual abuse images) would be excluded. If the BBFC believes it can act on types of material that come within the description of “potentially indecent images of children” because it falls within the legal definition of extreme pornography, it would be helpful to be clear on that in this guidance.

Paragraph 7 – it would be helpful to have an indication for what “a prompt timeframe” would be for those subject to requests for compliance and so the general public will know what the intention of the regulatory framework is.

### Section 3: Age-verification Standards

Paragraph 5(a) – the text implies that if age has been identified at registration then it need not be at the point of access. This is concerning as it implies that an adult could prove their age but a child could be the one accessing the material. Paragraph (c) contradicts this as does paragraph 7, so it would be helpful to have clarity about the intention of paragraph 5(a).

#### **Guidance on Ancillary Service Providers**

My comments on the Introduction, paragraph 2, and section 2, para 5 are the same as those I have made above.

#### Section 3: Classes of Ancillary Service Provider

Paragraph 3 - The list of classes of ancillary service providers is quite a different list from that provided in the Secretary of State's Guidance to the Regulator in paragraph 5.7 and it is not clear why that is the case.

Paragraph 8 – I suggest that the wording “under section 21 that the relevant” should be changed to “under section 21 if the relevant”

Your sincerely

Elspeth

Baroness Howe of Idlicote



## ROBERT HOWELL

Subject: AV guidelines

Dear consultation team,

The dangers of allowing private companies to be guardians of personal data, has recently been shown to be unwise and dangerous given the Cambridge Analytica scandal. The government forcing people to hand over private data in the privacy of their home, about their private lives will allow companies to collect and potentially sell or unwittingly lose such information will create mass opportunities for blackmail. Such information could be used by nefarious forces to force people to vote certain ways in elections, perform criminal acts or even be forced to perform degrading sexual acts and even the possibility of prostitution.

The government has not planned for any of these dangerous outcomes, which surely are a breach of the right to a private life in the home and the government haven't even bothered to set privacy guidelines with regulatory gaps between both organisations overseeing privacy.

This is one of the most dangerous, flagrant abuses of power which was done just to try and create a moral panic. A breach will create one of the biggest public scandals in British history, a government would collapse with peoples private lives becoming public and those affected will look to take legal action against those responsible.

My name and response does not need to be confidential.

Sincerely,  
Robert Howell

## RICHARD HUGHES

Subject: Age Verification concerns

Dear consultation team,

I'm concerned about how data could be collected and abused. As an adult there is no reason why my web activity need to be shared with additional private companies. I fear data could be exploited by the unscrupulous and absolute privacy should be a top priority.

My name and response to this consultation does not need to be confidential. But the perfectly legal information that I choose to read, view or download via the internet should be.

Sincerely,  
Richard Hughes

## PHILIP INGLESANT

Subject: Security and privacy of age verification

Dear consultation team,

I am very concerned that age verification proposals to ensure that only those over 18 are able to view pornographic content online contain no substantial privacy safeguards. These AV tools will be operated by private companies, which will have access to very sensitive personal information.

In the light of current revelations about Cambridge Analytica and Facebook, it is naive to believe that such data will not be mis-used. In fact, it is not at all hard to envisage some even more undesirable uses for this data. It might, for example, be used to target advertisements to encourage consumers to view more hard-core pornography or lead to pornography addiction.

It goes without saying that the consequences of a data breach would be catastrophic, not only for pornography users but for their families and colleagues.

Best regards,

My name and response does not need to be confidential.

Sincerely,

Philip Inglesant

## CONAL JARDINE

Subject: Be very careful with AV implementation

Dear consultation team,

As a parent and educator, I believe ensuring children and young people are protected is essential, however I have concerns about the apparent reliance on age verification to achieve this, in particular I am concerned that the technology used to achieve this will be put in the hands of private companies, giving them an opportunity to harvest very personal data on people. In light of the recent Cambridge Analytica scandal, and potential hacking attempts by foreign powers, it is essential that such technology is under very close government scrutiny.

My name and response does not need to be confidential.

Sincerely,

Conal Jardine

## ANDY JARY

Subject: Age verification privacy

Dear consultation team,

Please can you provide me with the details as to which documents will be used for A/V and, more importantly, how this information is to be securely stored and who will have access to this. Will this information be handed over to the police, GCHQ etc. without individual's consent?

Will you be following the GDPR rules?

My name and response does not need to be confidential.

Sincerely,  
Andy Jary

## MIKE JEROME

Subject: AV privacy

Dear consultation team,

How will you ensure privacy with AV tools? Your technical staff must be better than Facebooks which is no small ask.

My name and response does not need to be confidential.

Sincerely,  
Mike Jerome

## STEVE JOLLY

Subject: Castration of privacy is a no no

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Steve Jolly

## CHRIS JONES

Subject: Age verification

Dear consultation team, I am writing to express my disapproval of this measure. I think it jeopardises privacy and is a huge intrusion by government on personal liberties.

My name and response does not need to be confidential.

Sincerely,  
Chris Jones

## LAWRENCE JONES

Subject: Concerns about age verification

Dear consultation team,

My name and response does not need to be confidential.

I have grave concerns about the implementation of age verification gates for access to online sensitive material in the U.K. While important that we safeguard the younger generation and ensure they don't prematurely encounter content that is unsuitable for their maturity, it's my belief that enforcing age verification is going to be both ineffective at achieving this goal and actively damaging in other areas.

My primary concern is that enforcing age verification checks means condoning removal of privacy when browsing the internet. It has been shown time and again that even government bodies fail to adequately protect the privacy of those who trust them with their data, with data leaks occurring with alarming regularity.

There is no reason to believe that the variety of poorly regulated websites we are about to require to collect personal data are even remotely capable of protecting it, if even our government struggles to do so. If this type of data is leaked, it has a high potential to enable blackmail and other abuse of the people it concerns.

Combine this practical lack of privacy with a clear absence of accompanying regulation, and we're primed for several high profile data leaks. There are more effective ways to safeguard children's wellbeing that don't pose a risk to the wider citizenry, and we should think carefully before proceeding with this legislation.

Sincerely,  
Lawrence Jones

RHYS JONES

Subject: Please ensure privacy protections in AV tools

Dear consultation team,

I am very concerned about the lack of regulation of privacy controls in the proposed age verification tools.

You will be aware of the highly sensitive nature of the information that has been proposed for collection. You will also know that the market is dominated by one large company (Mindgeek) that runs its operations in Canada, outside UK and EU jurisdiction. There are also very many other smaller players, with systems that may be built on a budget and which, consequently, may not conform to best practice in data protection and security. The recent controversies over Cambridge Analytica, and most recently the revelations over Moneysupermarket data being used to target potential voters, show the necessity for strict data protection and privacy legislation, and the power to enforce them.

Not to include any enforceable privacy guidelines for AV tools would, I feel, deeply misjudge the public mood. It seems that we have recently woken up to the unauthorised use of our personal data by third parties, and were the BBFC not to take account of this in its regulatory framework, it would be a major mis-step.

Please ensure that the guidelines hold privacy in AV tools as a central concern.

My name and response does not need to be confidential.

Sincerely,  
Rhys Jones

## PAWANDEEP KAHLON

Subject: Regarding Public consultation of DEAct

Dear consultation team,

There is a serious vulnerability in the legislature regarding how age verification (AV) tools will be implemented. Pornography is a sensitive topic and data regarding an individual's consumption is one that is very susceptible for use as a coercive weapon. It can not be expressed more seriously as to what kind of disastrous impact it would have on society, if a leak of public viewing habits were to flood the open internet, or perhaps even worse, be used by a group for it's own purposes. Privacy is as paramount as the safety of children online. As important, and no less.

But this seems to not have been understood. There is a glaring patch, a hole, in the regulations between yourselves, the BBFC, and ICO where nobody is protecting public privacy. This is a real exploitable weakness.

As we have seen in the news media over the last few weeks, any exploitable piece of data is absolutely seen as valuable and perfectly reasonable to be collected, regardless of an individual's rights, according to private businesses. I am of course speaking of Cambridge Analytica. It is abundantly clear that privacy concerns are not the concerns of business and that the public absolutely will turn to look at the government for answers. It is not acceptable to leave clear vulnerabilities in the regulations or in the the AV tools and expect there to be no problems in the future. As things stands, it is inevitable that in a couple of years at most, a new scandal of immeasurable impact will hit the UK, and the public will again turn to look at the government. They will ask, why was a lesson not learned after Cambridge Analytica?

Can the BBFC please write strict privacy guidelines that properly protect the public's privacy.

My name and response does not need to be confidential.

Sincerely,  
Pawandeep Kahlon

## NAV KANDOLA

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Nav Kandola

## FRANCES KAY

Subject: AV tools and privacy

Dear consultation team,

The government must take responsibility for ensuring that our privacy is not subject to the very different priorities of private businesses. They have no social remit or interest in defending our rights. We depend on you to do that.

Thank you.

My name and response does not need to be confidential.

Sincerely,  
Frances Kay

## SCOTT KENNEDY

Subject:

Dear consultation team,

When drafting the Digital Economy Act (DEAct), the Government simply chose not to mention privacy much at all and leave the design of AV tools to the market. It is very likely that large companies will use this ability to collect highly sensitive records of the public's porn watching habits. This is data that can be abused, sold, or hacked.

By not issuing clear guidelines the Government can blame the private sector for any data breaches that occur.

The language of the DEAct fails to take privacy concerns seriously.

If the requirement for age verification is to remain a part of the DEAct then the Act must contain strict privacy guidelines as well as details of strong sanctions should these guidelines be breached.

My name and response does not need to be confidential.

Sincerely,  
Scott Kennedy

## KAHKASHAN KHAN

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
kakhkashan khan

DAVID KILHAM

Subject: Age verification

Dear BBFC consultation team,

The age verification agenda seems like a really good idea to keep pornography away from children. Using credit card, passport or driving licence details seem an easy solution. But all of these things exist in my house with easy access for my teenage son. Unless I buy a safe, or hide my wallet every time I come home from the shops, he will know where these things are, and could quite simply use them to avoid the checks and pass the 'responsibility' to an unwitting father. Will he have committed a crime? What sort of punishment is equal to the humiliation of a prosecution?

If the database is then leaked into the public domain, my job as a teacher would be intolerable, protestations that it is without my knowledge that I am on the site would mean nothing. I would almost certainly have to resign, finishing my career. Who is then responsible? My son? The private company? What arrangements are in place for the enforced payment of damages from the insecure database for the end of careers in these cases? I would certainly have to sue or live a life of penury, yet the private company will almost certainly be based outside UK jurisdiction.

Also, who will have access to these databases? Will I find myself campaigning against a government initiative only to find that 'part' of a database has been leaked, the part with my name on it? Or, more routinely, it is copied and used for blackmail. Member of the pornography industry are not known for their high moral values and they are often associated with organised crime, both inside and outside of this country. Also, journalists and other diggers of celebrity gossip are highly unlikely to pay for my name (unless I was in direct conflict with their organisation), but they would certainly pay large amounts of money to an organisation to find the names of the famous amongst the databases.

The idea seems worthwhile investigating, but the possible misery that seems to be too high a price to pay, when existing family filters exist for the vast majority (all?) of existing broadband suppliers.

My name and response does not need to be confidential.

Kind regards,

David Kilham



## ALEX KING

Subject: For progressive porn and proper privacy

Dear consultation team,

Your ill-conceived strategy to protect children from pornography by obligating age verification software will have profound negative consequences that far outweigh any success likely to be achieved in frustrating young people's access to pornography.

The technology requirements will promote monopoly over the Porn market by large amoral Porn companies - in a market that is worryingly non-diverse - and harm smaller, independent and more progressive producers. The progressive, indecent Porn scene in the U.K. has made a positive impact on the culture but could be destroyed by this legislation.

Recording Porn consumption habits creates serious privacy concerns and is likely to be abused.

I urge you to reconsider before it's too late.

My name and response does not need to be confidential.

Sincerely,  
Alex King

## BEVIS KING

Subject: Please think again about the plans for age verification for Porn sites

Dear consultation team,

Please think again about the plans for age verification on porn sites - the plans as they stand offer a simply huge opportunity for unlimited abuse of private data. The private sector cannot and should not be trusted with the level of personal information that is being proposed.

Please consider instead a system whereby the verification is performed once by a government authority and an anonymised key is produced. You can then use this key with existing two factor authentication technologies like Google Authenticator to provide a time limited key to access the services. This utilises existing IT industry best practice for security while at the same time affording the British public privacy over this most personal of internet activities.

This provides all of the same assurances that the person is who they say they are, without exposing their identities to an industry which has a far from stellar reputation,

My name and response does not need to be confidential.

Sincerely,  
Bevis King

## MATTHEW KIRSHEN

Subject: Age Verification laws

Dear consultation team,

I'm writing to express my deep concern about the proposed age verification (AV) law changes.

Private companies have shown time and time again that they aren't to be trusted with personal data, with scandals ranging from the intentional misuse or the likes of Cambridge Analytica to careless losses to hackers from small adult companies like Ashley Madison but also huge corporate giants like Yahoo, Target, and Equifax. If we can't trust one of the largest internet companies in the world, or one of the three major credit bureaus to keep our data safe, how are we to believe that these new companies formed in the wake of this law will keep our most private data secure?

Not only that, but there is no part of this new regulation that says these companies can't use this data to track adult website viewing habits of people. I firmly believe there will be leaks, and outings involving people's private lives, vulnerable people having their sexualities exposed, and so on.

Furthermore, this bill will hand over more financial power to companies like Mindgeek which already dominate pornography online, a market domination reached largely on the back of their own piracy.

This will further edge out small producers, and companies that cater to niche sexualities, further alienating minority communities.

Finally, this will not stop children from being able to access pornography. Numerous experts have explained how young people will still find workarounds, and ways to access pictures and videos.

This is a wide reaching, and dangerous bill, which will not do what it claims to, but will hurt small businesses, alienate people with minority sexualities, and risk exposing or exploiting millions of people's most intimate data. Please do not do this.

My name and response does not need to be confidential.

Sincerely,  
Matthew Kirshen

## ALEX KOTENKO

Subject: Online private is essential, even with age verification

Dear consultation team,

Lack of protections and rigorous rules around user privacy during the age verification process will inevitably lead to misuse and abuse of user data and powers it gives.

Mass surveillance and big data processing, linked with fully identifiable user records and highly sensitive personal data in hands of commercial companies like Cambridge Analytica will lead to abuse and subversion of the very foundation of our democracy.

If an obscure commercial company can mass blackmail whole nation on the basis of knowing each and every citizen's personal porn preferences - there is not much democracy left there.

My name and response does not need to be confidential.

Sincerely,

Alex Kotenko

## ROLAND LAYCOCK

Subject: privacy

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,

Roland Laycock

PETER M LE MARE

Subject:

Dear consultation team,  
Privacy is very important for those who want it. Freedom is not divisible.

That we should be controlled, listed organised and allotted our place, not only by governments, but by private corporations, is increasing, No data is confidential and it also depends on to whom it is confidential.

That there are bad people or at least that there are people who act badly, is undeniable but by demanding verification of a person is not a guard against false identity and any corruption because the worst people will "hack it" in some manner.

One persons pornography is another's eroticism and your definition is almost certainly not mine. And anyway why does age matter that much? The corruption and violence in society engendered in the young, I think obviously, is much greater from the normalisation of playing with guns and weapons to the fighting and aggression in almost all computer games. We cannot keep these influences from all of us and these influences are also part of maturation; becoming an adult. We have to create a way people and especially children react and learn from these influences not dragoon them and try to 'wrap them in cotton wool'. We should also pursue those who actually break the reasonable laws of society whether in pornography or elsewhere, especially against children and other vulnerable people. To collect data encroaching on their privacy which can be eventually available to those who would harm others is NOT the way.

I personally believe like Tennessee Williams in "Iguana" that "Nothing human is disgusting except that which is violent or malicious" Although it is implied I would add the word or "coercive".

My name and response does not need to be confidential.

Life, love, peace and freedom,  
Sincerely,  
Peter M Le Mare

## RICHARD LEEMING

Subject: Strong privacy is a must for age verification tech

Dear consultation team,

I am emailing you as I have grave reservations about the proposed approach to use both age verification tools and the technology underpinning them to control access to pornographic websites.

While it is essential to ensuring children and young people are protected, educated and given parental care, the government's proposed approach is deeply flawed.

Privacy must be integral to AV tools for the following reasons:

- AV tools will create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Richard Leeming

ALEX LINFIELD

Subject: No to more data collection!

Dear BBFC

In recent weeks, we've seen a relatively banal company like Facebook admit that our data is collected and sold for nefarious purposes to advertisers through companies like Cambridge Analytica.

On top of that, we continually see hacks and leaks as companies fail to keep their data safe. A chain's only as strong as it's weakest link and we constantly see these links break.

Even if carried out intelligently and respectfully, Adult Verification if not encrypted and safeguarded correctly opens the door to the LEGAL porn-viewing habits of the UK population being collected / hacked by people who will then be able to use it to invade privacy and potentially blackmail people.

Having some kind of database of what websites every adult in the UK has visited is a VERY bad idea.

Handing our data over to someone like MindGeek, who have made the majority of their money reposting stolen content to their tube sites is a BAD idea.

The government should NOT be encouraging the snooping on it's population like this!

Yes, minors need to be safe online, but the onus should first and foremost be with their PARENTS, and we already have safeguards in place with many ISPs ensuring that adult sites are blocked by default on most computers and internet enabled devices unless the removal of the block is requested by an adult.

Also any UK based small-business websites deemed "Adult" in nature will need to age check their users for free. 99% of visitors to these sites only go to window shop, so adding something that \*seems\* small like a 10p cost for every user verified will drive people out of business! If we're not going to start charging members of the public 10p to walk into Anne Summers or forcing cinemas to charge 10p to age check cinema-goers attending 18+ movies, we should NOT be attacking legitimate tax-paying business websites!

Thanks for your consideration.

My name & response don't need to be confidential.

Alex Linfield

## DOUG LIVESEY

Subject: Age verification is basically throwing sensitive data around without a care

Dear consultation team,

The proposed age verification measures are broken by design. They require users to scatter vital important, personal data around, thus massively increasing their risk surface for identity theft and a whole host of other dangers. Statistically, this *\*will\** increase cyber crime.

Essentially it's a form of censorship. One can only view sites that are deemed to require age verification if one is prepared to take significant risks with one's personal data.

The proposed AV measures decrease both digital security and freedom of expression on the internet.

Needless to say, I am very opposed to them!

My name and response does not need to be confidential.

Sincerely,

Doug Livesey

## JOE LOTITO

Subject: right to privacy

Dear consultation team,

Requirements for pornographic websites to verify UK users are over 18 will come into effect soon, and the BBFC is in charge of issuing guidance for how age verification (AV) tools must operate. Ensuring children and young people are protected, educated and given parental care is vital, however we have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

My name and response does not need to be confidential.

Sincerely,

Joe Lotito

## ANDREW MACADAM

Subject:

Dear consultation team,

It's bad enough that this ill thought out policy is going ahead as the evidence clearly shows it won't help as its intended to but if you insist on implementing it then you must at least do it right. Proper legislation to protect the public from private organisations must be at the centre of this if it is to happen.

My name and response does not need to be confidential.

Sincerely,

Andrew MacAdam

## PAUL MALLINSON

Subject: AV privacy

Dear consultation team,

It is obvious that a compulsory Age Verification system for pornographic websites, requiring the provision of legal documents, must abide by strict privacy rules. Without them, the system will be wide open to abuse. I cannot believe that provision is not being placed on strict privacy guidelines for AV tools. Privacy must be a priority, in my opinion.

My name and response does not need to be confidential.

Sincerely,

Paul Mallinson



## GRAHAM MARSDEN

Dear Sirs,

With regard to your invitation for responses to the Consultation on the planned Age Verification Arrangements, please find my response below.

Firstly I wish to state that, frankly, I think you are being sent on a Fool's Errand and are simply being used as a political tool by the Government for their own PR purposes, rather than them actually expecting you to achieve any noticeable positive good.

The idea that Age Verification will actually stop under 18s from being able to access pornographic material is laughable to anyone with more than a passing understanding of the internet and similar technologies and it is clear that it is just an example of "Magical Thinking" by Government Ministers who don't have such an understanding, but believe that it's enough for them to say "do this" and, somehow, private enterprise can wave a wand and make it happen.

I should point out that, when I was at school, even though there was no internet and adult magazines were kept on the top shelves of newsagents, none the less it was not difficult for such material to be accessed. The idea that, in the modern age, an Age Verification system could do any better is ridiculous.

Secondly, the majority of households in this country do not have children. Why should everyone be treated as such? "Think of the Children" is never a good reason for passing a law, it is simply a way of trying to avoid people questioning such laws before they are on the Statute Books.

Regarding your questions, here are my replies:

\* \* \* \* \*

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

No.

I run a site making and selling Bondage and BDSM equipment to adults. To advertise my products, I have photographs of them on models which could easily be classed as pornographic. I have, of course, registered the site with services such as NetNanny etc and include tags to allow system such as CleanFeed to block it for adult content.

It is easy for you to state that you will take a "proportionate" approach and that this legislation will only affect those who make pornography available on a "commercial" basis, however past experience and examples from other countries have shown that it is much more likely that a "sledgehammer to crack a nut" approach will be taken resulting in many false-positive results or a "block first, respond to appeals later" attitude simply so the Government can claim that their system is "working".

The fact that this would cripple many small businesses who could not afford to lose money whilst their site is unavailable, nor have sufficient resources to pay for the legal

advice to lodge a successful appeal, does not seem to be important to those who passed this legislation.

I would also point out that there seems to be no clear details for how any appeals process would operate in the first place, making life even more difficult for businesses like mine.

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

Absolutely not.

The idea that, somehow, you can "confirm age but not identity", is absurd. There is no practical way to do such a thing and achieve the aim of preventing children accessing this material.

Not only that, but it would leave open the very possibility of a massive data breach with people's private information being a prime target for hackers (see the Ashley Madison case and, more recently, the leak of gay men's HIV status from the Grindr dating site).

Imagine you were to visit an Adult Shop and, to enter, not only would the shop keeper have to decide if you were over 18, but was required to note down your name, address and other identifying information. Would you feel safe handing those details over, not knowing how they might be used or distributed?

- Do you have any comments with regards to Chapter 4?

The ICO is a reactive, not a proactive organisation.

As has been seen from the way that people's data was treated by FaceBook and Cambridge Analytica, it is clear that private enterprise cannot be trusted to adhere to even the most basic and ethical data handling requirements.

The idea that a big company can acquire information on customers and then, retro-actively, change their privacy policies, relying on "if you don't do anything we'll assume you consent" is contemptible. The ICO simply does not have any powers to stop such a thing happening and subsequently possibly giving these companies a slap on the wrist (even assuming they have the ability to do so for businesses which are run out of different countries) is hardly any deterrent.

It should also be pointed out here that the Ashley Madison hack was linked to a number of suicides, for which nobody has been held responsible.

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

Definitely not.

ISPs and Payment Services are not censors and should not be required to undertake such work. As mentioned above, to do so would inevitably result in a "block first, appeal later" approach which would have a massively chilling effect on Freedom of Expression.

- Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

No. See above.

In closing I strongly urge you to reconsider the BBFC's participation in this scheme. In 1984, as I'm sure you're aware, your organisation's name was changed from the British Board of Film Censors to the British Board of Film Classification.

The Government now wishes to turn the clock back and make you the British Board of Internet Censors, something which is unwelcome and unneeded.

The Government has handed you a poisoned chalice and when, inevitably, this law fails to "protect" children from accessing adult material, you are the ones who will be left with the blame.

Yours Faithfully,

**JOESEPH MARSH**

Subject: Age verification technology

Dear consultation team,

I find it laughable that this step is even being considered given the recent controversy over the scandal involving Cambridge Analytica. We have seen that such information, when in the wrong hands, can be used harmfully. To allow a private company to hold such information without strict rules considering its use is careless in the extreme. Myself, and many others besides, will be sure to hold not only the government but also the BBFC to account if this information is used in a way that we feel is not in our interest.

Many members of the public, including a great number whom I have personally come in to contact with, share these concerns. We are finished with the systematic degradation of our personal privacy.

If AV tools must be implemented then clear guidelines which control the use of the data garnered must be put in place to protect the general public.

My name and response does not need to be confidential.

Sincerely,

Joseph Marsh

## STEVE MARSHALL

Subject: Government for the people

Dear consultation team,

Privacy is essential in all walks of on-line life. If it can be ignored here then the same will happen with financial and medical data as it has with FB data. This is an opportunity to lead in ensuring individual privacy is maintained.

My name and response does not need to be confidential.

Sincerely,  
Steve Marshall

## DANIEL McCAFFERTY

Subject: Age verification and privacy

Dear consultation team,

When considering potential vendors for age verification, please bear in mind the absolute requirement of individual privacy. No single party should have access to both a person's personal information and the sites they are requesting. There needs to be a clear separation of concerns in this regard.

My name and response does not need to be confidential.

Sincerely,  
Daniel McCafferty

## KEVIN McDONNELL

Subject:

Dear consultation team,

considering the seemingly endless slew of hacks it is an extremely unwise idea to create a single point of attack for such sensitive data. People who for whatever reason may not be able to openly express their sexual identities could be held to ransom, all in the name of protecting children, a job that if memory serves is the firm remit of parents.

My name and response does not need to be confidential.

Sincerely,

Kevin McDonnell

## ANDREW McDOUGALL

Subject: Age verification processes

Dear consultation team,

I note with dismay that the proposals for age verification processes for adult-only internet access do not seem to have adequate provision for ensuring confidentiality. This is, to my mind, quite unacceptable. Recent events concerning Cambridge Analytica are only the tip of the data mining iceberg which is being exploited by innumerable companies for purposes which are certainly not in the interest of the people who unwittingly provide the input to the algorithms used. It is high time a far stricter regime was imposed by the government, which will quite rightly be blamed if this laxity is allowed to continue.

My name and response does not need to be confidential.

Sincerely,  
Andrew McDougall

## BRENDAN McGOWAN

Subject: Adult Site Privacy

Dear consultation team,

I note with concern the lack of privacy controls in the proposals to require identification for adult sites.

Whilst I understand the need to protect young people, the lack of controls on how the information provided will be safeguarded is extremely concerning and proper checks and controls should be installed.

My name and response does not need to be confidential.

Sincerely,  
Brendan McGowan

## MARTIN McGOWAN

Subject: age verification tech

Dear consultation team, I am appalled that things like driving licences could have to be entered into a database in some way where there is no strict privacy guidelines for AV tools, in fact there looks to be do weak guidelines even.

Privacy is essential we have all heard what happened with Cambridge analytica. for age verification to have any chance of working they would have to film the person entering the data to prove that an underage person wasn't providing the information.

My name and response does not need to be confidential.

Sincerely,  
Martin McGowan

CRAIG McINALLY

Subject: AV requirements.

Dear consultation team,

Frankly, this entire situation is absurd. The requirement to "protect the children" is idiocy, plain and simple, and is being pushed as a first step to allow deeper regulation of the internet. This cannot be allowed to stand. If AV must be a thing, have it be done at an ISP level with an option of "Allow access to everything", and varying levels of limitation as needed. Forcing AV on specific sites simply means more sensitive data and presuming identities being collected, and therefore far more open to abuse.

Children will gain access to pornography regardless of these attempts at regulating it, and the steps taken will cause significantly more harm than good.

My name and response does not need to be confidential.

Sincerely,  
Craig McInally

ALY McNAB

Subject:

Dear consultation team

Privacy is a right, and pornography is not illegal. If the government wish to introduce ID - verified checks, then they should provide the ID for free. I'm disabled so don't have a driver's licence or passport.

My name and response does not need to be confidential.

Sincerely,  
Aly McNab

ALAN McQUEEN

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Alan Mcqueen

CONNOR McROBERT

Subject:

Dear consultation team,

After the Cambridge Analytica scandal there is a grave concern among the public that new age verification will lead to more panic.

If a breach of this privacy occurs there will be mass outcry at the government.

My name and response does not need to be confidential.

Sincerely,  
Connor McRobert

C MIDDLETON

Subject:

Dear consultation team,

What fresh lunacy is this ?

Requiring people to share personal data, with no data protection requirements, is idiotic and probably illegal.

Wouldn't the resources earmarked for this be better spent on something that actually creates a threat, such as combatting terrorism funded by the government's allies in the Middle East ?

My name and response does not need to be confidential.

Sincerely,  
C Middleton

ANDREW MORGAN

Subject: Strong privacy is a must for age verification tech

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Andrew Morgan

WILLIAM MORLEY

Subject:

Dear consultation team,

It is of the utmost importance that strong privacy tools be used to protect the identities of millions of people submitting their identity information.

We cannot trust private companies to protect our data and therefore they must be made to fear harsh penalties for misuse of data.

My name and response does not need to be confidential.

Sincerely,  
William Morley

SAMUEL MORRIS

Subject:

Dear consultation team,

Age verification will be a disaster for the adult industry in this country should a single data breach occur. Frankly, if privacy isn't a priority in age verification, then age verification shouldn't be implemented at all.

My name and response does not need to be confidential.

Sincerely,  
Samuel Morris



## PAUL MOSSON

Subject: Age Verification

Dear consultation team,

This is the first step towards outright censorship. As a UK citizen and tax payer, I strongly object to these proposals. The government is supposed to safeguard the interests of its citizens not put them in harms way!

I also object to the imposition of this law. Morality is subjective. How dare the government consider their morality superior to mine.

The enforcement of this environment makes me concerned and angry. Can Britain really be regarded as a democracy?

Paul Mosson

My name and response does not need to be confidential.

Sincerely,

Paul Mosson

## PETER MOUNT

Subject:

Dear consultation team,

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

Peter Mount

MATT MOWER

Subject: Age verification consultation

Dear consultation team,

I applaud your goals. It makes perfect sense to try to ensure that minors are not exposed to content they should not be seeing.

But the means by which this is attempted must be considered very carefully. In particular the side effects of any particular means under consideration.

For example, allowing private companies to create large databases of information about what people are watching is a MASSIVE privacy concern.

We have seen far too many instances of private companies selling information and creating a privacy issue for people. This also extends to misuse.

What will happen with the databases you are enabling? How will you deal with the inevitable breaches and misuses of this data? How will you help people who fall foul of these breaches and misuses? What is your responsibility?

Also there may be a chilling effect. There is nothing wrong with pornography or watching pornography but people may feel their perfectly legal choices are going to be leaked or used against them. This is not healthy.

We should also question whether proposed technology solutions to this problem are even going to be effective in what they seek to do. Will the controls be easy to circumvent. I think that they will.

Think very carefully as it will be your reputations at stake for what you are about to do.

My name and response does not need to be confidential.

Sincerely,

Matt Mower

MATTHEW MOYES

Subject:

Dear consultation team,

I would like to express my concerns regarding requiring private companies to hold confidential information, such as, for age verification. Moreover, the kinds of companies required to gather such information do not have the best track record of vigilance in this area. Unless the government or one of its agency is able to step up as a middle man I cannot see any reasonable safeguards that can be actioned. Finally, any tech-savvy person is aware that such measures are always circumbentable and of no protection.

My name and response does not need to be confidential.

Sincerely,

Matthew Moyes

## ALEC MUFFETT

Subject: Consultation on draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers

To:  
BBFC

Subject:  
Response to draft Guidance on Age-Verification Arrangements and draft Guidance on Ancillary Service Providers

(1) My name is Alec Muffett. I am submitting this response as an entirely personal effort, however for context:

- I am a recognised authority on internet security, and have worked in and around the computer & network security industry for about 30 years.

- In previous employment, I was Chief Architect for Security for Sun Microsystems Professional Services in EMEA, designing systems for deployment in investment banks, telcos, internet service providers, stock-exchange clearance houses, etc.

- In previous employment I was a software engineer for Facebook's "Security Infrastructure" team, leading several major projects.

- I am a member of the board of directors of the Open Rights Group.

- I am a member of the newly-established "Security & Privacy Executive" of the British Computer Society.

(2) I find many causes for concern in the drafts regarding age-verification arrangements and ancillary service providers, however I shall limit this response to a solitary, most pressing, issue.

(3) I am deeply concerned by the lack of regulatory oversight, and the lack of standards regarding the operational and functional aspects of data and information security, which speaks to this consultation via:

"It also includes information about the requirements that age-verification services and online pornography providers must adhere to under data protection legislation and the role and functions of the Information Commissioner's Office (ICO)."

(4) I aver that these dual lacks risk irreparable damage to the privacy of millions of Britons. In reverse order:

SECTION: The lack of standards regarding the operational and functional aspects of data and information security

(5) Data pertaining to "an individual's sex life or sexual orientation" is clearly of a highly sensitive nature, evidenced by the fact that it is a category of data which is (several times) called-out for special treatment in the upcoming Data Protection Act 2018.

(6) Further, we are aware from "Mosley v News Group Newspapers Ltd" that matters of privacy related to sexuality are hard, perhaps impossible to adequately redress.

(7) Moreover we are aware that a prurient market for such information exists; again the Mosley case, plus also the history and behaviour of British tabloid journalism; not to mention matters of criminality, blackmail and extortion.

(8) However the only standard which speaks to the protection of age verification data is "BSI PAS 1296" which is a general-purpose document that can be characterised as "how to age verify" (with related concerns) for all businesses from online penknife sales to hardcore pornography.

(9) It should be obvious that there is a difference in the sensitivity of data between "John Doe purchased a Swiss Army Knife from Amazon", versus "Jane Doe visited LesbianSpankInferno.co.uk"

(10) The fact that "Jane" visited "LesbianSpankInferno.co.uk" suggests that Jane may be a Lesbian, and thus is information that pertains to "an individual's sex life or sexual orientation"

(11) Again, per "Mosley", if this information leaks, then redress is hard and expensive; published information cannot easily be "put back into the bottle"; this distinguishes such information from (say) credit card data, where in the case of "identity theft" the banks (etc) underwrite losses and will recompense a victim of credit-card data theft.

(12) Yet the entire architecture of "age verification" is to create large, centralised, attractive-to-hack repositories of personal information that "Jane Doe" sought age-verification for "LesbianSpankInferno.co.uk"; and these repositories are expected to "sort out" their own "homebrew" operational and functional data protection standards via "laissez faire" regulation.

(13) Thus, to summarise this section:

- regulation is creating a few, large, centralised, attractive-to-hack repositories

- of personal information which pertains to "an individual's sex life or sexual orientation"

- yet we are proposing that such data is adequately "protected" by a

general-purpose document that describes how to perform age verification for purposes including such as online penknife sales

- and which in turn punts data protection requirements to GDPR / the upcoming Data Protection Act,

- in the misconceived expectation that GDPR and the Data Protection Act provide operational and functional standards

- when in fact they provide only yet more regulatory requirements

- leading, inevitably, to diverse "homebrew" security implementations,

- breach of which will lead to bulk leakage of sensitive data which is hard to redress, per Mosley.

(14) This does not appear to offer proportionate protection for this character of data, especially at the scale of millions of Britons in a handful of weakly-regulated, "homebrew"-secured, databases; we are thereby setting the stage for another "Ashley Madison"-like data breach, which in that case led to the suicide of several people because of the nature and sensitivity of the information leaked.

#### SECTION: The lack of regulatory oversight

(15) Above, I mention credit-card payments for comparison; payment card information is not called out for special processing under the upcoming Data Protection Act, instead it is merely expected to be treated "normally".

(16) Further: data breaches surrounding payment card information are redressable; compensation can be paid, well-established mechanisms and processes exist to support recompense, even in the instance that one of the entities should go bankrupt.

(17) So: payment card information is of a considerably less "existential" nature than pornography-site age verification data, however it is protected by a considerably better operational and functional standard which must be adhered to in order that an operator or vendor/commercial customer of payment card services can operate: the "Payment Card Industry Data Security Standard", or PCI-DSS.

(18) The PCI-DSS is a comprehensive suite that defines concrete requirements for protective technologies (firewalls, encryption), access controls (passwords, more encryption), sensitivity levels (which aspects of card data are most secret, as opposed to visible "on-screen"), operations, and screening of personnel (background checks)

(19) PCI-DSS also defines what portion of payment-card data (if any) is visible to the vendor who is selling to a customer.

(20) "BSI PAS 1296" covers none of this; again, its primary focus is upon the process of age-checking (and, eg., assuring that the customer cannot bypass an age check) rather than to protect the fact of age checking.

(21) Further: there is no mention of performing criminal records (CRB) checks on staff, nor of checking whether ones' new employee might previously have worked at some Sunday tabloid.

(22) There is no definition of "adequacy" for protection of different aspects of age-verification data (viz: "Jane Doe", her address, or which of several websites she has age-verified with).

(23) In short: PAS 1296 is wholly insufficient for the purpose of defining protection of "sensitive age-verification data".

(24) There are many steps that would be necessary to address this tremendous gap:

- a regulator will need to define operational and functional security standards (akin to PCI-DSS) for provision of "sensitive age-verification data services",

- it will need to be able to regularly audit and shut down non-compliant providers of (and, per PCI-DSS, larger customers of) sensitive age-verification data services.

- liabilities will need to be assigned, sensitivity of differing classes of information will need to be defined.

- a means of redress/compensation would need to be defined for people who have had data leaked in the instance that an age verification provider is bankrupted by GDPR fines, etc, subsequent to a breach.

- other...

(22) I would appreciate the BBFC's addressing this matter, raising it with the Government that existing regulations are insufficient, and the associated standards are not yet fit for purpose, to permit us to move forward with deployment of age verification.

Yours,

Alec Muffett

## RICHARD NEILL

Subject: Age Verification is a privacy disaster

Dear consultation team,

Age verification on the web is going to be a privacy catastrophe. This is almost certain to result in a data-breach, and when it happens, millions of people will be susceptible to blackmail.

Please, ensure that age-verification tools have very strict requirements on anonymity - and it's more important to guarantee strong privacy than to have perfect age-verification.

My name and response does not need to be confidential.

Sincerely,  
Richard Neill

## JOANNA NEILSON

Subject: Age verification

Dear consultation team,

Privacy standards should be ensured at any time, but especially for such sensitive information. The DEAct does not contain reassuring information in thus regard.

My name and response does not need to be confidential.

Sincerely,  
Joanna Neilson

## JILL O'SULLIVAN

Subject: Strong guards on privacy are essential

Dear consultation team,

I appreciate that it is important to protect children and young people. It is also important to ensure that everyone's privacy is protected. The current proposal to leave such protections in the hands of private companies, in effect unregulated - in light of Facebook and Cambridge Analytica - is unacceptable.

It is in everyone's interests to make sure AV tools protect privacy.

My name and response does not need to be confidential.

Sincerely,  
J O'Sullivan



DAVE OWEN

Subject:

Dear consultation team,

While I consider it a good thing to safeguard the online viewing habits of underage citizens I do not feel that it is warranted for websites to request that I enter passport or credit card information so that I as an adult can access a pornographic website. I am a grown adult and I do not need the permission of the government nor do I expect them to keep track of my online viewing. Let me be perfectly clear you work for us not the other way round and I do not expect my personal information on my pornographic viewing habits to be recorded by anyone. You have clearly shown in the past that you are wholly incapable of keeping information remotely safe and I have no confidence whatsoever in your ability to safeguard said information therefore I expect a stringent and well thought out proposal be made public before you carry on with this quite frankly absurd law

My name and response does not need to be confidential.

Sincerely,

DAVE OWEN

GEORGIA PEARCE

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,

Georgia Pearce

NISH PFISTER

Subject: age verification

Dear consultation team,

Introducing age verification without regulation to ensure privacy is inviting trouble. It would have to be based on some document that provides sensitive data to the agent asking for age verification.

The responsibility obviously lies with the one forcing the verification to happen.

To me the importance of clear guidelines and control of the agents doing the age verification is quite obvious.

My name and response does not need to be confidential.

Regards,

Nish Pfister

JEFF PIPER

Subject: AV Guidelines Comment

Dear consultation team,

Requirements for pornographic websites to verify UK users are over 18 will come into effect soon. Ensuring children and young people are protected, educated and given parental care is vital.

However I have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority and there is no excuse why the Government should not be prioritising privacy for AV technology.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Jeff Piper

## PROFESSOR BLAINE PRICE

Subject: Strong Privacy for Age Verification

Dear consultation team,

While the need for Age Verification (AV) is clear, I must strongly urge you to consider the privacy implications of any AV guidelines you may produce. At the time of writing the Cambridge Analytica scandal was current, but I have no doubt other scandals and data breaches will have occurred by the time you read this and you can look at news reports from the past decade to find regular reports of such breaches. By requiring companies to hold large databases of credit card and identity documents and further giving them no incentive to protect them you are inviting fraud and identity theft on a colossal scale. Data breaches will occur, history tells us this, you have the potential to create one of the biggest honeypots for malicious actors imaginable.

There are many simple measures that can be taken to protect data used for age verification from being stored and open for misuse. I urge you to make this a priority in creating the guidelines.

My name and response does not need to be confidential.

Sincerely,

Professor Blaine Price

Professor of Computing

The Open University

## MARTIN PUTT

Subject: Age Verification

Dear consultation team,

While it is admirable and makes sense to ensure that people under 18 don't view pornography Age Verification technology as highlighted by the Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

My name and response does not need to be confidential.

Sincerely,

Martin Putt

## LAURA QUIN

Subject:

Dear consultation team,

I do not trust that age verification can be implemented in an effective way without putting users' personal data at an unacceptable risk.

In order to be effective will require obtaining copies of millions of identity documents such as passports and the stealing of this data puts victims at risk of identity theft which can utterly ruin a person's life. To me this is not an acceptable risk for an adult wishing to view perfectly legal material.

My name and response does not need to be confidential.

Sincerely,

Laura Quin

## AARON QUINN

Subject: Age Verification Consultation

Dear consultation team,

Greetings ! I am writing to you today regarding the Age Verification legislation and would like to bullet point my concerns with you.

1. Regarding the recent and very public Cambridge Analytica scandal, a failure to take our privacy concerns seriously is now unconscionable. Private companies are quite obviously capable of breaking out trust, of wilfully disregarding our user privacy, thus they do now require being given strict privacy guidelines.
2. Are you aware that you are courting disaster because between the BBFC and ICO, there is a regulatory gap where nobody is assigned to oversee our privacy.
3. Age Verification tools may create a sensitive record of the public's porn watching habits. Personally I do not wish to know or care what porn adults watch as long as it is of consenting adults, is not with animals nor the horrific global evil that is child porn. Tackling child porn needs to be the No1 priority here. The consequences of such a breach could be catastrophic for millions of all UK citizens. Our privacy has to be respected and needs to be a priority.
4. Surely it is in the BBFC's interest to ensure AV tools, on balance, do protect the public's privacy while also ensuring that the global scourge of child pornography is flagged up for the authorities. If a breach does occur, people will see both the BBFC and the Government as responsible, and will be held to account.

Thank you for your consideration of these points and await your response.

My name and response does not need to be confidential.

Sincerely,

aaron quinn

## JONATHAN RAYMOND

Subject: Strong Privacy for Age Verification

Dear consultation team,

Age verification is an important tool for keeping young people safe online, but should not be used as a way to track legitimate users or leak private information.

With the recent Cambridge Analytica scandal, it should be clear that private data can be exploited in some quite devious ways for profits and other gains.

While browsing adult content is not illegal in the UK, it is still sometimes seen as very taboo, and as such is something people should be allowed to keep private.

While making sure AV is hard to circumnavigate is important, it should also have robust provisions to protect privacy

My name and response do not need to be confidential.  
Thank you.

Yours Sincerely,  
Jonathan Raymond

## CLIVE RICHARDS

Subject:

Dear consultation team,

It is absolutely essential that the highest degree of privacy standards be applied to any verification tools in order to prevent leakage and abuses

My name and response does not need to be confidential.  
Sincerely,  
clive Richards

LUKE RIGLEY

Subject: AV Privacy

Dear consultation team,

While age verification and protection of minors from viewing unsuitable content seem like thoroughly positive ideas, putting them into practice in a top down manner could be catastrophic for personal privacy.

At this time, it seems likely that this will be handled by private companies who can be expected to produce a comprehensive database of the public's pornographic interests. This data is obviously highly personal and sensitive, yet we have seen time and again that private companies cannot be trusted to take privacy and security seriously, with regular breaches and leaks from even the largest and most theoretically capable organisations.

Private companies are incentivised by profit, and this sensitive information has the potential to be hugely valuable, even without breaches. To combat this, if there is to be a widespread age verification system, strong regulation and a prioritisation of privacy are essential.

As a government initiative, any breach or general failure to handle this data properly and safely will be seen as failures on the parts of both the BBFC and the government, for trusting whoever is responsible. Steps must be taken to prevent this.

Alternately, such a system could just not be built, and rather than trying to keep in check private companies who hold enormous amounts of valuable and extremely sensitive data, more could be done to educate parents and promote the use of non-centralised methods of age verification and content control.

Which seems more dangerous? Building a vast database of private data which you have responsibility but not control over, or encouraging parents to work with their children?

My name and response does not need to be confidential.

Sincerely,  
Luke Rigley

JON RISDON

Subject: Digital Economy Act (DEAct)

FAO the consultation team:

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

Ensuring children and young people are protected, educated and given parental care is vital; however I have grave concerns about the apparent reliance on age verification to achieve this, and the technology itself:

- AV tools might create a sensitive record of the public's pornography watching habits. The consequences of a breach would be catastrophic for millions of UK citizens - privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy: this is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

More information about ORG's position on this consultation can be found here:  
<https://www.openrightsgroup.org/blog/2018/tell-the-government-to-protect-porn-privacy>.

Please give these points serious consideration.

Thank you and best wishes.

My name and response does not need to be confidential.  
Sincerely,  
Jon Risdon

DAVID RIX

Subject: Digital Economy Act (DEAct) - call for public comment

Dear consultation team,

You will no doubt have received many messages highlighting the very real privacy issues surrounding an idea like this. Therefore I will not talk about this here save to say that I share their concerns. Please do not make an absurd step backwards even worse by failing to implement the most stringent privacy protections! However, I regard this entire project as totally pernicious and even damaging for for the internet, achieving no benefit in exchange for a lot of messing around and expense.

My experience with such filters has shown me one thing: filtering porn makes porn worse. This is simply because there will always be material that gets round the filters, sometimes very disturbing material, while the block does screen out plenty of material that may be considered beneficial. For example (and this is from experience of testing filtering technology), medical information, art, education, scientific research, beneficial community discussion and sharing, gender and other identity discussion, some material and support groups concerning abuse, etc. Meanwhile, what you might call 'porn' is always easily at hand. What these filters do is distill online sexual media and material down so that only the least healthy and the most damaging remains - and ensures this is ALL that is available. It is entirely unreal and fictitious to imagine that filtering technology will not both let a considerable amount of material through and cause a large number of false positives.

The crucial point is that if there is concern for people growing up or living their lives with access to online sexual material, then there should only be more concern about those same people with access only to what gets around the filters. I consider these screening projects not only futile but damaging - not only useless but worse than useless. It is purely an effort to 'be seen to be doing something' even though the results will inevitably be negative.

My name and response does not need to be confidential.

Sincerely,  
David Rix



## LUKE ROBERTSON

Subject: AV tools

Dear consultation team,

My name and response does not need to be confidential.

I am quite concerned about the age verification tools that are due to come into effect. I, of course, like anyone else believe that children should be protected from images that could be disturbing, or even dangerous in some cases, to a young mind. But I equally believe that privacy should be protected and that age verification tools should be used responsibly if put into place.

I recently left social networking due to the Cambridge Analytica scandal. And I had never liked that fact that I could be looking at a pair of shoes on one website, and suddenly it was thrown up on my Facebook feed. I am due a medical procedure and have read up on that, who knows what else was being recorded. Like the majority of people in this country, I don't feel I have anything to hide but the point being that there is very little policing of privacy as it is at the moment. Whether it is something as mundane as looking at a pair of shoes or someone looking at pornographic images, provided they are staying within the confines of the law, people's privacy must be protected. If AV tools are going to work, there has to be a person or team assigned to oversee privacy.

I do appreciate concerns for children coming across something they shouldn't on the internet, but there is something to be said for parental responsibility and parental controls being encouraged on the internet, and there is of course wider issues of how sex should be taught, how young people should feel the need to look at websites inappropriate for them to learn about sex, but it is a different issue and not one that needs to go hand-in-hand with disregarding concerns for people's privacy.

I believe it is in everyone's best interests that the issue of AV tools is looked at carefully. Serious breaches of privacy, which is extremely plausible. Would cause an absolute outrage and the public would understandably see the Government and BBFC as the culprits should the need for stringent prioritising of privacy be neglected by both when implementing this policy.

Sincerely,  
Luke Robertson

## MARK RUARK

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Mark Ruark

## ALAN RUSHWORTH

Subject: Privacy impact of the Digital Economy Act

Dear consultation team,

I am writing to express my strong concerns over the likely impact of the Digital Economy Act (DEAct) on individual's privacy, and specifically its requirement for age verification (AV) in order to view pornographic material via the internet.

The Government has made little reference to the need to protect individual privacy in drafting the Act and has essentially left it to the market to design the AV technology and tools, with no plans to issue guidelines regarding the protection of privacy.

This measure will lead to companies building up large datasets relating to the public's porn-watching habits, which may then be subject to abuse, whether directly or indirectly. Moreover even if the companies do act responsibly and do not misuse, sell or otherwise deliberately make accessible that data, it will still be vulnerable to hacking by criminal groups, given the determination such groups habitually exhibit and the often inadequate protection methods adopted by those responsible for protecting data and systems (cf. NHS, Ashley Madison etc).

As the scandal over the activity of Cambridge Analytica has dramatically underlined, this approach is wholly inadequate and the bill needs a fundamental redesign. If AV is to be adopted the Government needs to stipulate strong privacy requirements for AV tools and issue relevant guidelines.

The government and BBFC cannot simply assume that any resultant data breach will be blamed on the companies. The Government is the author of the process and the BBFC is its agent and they will ultimately to blame for any such disaster, doubtless accompanied by much hand-ringing, the usual grovelling apology to Parliament and squirming appearance in front of the relevant committee of MPs by all concerned, none of which will be much consolation to those affected.

DEAct is yet another ill-designed sledgehammer to crack what I suspect is a largely imaginary, or at any rate greatly exaggerated, nut, a legislative format which, sadly, has a long heritage in this country.

My name and response does not need to be confidential.

Sincerely,

Alan Rushworth

## SIMON RUSSELL

Subject: privacy policy

Dear consultation team,  
Please consider strengthening privacy laws.  
My name and response does not need to be confidential.  
Sincerely,  
Simon Russell

## IAN SAMBROOK

Subject: Privacy verification

Dear consultation team,  
  
My name and response does not need to be confidential.  
Sincerely,  
Ian Sambrook  
It is Essential that privacy is protected.  
Particularly given the example of the scandal of Cambridge Analytical.

## ANNA SANDFIELD

Subject: AV Tools

Dear consultation team,

I am gravely concerned about that the government is leaving it up to private companies to creat AV technology.

The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.  
Sincerely,  
Anna Sandfield

THOMAS SARGEANT

Subject:

Dear consultation team,

The fact that there is a regulatory gap between BBFC and the ICO, with no one assigned to oversee privacy, is ludicrous. In the wake of scandals such as Cambridge Analytica, our privacy must be at the forefront of our thinking for any large scale data collection and retention.

Similarly, 4.3 uses the word "should" with regards to data protection and compliance with the IOC guidelines. This is once-again non-binding, which is a major point of concern for those submitting information potentially as personal as their pornography viewing habits.

Furthermore, to trust private companies, without having strong sanctions in place, resulting from clear and robust guidelines, leaves people vulnerable. To hold the identities of individuals, plus their pornography habits, invites attacks such as the Ashley Maddison leak. Something that could have a profound, and damaging impact on people, both professionally and privately.

My name and response does not need to be confidential.

Sincerely,

Thomas Sargeant

ALEX SARLL

Subject: Consultation on age verification

Dear consultation team,

The risks of the proposed approach far outweigh the intended child protection benefits - especially since history shows that inventive teenagers are likely to get around whatever barriers are erected (whether by high tech methods, or simply 'borrowing' parental ID).

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Alex Sarll

## BEN SAXON

Subject:

Dear consultation team,

I am writing to register my concern and alarm about the lack of provision for ensuring privacy in any age verification technology which may be employed to ensure that users are over 18 years of age when visiting porno graphic websites.

I understand that it will be left to private companies to develop and implement the technology, and that there has not been sufficient safeguarding put in place to ensure that this technology ensures privacy.

In a world where privacy of personal data is increasingly difficult to control, and with recent scandals involving Facebook and other social media platforms, it is more important than ever that you ensure privacy of UK residents is protected as well as it can be.

Please do not put citizens' privacy at unnecessary risk and open yourselves up to a scandal in the process. It's in everyone's best interest that privacy is taken seriously in this matter.

My name and response does not need to be confidential.

Sincerely,  
Ben Saxon

## IAN SAXTON

Subject: Age verification technology

Dear consultation team,

I am writing to express my concern that proposed legislation around age verification and pornographic websites.

It seems to me that in the light of the Cambridge Analytica scandal, the government should be doing all it can to ensure privacy and that details of individuals usage of the internet remains private information, protected from commercial activity (unless that is what the individual specifically wants).

The proposed legislation is woefully inadequate, where nobody is assigned to oversee privacy. This is inviting trouble.

Private companies have been proven to disregard user privacy, so they must be given strict privacy guidelines.

My name and response does not need to be confidential.

Sincerely,  
Ian Saxton

## JOHN GARETH SCRATCHER

Subject: UK age verification nonsense

Dear consultation team,

It is my strong belief that an age verification system for pornographic content is most worryingly a slippery slope toward a database of the nation's viewing habits and yet a trivial hurdle for thousands of tech-savvy young people.

As you already know, we already have an adult content block on the web, enforced by the ISPs, in addition to optional child protection software provided by the vast majority of ISPs

This is a hugely disproportional response to the problem of children viewing unsuitable content. Imagine if to curb under-age drinking the government announced passport scanners were to be fitted to the doors of every pub in the country.

A private company with a database of a whole countries porn viewing habits would be a huge target for hackers, especially at a time when Russia is threatening cyber-warfare. That data is far to sensitive, the divorce rate could sky-rocket if it was leaked.

Finally, I highly doubt how effective it would be, once an adult film has been saved to someone's hard disc or mobile phone any age verification system would be wholly pointless as it could be shared by dozens of other methods. I'm young enough that I was still in education when the first bluetooth mobile phones were released and I saw some pretty extreme content shared over that primitive medium. Now multi-terabyte portable hard drives have built in Wi-Fi for transferring content locally to multiple devices with no web access required. It is foolish to think that playgrounds wouldn't simply replace streaming sites as places for hormone-riddled teens to share clips.

A step toward Chinese-style oppressive state censorship is the wrong way to solve this problem. I hope you agree.

My name and response does not need to be confidential.

Sincerely,  
John Gareth Scratcher

## COLIN SCOTT-MONCRIEFF

Subject: Age verification system

Dear consultation team,

I am greatly concerned about the future prospect of individuals having to have their age verified to view adult material for the following reasons -

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

I don't believe that the system proposed is open to abuse and wouldn't be fit for purpose.

Please reject the plans as they stand. More work needs to be undertaken to make this work.

My name and response does not need to be confidential.

Sincerely,

Colin Scott-Moncrieff



PARESH SHAH

Subject:

Dear consultation team,

I am opposed to the current proposals for age verification (AV) for pornographic sites and do not think enough thought has been put in to AV tools by Government.

Privacy should be an integral feature for any AV tools.

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a security breach could be catastrophic for millions of UK citizens, especially as any associated data on addresses, banking details etc. may be used for criminal activities. This is why privacy must be a priority.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Facebook/Cambridge Analytica scandal and Russian-inspired cyberhacking, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will hold both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Paresh Shah

## CRAIG SHAW

Subject:

Dear consultation team,

I am concerned about the proposed introduction of age verification tech. The Cambridge Analytica scandal is a vivid reminder that private companies are not reliable guardians of our personal data.

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Craig Shaw

## ROGER SHEPHERD

Subject: Age verification (AV)

Dear consultation team,

I understand the BBFC is to guide how AV tools operate. I am very concerned that AV tools might open up another way in which people's privacy is undermined. I think it is essential that the very sensitive records of people viewing habits are kept private - in practice that means they must not be recorded. I would advise that the BBFC takes this matter very seriously - when (not if) the first breach occurs, people will see the BBFC as responsible.

My name and response does not need to be confidential.

Sincerely,  
Roger Shepherd

NICK SMEDLEY

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Nick Smedley

If I want to view sensitive material and have to pay and/or join to view a site then my details should be treated as sensitive also- I'm not paying to have my confidential information shared around or stored.

JACKY SMITH

Subject: Strong privacy is a must for age verification tech

Dear consultation team,

In response to the call for public comment on AV guidelines, my first thought is that the GDPR requires the data companies store to be proportionate and secure, while you are leaving it up to private companies to create AV technology. There's a regulatory gap here, surely?

The Cambridge Analytical scandal is just one example of the sort of problems that arise when you do this. Companies based outside the EU can use the AV requirements to obtain person identifiable and verified data on people's real world identity - and then record their porn habits. A blackmailer's paradise.

This will increase demand for stolen identities, already easily available on the black market. Can we foresee acid attacks run to obtain driving licences?

On the other hand, the sort of company that ignores regulation will simply operate as at present and therefore collect more young and vulnerable users, since young people will be unable to obtain access to less irresponsible sources.

I cannot see how the proposals will improve the current chaotic situation.

My name and response does not need to be confidential.

Sincerely,  
jacky smith

## MAX SNYDER

Subject: Verifying adult content viewing

Dear consultation team,

I have serious concerns around data in regards to:

'Requirements for pornographic websites to verify UK users are over 18 will come into effect soon, and the BBFC is in charge of issuing guidance for how age verification (AV) tools must operate.'

Trusting third parties online, let alone adult entertainment sites with your personal information causes serious concern. Also, these sites will then have data on the users that causes equal concern.

My name and response does not need to be confidential.

Sincerely,

MAX SNYDER

## THOMAS STACKHOUSE

Subject: Privacy

Dear consultation team,

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

Thomas Stackhouse

## TORBEN STEEG

Subject: Age verification technology requires strong privacy rules

Dear consultation team,

I support the idea of age verification tools to protect minors from pornography. However such tools must come with strict privacy guidelines.

We cannot (as the recent news about Facebook and Cambridge Analytics has shown) rely on private companies to set their own rules on privacy; the financial incentives to use data for profit and reduce security costs are too high.

Please ensure that age verification is accompanied by strict privacy guidelines and associated high penalties for breach of the guidelines.

And please make it clear where, between the BBFC and the ICO, responsibility for oversight of the privacy regulations lies.

There is really no excuse, in the light of what we know about how private companies have repeatedly failed to keep data private, for this issue not to be dealt with robustly and clearly.

My name and response does not need to be confidential.

Sincerely,

Torben Steeg

## SHAUN STEINER-GOLDBERG

Subject: Age Verification

Dear consultation team,

While I applaud protecting young people online, AV as described doesn't seem to be the way to do it.

AV tools have been created by companies who would doubtless collect records of pornography use and not be averse to selling them. Money is, after all, the driving force behind private companies. That is without considering the risk of data breaches and hacking. Privacy has scarcely been mentioned in relation to this, and the BBFC would be pretty toothless in regard to this.

Until privacy is taken seriously in this bill, I will be against AV as it stands. A better way for keeping online pornographic material away from minors needs to be found.

My name and response does not need to be confidential.

Sincerely,

Shaun Steiner-Goldberg

## RICHARD STEWARD

Subject:

Dear consultation team,

In this age of data collection exploitation, there has to be a better way to achieve your goals than to give more websites sensitive data than this. If I can see the folly in this agenda, then surely you can.

Don't throw the baby out with the bath water.

My name and response does not need to be confidential.

Sincerely,  
Richard Steward

## LAUREN STONEBANKS

Subject:

Dear consultation team,

My name and response does not need to be confidential.

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

Sincerely,  
Lauren Stonebanks

## DARREN STYLES

Subject: Age verification for pornographic sites

Dear consultation team,

Age verification for pornographic sites will inevitably involve those pornographic websites, and / or other third parties working on behalf of the government, retaining the personal details and pornographic browsing history of users. How will this data be kept secure? I argue that this data would be open to misuse (scams, spam etc.), hacking, identity theft and blackmail - and that given the quantity of pornographic websites online it would be near impossible for the government to effectively control this and keep users details secure. Also it will be impossible to stop fraud scam websites from obtaining peoples details under the guise of 'government requirements' in order obtain or exploit peoples details - there would be a huge trend toward this kind of 'scam' and it would be an immensely distressing and commonplace occurrence.

The Government is leaving it up to private companies to create AV technology. That means companies will collect highly sensitive records of the public's porn watching habits, yet there is no plan for the Government to issue strict privacy guidelines for AV tools.

The Cambridge Analytica scandal is a very vivid reminder that private companies are not reliable guardians of our personal data. The Government should therefore be prioritising privacy for AV technology. The consequences of a data breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

I understand that between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

Furthermore, what is the governments position on the impact of this legislation as an international precedent - and the impact such a precedent will have on the potential for data collection, blackmail and the persecution of sexual minorities in other nations? This is a very dangerous precedent for millions of people around the world.

My name and response does not need to be confidential.

Sincerely,  
Darren Styles

## MARCUS J. SWIFT

Subject: DE Act

Dear Consultation Team,

Although this will not personally affect me, I am nonetheless supporting those for whom it does, plus I do not wish any precedent to be established that does not protect privacy at its core for Age Verification systems in any field.

Whilst it is obviously important to protect children, it is the method that is of concern. Privacy is an important right in the digital era, and this Act does not protect the privacy of the legitimate users, leaving those users at risk of breach of privacy, sale of personal information, and even potential hacking of such information.

Protection of privacy must be the first priority for any use of Age Verification systems in any field. My name & response do not need to be kept confidential.

Yours sincerely,

Marcus J. Swift.

## DAVID SYMES

Subject: Data protection in age verification

Dear consultation team,

It is absolutely vital that any technology - including age verification - respects each user's right to privacy, with uses of the data gathered restricted solely to that explicitly notified to the user.

The Cambridge Analytica scandal is, no doubt, just the tip of a far larger iceberg; and there is a grave danger of similar abuses spreading if a tight rein is not kept on these systems, which we are set to see proliferate.

You may be sure that a profit-driven company will "earn a little on the side" from harvesting users' data, unless very tight regulation explicitly forbids this; there is no surprise in this, as far too many profit-driven entities lack any sense of ethics or morality, as I see it.

Apparently, with neither the BBFC nor the Information Commissioner's Office having an explicit responsibility to oversee adequate privacy mechanisms, someone must "step up to the plate;" I sincerely hope that your organisation will do so, at least on this particular issue.

My name and response does not need to be confidential.

Sincerely,

David Symes



CHRISSI TAYLOR

Subject: Digital Economy Act and privacy

Dear consultation team,

I'm very concerned about the DEAct and the lack of government care for private data/security.

There is a massive chance for a data breach or hack, which could now contain passports, drivers licences, and credit card details as well as the publics porn viewing habits LINKED to those details.

Not only that, but any child could find their parent or guardian's passport and send a copy to any company to get access to porn, and they'll have far less concerns about the legitimacy or safety of that site and could potentially open their parent up to massive issues.

By not issuing clear guidelines the Government can blame the private sector (You, in this case) for any data breaches that occur.

I'm all for stopping children from having access to porn before they're of legal age, but this seems poorly thought out and ultimately dangerous for the general public.

My name and response does not need to be confidential.

Sincerely,

Chrissi Taylor

## DAVID TAYLOR (MELONFARMERS)

### **Re Guidance on Age-Verification Arrangements Re the BBFC's Approach as set out in Chapter 2?**

I don't agree with the government's age verification law, but given that the law has been passed, I agree that the BBFC Approach to implementing the law is reasonable

### **Re Age-verification Standards set out in Chapter 3?**

I don't think that these standards are adequate for the task in hand, and need further technical development.

### **4. This guidance also outlines good practice in relation to age-verification to encourage consumer choice and the use of mechanisms that confirm age but not identity.**

I think you should point out to porn viewers that your ideas on 'good practice' are in no way enforceable on websites. You should not mislead porn viewers into thinking that their data is safe because of the assumption that websites will follow 'best practice'. They may not.

### **5c. A requirement that either a user age-verify each visit or access is restricted by controls, manual or electronic, such as, but not limited to, password or personal identification numbers**

This is a very glib sentence that could be the make or break of user acceptability of age verification.

This is not like watching films on Netflix, ie entering a PIN and watching a film. Viewing porn is more akin to browsing, hopping from one website to another, starting a film, quickly deciding it is no good and searching for another, maybe on a different site. Convenient browsing requires that a verification is stored for at least a reasonable time in a cookie. So that it can be access automatically by all websites using the same verification provider (or even different verification providers if they could get together to arrange this).

At the very least the BBFC should make a clearer statement about persistence of PINs or passwords and whether it is acceptable to maintain valid verifications in cookies.(or age verifier databases).

The Government needs adults to buy into age verification. If the BBFC get too fussy about eliminating the risk that under 18s could view porn then the whole system could become too inconvenient for adults to be bothered with, resulting in a mass circumvention of the system with lots of information in lots of places about how and where porn could be more easily obtained. The under 18s would probably see this too, and so this would surely diminish the effectiveness of the whole idea.

The very suggestion that users age verify each visit suggests that the BBFC is simply not on the right wavelength for a viable solution.

Presumably not much thought has been put into specifying advance requirements, and that instead the BBFC will consider the merits of proposals as they arise. The time scales for enactment of the law should therefore allow for technical negotiations between developers and the BBFC about how each system should work.

**5d. the inclusion of measures that are effective at preventing use by non-human operators including algorithms**

What a meaningless statement, surely the age verification software process itself will be non human working on algorithms. Do bots need to be protected from porn? Are you saying that websites should not allow their sites to be accessed by Google's search engine bots? Unless there is an element of repeat access, a website does not really know that it is being accessed by a bot or a human.

I think you probably have a more specific restriction in mind, and this has not been articulated in this vague and meaningless statement

**7. Although not a requirement under section 14(1) the BBFC recommends that age-verification providers adopt good practice in the design and implementation of their solutions. These include solutions that: include clear information for end-users on data protection**

When have websites or webs services ever provided clear information about data protection? The most major players of the internet refuse to provide clear information, eg Facebook or Google.

**9. During the course of this age-verification assessment, the BBFC will normally be able to identify the following in relation to data protection compliance concerns: failure to include clear information for end-users on data protection and how data is used; and requesting more data than is necessary to confirm age, for example, physical location information.**

Excellent! This would be good added value from the BBFC

At the very least the BBFC should inform porn viewers that for foreign non-EU sites, there will be absolutely no data protection, and for EU websites, once users give their consent then the websites can do more or less anything with the data.

**10. The BBFC will inform the Information Commissioner's Office where concerns arise during its assessment of the age-verification effectiveness that the arrangement does not comply with data protection legislation. The ICO will consider if further investigation is appropriate. The BBFC will inform the online commercial pornography provider(s) that it has raised concerns with the ICO.**

Perhaps the BBFC could make it clear to porn users, the remit of the ICO over non-EU porn sites, and how the BBFC will handle these issues for a non-EU website.

**Re Data Protection and the Information Commissioner's Office**

The world's major websites such as Facebook that follow all the guidelines noted in this section but end up telling you nothing about how your data is used, I don't suppose porn sites will be any more open.

**3b Where an organisation processing personal data is based outside the EU, an EU-based representative must be appointed and notified to the individual**

Will the BBFC block eg a Russian website that complies with age verification by requiring credit card payments but has no EU representative?

I think the BBFC/ICO needs to add a little bit more about data protection for websites and services outside of the EU. Porn viewers need to know.

### **General**

Perhaps the BBFC could keep a FAQ for porn viewers eg Does the UK vetting service for people working with children have access to age verification data used for access to porn sites?

## **JASON TEMPLE**

Subject: Verification Proposals

Dear consultation team,

I am adding my concerns to the list of people worried about the implications of this poorly thought out and totally unnecessary legislation.

1. Putting sensitive personal data about use of adult resources in the hands of private companies, or indeed the government, is outrageous and dangerous for varying and obvious reasons.
2. There is simply no need to implement age verification. Anyone who wants to will get around it as a supplier or user, and the under 18's can still get unlimited whatever they want from other sources like social media.
3. This smells like a step towards the ludicrous US FOSTA law which is currently destroying lives, careers and stigmatising sex workers for literally NO benefit anyone can define in terms of limiting sex trafficking, or underage content, which could be stopped under the US, and can by UK laws as they stand.
4. There is a freedom of expression and right to privacy issue here that is already a problem in this country, where already confirmed as 18+ mobile phone users have to call to ask for adult content blocks to be removed, which is obviously logged in a database and could be hacked for blackmailing.

My name and response does not need to be confidential.

Sincerely,  
Jason Temple

## COLIN TEMPLEMAN

Subject:

Dear consultation team,

My name and response does not need to be confidential.

I would like to comment on the Age Verification process requiring porn sites to verify users are over the age of 18.

- The use of AV tools inherently have the capability of capturing data on an individual's porn watching habits and could in the wrong circumstances create leverage against the individual using the stigma of revealing such to other parties. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the recent Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.
- Any processes deployed must of course be 100% General Data Protection Regulation (GDPR) compliant.

Sincerely,  
Colin Templeman

## ADAM THOMAS-HAYTER

Subject: Age verification

Dear consultation team,

You must implement strict rules and regulations with regards to personal data and age verification.

My name and response does not need to be confidential.

Sincerely,  
Adam Thomas-hayter

CHRIS THOMSON

Subject: Privacy considerations with regards to AV technology

Dear consultation team,

I have a number of concerns with regards to the upcoming requirement to implement technology with intent to verify the age of consumers of adult content on the internet ("AV" tech).

First and foremost, if we are to have such a system I feel it is important to have strong regulatory oversight over how such a system is implemented, and clear limitations as to how that data may be used. It is my understanding that at the present time there is little in the way of codified regulatory practices for private companies to adhere to when handling this data.

If no regulations are upheld, I expect that information collected by the facilitators of such content would be attributed to user accounts and potentially used in tandem with site analytics to build demographic profiles for sale to advertisers and other third party agents.

Further, should no regulations over how this data may be used be put in place I foresee an event where information such as the viewing data of identifiable private citizens is irrevocably leaked into public hands as a result of a data breach - an event that would certainly provoke outrage.

Additionally, I feel that if there is a data breach that puts into jeopardy the security of collected user information - then the government and the BBFC ought to be held to account for not presenting more stringent regulatory measures, and it is my view that they will likely be seen as accountable in the public eye by virtue of their initial mandate for the implementation of these systems.

My name and response does not need to be confidential.

Sincerely,  
Chris Thomson

## REBECCA THOMSON

Subject: Privacy Concerns

Dear consultation team,

I am concerned that current age verification techniques would pose a huge risk to people's privacy. Which is a serious threat in this day and age.

This will also have a huge impact on independent producer's/seller's and could cause many people to struggle financially. If a verification system becomes mandatory it will give those with a larger influence/profit an unfair advantage whilst forcing out the smaller producer's.

My name and response does not need to be confidential.

Sincerely,  
Rebecca Thomson

## JAMES TOLMIE

Subject: Age Verification Concerns

Dear consultation team,

While I agree that protecting young people is vital, I have some grave concerns about the current plans for implementing age verification tools.

As the government has let private companies build those tools, I believe that (especially in the wake of the Cambridge Analytica scandal) there is a serious risk that sensitive personal data for millions of citizens could be misused. Private companies are clearly capable and willing to bend or ignore guidelines, so I believe they must be as strict as possible to avoid yet another scandal.

I am also concerned that seemingly neither the BBFC or the ICO have been assigned to oversee privacy in this matter.

My name and response does not need to be confidential.

Sincerely,  
James Tolmie

TOM TRAINER

Subject: tomtrainer@gmail.com

Dear consultation team,

Allowing private companies to run AV would be a disaster for the following reasons:

- AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.
- Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.
- In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.
- It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response do not need to be confidential.

Sincerely,  
Tom Trainer



## ZACH TYBALT

Subject: Age verification

Dear consultation team,

Please don't sleepwalk into linking private personal data with private viewing habits. This should be so completely obvious with all of the fallout surrounding Facebook and the exploitation of private data to manipulate the public. You could well be involved with facilitating the next level of manipulation. How can you guarantee sensitive data cannot be hacked, stolen or sold illegally? You can offer zero guarantee as that is the very business model of these big data companies who buy our medical records and credit histories without our knowledge never mind criminal gangs who trade stolen details like this. Will it be the BBFC who are ultimately liable when the class action suits start? I know that sounds bleak but this seems inevitable when you are offering up such intimate data directly linked to individuals and exposing them to corruption, blackmail, extortion and who knows what else. The fact that there are no mandated safeguards in addition just beggars belief.

My name and response does not need to be confidential.  
Sincerely,  
Zach Tybalt

## SIMON TYSZKO

Subject: age verification

Dear consultation team,

Time and time again we have seen how the 'free market' has worked against the original 'utopian' open principles of the internet, and turned the 'information superhighway' into a kleptocratic free for all, where our most basic privacy is capitalised and repeatedly sold beyond any possible control. This proposed legislation is a classic 'grandad' knee-jerk reaction, that creates far far more problems than it could possibly solve (and it will not solve this basically 'Daily Mail' non problem). This legislation is ill thought out, extremely dangerous, and totally ineffective in any realistic scenario.

It must be stopped and taken back to a drawing board.

My name and response does not need to be confidential.  
Sincerely,  
simon tyszko

## CHARLES UNDERHILL-TYRELL

Subject: Verification 18+ web porn

Dear consultation team,

Porn is a very private thing. People from the age of puberty are going to masturbate and get their hands on pornography.

There will be very easy workarounds to this that make it a pointless and fascistic puritanical endeavour.

All this will be is a data mining act where your kinks and use of pornography could be used for dubious motives.

The Cambridge Analytica and Facebook scandals show that private companies are the last people who should have access to details of what you like get yourself off to.

My name and response does not need to be confidential.

Sincerely,

Charles Underhill-Tyrell

## SEAN URQUHART

Subject: AV verification

Dear consultation team,

AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.

Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.

In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.

It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,

Sean Urquhart

FABIO VALENTI

Subject: Balancing Protection with Responsibility

Dear consultation team,

I am very much for the age verification process that will undoubtedly help protect children from being exposed to pornographic material. I believe that such exposure may in many instances have a deleterious effect on a child's mental health.

However, the process of verification will ask for an internet user to enter sensitive information onto the world-wide web. This leaves them open to significant risk. The government cannot implement a policy that increases the risk of a massive proportion of the public being exposed to online crime, without taking the basic responsibility of ensuring that such a risk is minimalised. The way to do this is through strong privacy guards and privacy regulations. I do not think it is too strong to say that if the government requires what is probably the majority of the adult British Public to hand over information which could be used to commit crimes against them, that the government also makes an effort to protect that public from the risk it is asking them to take on. To do less would be reckless and irresponsible.

On the one hand the government is acting in an ethically admirable way- by attempting to protect children. But on the other hand the current legislation as it stands, with its vague and sparse attention to protecting the rest of the public from online crime, is totally unethical.

If the government compels one to take on greater responsibility for the benefit of society, then one would expect that the government also takes on its fair share of that responsibility, and not needlessly increase the risk of nationwide hacking, data mining, online blackmail etc. It is simply unethical, short sighted, and will undoubtedly leave us with more complex problems as a nation.

I rather feel the government is whistling past the graveyard on this matter, and I for one would appreciate a robust outline of how exactly they propose to protect the public from the inevitably negative consequences of their legislation.

My name and response does not need to be confidential.

Yours faithfully,  
Fabio Valenti

## FRANCIS VOISEY

Subject: Pornography and age verification technology

Dear consultation team,

I am writing to you in response to the government's proposed requirements for age verification for pornographic websites, something about which I have serious concerns, especially in view of the recent scandal involving Facebook users and Cambridge Analytica. I am not ashamed to say that I regularly use pornographic websites. I am over 18, in fact almost 66. What does concern me is that I do not drive a car and have not been abroad for some years; I do not therefore have a driver's licence or a valid current passport. I would therefore be forced, presumably, to give details of my credit card. I do not wish to receive a bill from Barclaycard next month for say £16,000 because my credit card details have been stolen after I was forced to give them out to this AV scheme.

My name and response does not need to be confidential.

Sincerely,  
FRANCIS VOISEY

## SAMI WANNELL

Subject: Privacy guidelines for age verification

Dear consultation team,

The current climate indicates that self-regulation will not give internet users an adequate amount of privacy.

That's especially an issue with the Digital Economy Act regulations around pornography viewing. Standard data breaches are bad enough, but it's hard to imagine the damage that could come from porn viewing leaks - blackmailing of elected officials? Teachers losing jobs due to public prudishness rather than actual moral issues? Outing of people who are closeted for safety reasons?

For this reason, I think that the BBFC should make sure that strict privacy guidelines are stuck to.

My name and response does not need to be confidential.

Sincerely,  
Sami Wannell

## CHARLES WARD

Subject: Age verification

Dear consultation team

I am writing to express my grave concerns about the implementation of age verification (AV) technology in the UK.

To take but one recent example of Cambridge Analytica, it is clear that private companies are not reliable guardians of our personal data and the government should be taking responsibility for ensuring that privacy is at the heart of AV tools.

It is obvious that AV tools could be used (maliciously or otherwise) to create a sensitive record of the public's pornography watching habits. The consequences of a breach would be catastrophic for millions of UK citizens.

As I understand the current situation neither the ICO nor the BBFC are responsible for overseeing privacy in the AV area. This creates a huge opportunity for abuse.

Strict guidelines, backed by enforceable penalties, must be in place to protect our privacy in this area. Not only does the weak enforcement of AV lead to risks for the public but, if a breach occurs, the public and media will see both the BBFC and the Government as responsible.

My name and response does not need to be confidential.

Sincerely,  
Charles Ward

## DAVID WARD

Subject: Privacy

Dear consultation team,

Your proposed rules make it nearly impossible to adolescents to discover facts about themselves or others. Sometimes, such shortages of facts can result in death, or worse, a lifetime of feeling persecuted, maligned or feeling insignificant. Simply leave things as they are so Parents, not governments or corporations, can decide such issues and, if parents are part of the problem, then the adolescents can still discover the information they seek.

My name and response does not need to be confidential.

Sincerely,  
David Ward

## JAMES WARREN

Subject: Privacy is vital

Dear consultation team,

The levels of potential danger as a result of age verification on adult content is extreme, and there is little action to address these issues. A key lesson in computer science is that no system is ever perfect. The collection of citizen's data, as enforced by law, by literally millions of organisations is a disaster waiting to happen. Data breaches are increasing in commonality, and where some providers will properly isolate and protect data, there is a non-zero chance that many won't. If this data is illegally accessed, it will leave potentially hundreds of citizens in serious danger from blackmail, to spying, to harassment, to possibly even unemployment as a result of a data breach. Data breaches aren't always external. Internally, a group could steal data inflicting the same damage.

The second issue is regulation. There is simply no possible way to ensure that all providers are handling and processing data correctly. To add insult to injury, neither the ICO or the BBFC are taking responsibility. In the end, this means that there are no checks to protect citizens from providers not operating within the requirements for privacy and security. If ever the likely situation of a data breach occurs, it will be found that no one was in control. This will devastate the BBFC, ICO, and government in general. Labelling the UK as a pseudo-police state with no control over itself, with thousands or even millions of users data no exposed. It is your own interest to organize regulation ASAP. Failure to do so, and there will be huge outrage with the BBFC and the government. Considering the kind of data, huge might be an understatement. You'd need a PR miracle to recover within the next century.

After the event of the Cambridge Analytica scandal, the lack of care for privacy is ridiculous. The same has an even greater chance of happening again, only this time with an individual's personally identifying information and sexual activities/preferences. The power that this has to disrupt people's lives and even the political process is one of the most shocking and terrifying threats to our nation's stability and democracy, ever. The influence individuals had with the kind of data Facebook kept, will be nothing like this. It's like comparing the devastation of a slingshot, to an ICBM.

As a computer scientist, and a citizen, I implore you to take this with the kinda of colossal concern this requires. The government has made a terrible mistake with this rule, and has put your organisation in a horrible position. None-the-less, for the reasons stated, you need to take action. For your sake, and for what the BBFC was made for. To protect the citizens of the UK.

My name and response does not need to be confidential.

Sincerely,  
James Warren

## RICHARD WEBB

Subject: Data protection and privacy

Dear consultation team,

With regards to data protection, privacy and information collection connected to website age verification practices:

I believe that the processes related to age verification should have protection of privacy as a core goal rather than as an aside, and as such, there should be strict requirements for keeping peoples personal information secure and strong oversight to ensure that the requirements are met.

As well as requiring that companies and sites keep collected information secure, there should also be a goal of minimising the amount of sensitive information that is collected in the first place, possibly via regulation or by the use of systems that separate age checks from identity (individual sites don't need to know all the personal details of a viewer, just that their age is over 18).

In short, we need to consider and try to avoid issues before the regulations come into force, rather than waiting for something to go wrong and then patching it up later.

My name and response does not need to be confidential.

Sincerely,

Richard Webb

## MIKE WHEELER

Subject: age verification

Dear consultation team,

Ensuring children and young people are protected, educated and given parental care regarding pornography websites is vital. There are, however, grave concerns about the apparent reliance on age verification to achieve this, and the technology itself.

AV tools may create a sensitive record of the public's porn watching habits. A breach of privacy, such as that recently witnessed in the case of Cambridge Analytica would have catastrophic consequences for millions of UK citizens. Privacy must be a priority.

My name and response does not need to be confidential.

Sincerely,

Mike Wheeler

## ROBERT WHITE

Subject: Age Verification Tools

Dear consultation team,

Privacy must be a priority. Privacy breaches such as the recent Cambridge Analytica fiasco make it imperative that privacy concerns have to be taken seriously. Clearly it is not beyond private companies to disregard user privacy so require strict guidelines on the issue.

A breach of the highly sensitive records of the public's porn-watching habits would be a disaster. What's more, if such an embarrassing breach occurred the public would see both the government and the BBFC as being responsible.

My name and response does not need to be confidential.

Sincerely,  
robert white

## EDGAR WHITLEY

Subject: Response to Consultation on draft Guidance on Age-Verification Arrangements

I am hoping that, although I missed the deadline for responses, you will include my submission in your considerations.

Edgar

## PR WICKENDEN

Subject:

Dear consultation team,

When drafting the Digital Economy Act (DEAct), I am told by the OpenRightsGroup, that the Government did not mention privacy much at all and left the design of AV tools to the market.

Surely, companies will take advantage of this ability to collect highly sensitive records of the public's porn watching habits. This is data that can be abused, sold, or hacked.

By not issuing clear guidelines the Government will be able to blame the private sector for any data breaches. The Government has opted out of its responsibility and I ask that this be reconsidered and that the government moves to protect the public's privacy.

My name and response does not need to be confidential.

Sincerely,  
PR Wickenden



## PINKY WILDING

Subject: Age Verification

Dear consultation team,

I would like to express my concern over the current plans for age verification. I have huge concerns over the way it's being proposed, including the potential for a data breach. The privacy of internet users must remain key.

My name and response does not need to be confidential.

Sincerely,  
Pinky Wilding

## MATTHEW WILLIAMS

Subject: You will not be able to put strong enough privacy controls in place

Dear consultation team,

I am keen to know what recourse members of the public will have when their personal information is INEVITABLY misused? Personal information that should never have been gathered in the first place. Personal information gathered with no oversight.

How will members of the public distinguish between trustable parties and bad actors?

This, in light of the recent Cambridge Analytica scandal that has shown Facebook to be a bad actor, unable to secure the personal data of tens of millions of individuals. Misusing personal data to corrupt our democratic process in the vote leave campaign.

My name and response does not need to be confidential.

Sincerely,  
Matthew Williams

## MATTHEW WILLIAMS

Subject: Privacy considerations for Age Verifications

Dear consultation team,

I wish to express my concerns for the new Age Verification technologies to be used on pornography. Clearly there is no way to verify a persons age without also exposing personal details of the user (especially if the companies are in control of their own technologies to check). This data, including the sexual preferences of the user should be considered as sensitive if not more sensitive than their financial data and treated as such with strong encryption and protection (as well as internally at the companies not just for data breeches), this data should not rely on the standard Data Protection Act as standards for storing but should largely exceed as stated above.

Overall the Age Verification and personal data stored needs to require that rigorous, legally enforceable data protection, privacy and security standard is implemented up to similar standards as financial and email data.

My name and response does not need to be confidential.

Sincerely,

Matthew Williams

## MIKE WILLIAMS

Support: Age verification tools

Dear consultation team,

The Government must take responsibility for protecting the public's privacy, they have a duty to do this; they cannot simply leave the design of AV tools to the market.

AV tools collect the most sensitive information. Strong privacy requirements for these tools are essential.

My name and response does not need to be confidential.

Sincerely,

mike williams

ZAC WILLIAMSON

Subject: Consultation regarding Age Verification for internet access

Dear consultation team,

The proposals in there current form are very concerning, especially in light of recent data leaks from the Cambridge Analytics scandal.

The current proposals wil require UK internet users to provide sensitive personal information to a third party organisation - I have no confidence that this information will be secure.

The proposed AV tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens, who could have their lives ruined simply for accessing legal pornographic material.

This is without the consideration that the AV project is unlikely to accomplish it's stated aims, as those under 18 are often far more technologically literate than they are given credit for, they will simply use VPN or TOR systems to bypass any barriers put in place.

I would urge the BBFC to prioritise privacy and data security in any final guidelines.

My name and response does not need to be confidential.

Sincerely,

Zac Williamson

ANDREW WILSON

Subject: Age Verification Technology

Dear consultation team,

I was deeply concerned to learn of the lack of privacy protections in place in the new age verification regulations for pornographic material.

Whilst we are still grappling with privacy legislation designed before the internet was conceived, it is hard to see why the government would consider any legislation for the digital age without proper consideration for the ease at which our private information is illegally obtained from data storage facilities and used against the owner's wishes.

Requiring websites to gather private and identifying documents to view legal material has a vast potential to infringe human rights, whilst better safeguards (such as a parental protections systems) exist. Further I am very concerned by the lack of future proofing in the legislation.

My name and response does not need to be confidential.

Sincerely,  
Andrew Wilson

IAN WINGMORE

Subject:

Dear consultation team,

My name and response does not need to be confidential.

Sincerely,  
Ian Wingrove

## MIKE WOOLFE

Subject: Age verification and BBFC

Dear consultation team,

Please note that this Big Brother approach to controlling viewing habits of the public is ill conceived and easily sidelined by determined younger viewers. The Privacy side of your arrangement seems lacking in clarity and would seem to be equaling Facebooks dismal lack of social responsibility.

Private Companies and Governments are regularly proven to be inadequate gatekeepers of personal data, whether by blatant misconduct or leaving electronic devices and storage media in taxis and public transport.

I strongly oppose the methodology and concept being put forward by this type of verification. This should be put into the realm of businesses that are used to working with sensitive information in a secure way with end to end encryption. The technology is there get those who know how to use it to apply it, this is NOT the Government ( NHS systems a good case in point) and not some political lap dog company such as BBFC, .

Sincerely Mike Woolfe

My name and response does not need to be confidential.

Sincerely,

Mike Woolfe

## DAVID WRAGG

Subject: AV requirements

Dear consultation team,

I work in the tech sector. When it comes to data breaches, it is simply a matter of when, not if, data leaks into the public sphere. Once it is out, it cannot be reclaimed.

The simple rule is this: do not collect data you would not wish to be leaked.

I would have thought the headlines of the last few years (and especially the last few weeks) would be instructive on this, but perhaps some of the nuance has proved elusive.

The only way to prevent sensitive data falling, eventually, into the hands of malicious actors is not to collect it in the first place.

My name and response do not need to be kept confidential.

Sincerely,

David Wragg

DOUGLAS WRIGHT

Subject: Adult Verification

Dear consultation team,

It is increasingly clear that legislation is not keeping track with innovative technology and it is to be applauded that more time has been assigned to study ways of implementing adult verification rather than rushing in with half-baked laws.

However, and in light of an increasing number of data breaches, I feel that relying on the private sector to administer such as scheme is doomed to failure. The free market can provide solutions but experience shows that they cannot always be trusted with running them. Failure in terms of data retention and forwarding is far more harmful than - say - overcharging on electricity bills. Once sensitive data is released it cannot be retrieved or compensated for.

At present the state provides the definitive information as to how old a person is- passports, birth certificates, etc. It should be a simple matter to arrange for a suitable digital certificate to be made available upon request and based on currently-held records. A comparison might be the Police Scotland criminal record check (in simple terms a personal DBS check). Completed online it is turned around in 48 hours or so and costs £25. Those wishing to view adult material online (I note that there is no requirement for television reception) would surely pay for a lifetime certificate confirming their eligibility if it means safeguarded data. It would also permit those adults not permitted to access material, such as on the sex offenders register, to be excluded.

If the state wishes to impose upon its citizens then it should be up to the state to provide adequate solutions, not relying on lowest tenders, hidden agendas and myriad other flaws. The state supplies passports, it prosecutes criminals and it collects taxes. It should also take responsibility for confirming age.

My name and response does not need to be confidential.

Sincerely,

Douglas Wright

## CHRIS YOUETT

Subject: Re: strong privacy is a must for age verification technology

Dear consultation team,

A legal requirement for pornographic sites to verify UK users are aged over 18 will come into effect soon - and the BBFC is responsible for issuing guidance on how age verification (AV) tools must operate.

At the Government is passing the buck to private companies to create this technology, they will be able to build up highly sensitive records of users' tastes. This gives AV tool suppliers wide opportunities to pressure and blackmail users. There is no proper regulation of these tools - and it is in the BBFC's interest to make sure that all AV tools protect the public's privacy

My name and response does not need to be confidential.

Sincerely,  
Chris Youett

## ANDREW YOUNG

Subject: Privacy and data protection under age verification proposals

Dear consultation team,

With regard to the proposals concerning age verification for adult websites. It is most disturbing that privacy and data protection appear to have taken a back seat in this process. It is essential, especially in light of recent events, that privacy and personal data are seen to be treated with the utmost care and responsibility. Please take these views into account when finalising any proposals.

My name and response does not need to be confidential.

Sincerely,  
Andrew Young

CRAIG YOUNG

Subject: Privacy must be protected

Dear consultation team,

I'm writing to express my concerns at the lack of privacy controls upon the introduction of the new age verification (AV) tools.

As a parent, naturally I want my young child to be kept safe from viewing pornography, but I'm also concerned that the government appears to be leaving it up to private companies to create their own AV technology.

If companies are going to be charged with collecting highly sensitive records of the public's porn watching habits, then the government must issue strict privacy guidelines for AV tools.

Privacy must be integral to any and all AV tools; the Cambridge Analytica scandal proved that unregulated private companies are not reliable guardians of our personal data. Private companies are clearly capable of disregarding user privacy, so strict privacy guidelines must be laid down, with meaningful consequences for their breach.

My name and response does not need to be confidential.

Sincerely,  
Craig Young



## ANONYMOUS #1

Subject: Age verification

Dear consultation team,

I am unlikely to sign up to any age verification to be able to access porn sites, so age verification per se does not bother me.

However, I am very concerned that any age verification technology is being left to private companies to develop and provide. What motivation would any such company have re: safeguarding any data about users that is collected? On the contrary, they would have an incentive to collect and sell information about user viewing habits, especially if this involves pornography. The recent revelations about Facebook, and the Cambridge Analytica scandal in particular, is a reminder that private companies are not reliable guardians of personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

In any case, any person with much technical savvy will find a way round any need for authorisation, - although I fear that some of the means for this may be banned, as some now are in Russia.

I am happy to be counted, and hope that my views are taken into account, but I want my name to remain confidential please.

Sincerely,

## ANONYMOUS #2

Subject: Privacy and Age Verification

Dear consultation team,

I am unlikely to sign up to any age verification to be able to access porn sites, so age verification per se does not bother me.

However, I am very concerned that any age verification technology is being left to private companies to develop and provide. What motivation would any such company have re: safeguarding any data about users that is collected? On the contrary, they would have an incentive to collect and sell information about user viewing habits, especially if this involves pornography. The recent revelations about Facebook, and the Cambridge Analytica scandal in particular, is a reminder that private companies are not reliable guardians of personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

In any case, any person with much technical savvy will find a way round any need for authorisation, - although I fear that some of the means for this may be banned, as some now are in Russia.

I am happy to be counted, and hope that my views are taken into account, but I want my name to remain confidential please.

Sincerely,

## ANONYMOUS #3

Subject: DEA Consultation

Response from private individual. I am satisfied for you to publish my response subject to my name and email address not being published.

Response as follows:

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

No. Section 5 of Chapter 2 makes reference to sites most frequently visited, particularly by children. Currently there is no quantifiable data what constitutes a site that can be particularly visited by children, and any such assertion may be based on subjective assumptions which can lead to the inappropriate targeting of resources.

Section 11 makes reference to presence on search engines. Due to algorithms of search engines it is almost impossible for legitimate web content to completely avoid appearance on search engines, and as such this reference is not one I consider holds any significant merit in relation to enforcement action.

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

No. There are significant concerns around large sections of Chapter 3. Section 6 holds a number of areas which BBFC considers in isolation not appropriate control measures, but does not draw conclusions on the efficacy of combination of these control measures.

Section 12 discusses responsibilities lying with the content provider, however this is impractical. If a person under the age of 18 is able to access inappropriate content online following personal misappropriation, there is no possibility of the content provider having control over this.

The ethics of Chapter 3 revolve around age verification in a simple manner, yet then go on to discuss passport, driving licence or credit card verification. Current roll-out of the Government's flagship welfare programme data, early indications suggest there are large numbers of citizens who do not possess any of these documents and are likely to be low income households. Therefore these control measures are divisive and punitive by their implementation nature. Before any implementation of this guidance an impact assessment needs to be completed to assess how low income households may be affected with these controls and data is can be obtained on household income combined with age verification document availability.

Do you have any comments with regards to Chapter 4?

A new generation of data is being collected with a suggestion this is required to comply with DEA S14(1). The method of implementation appears vast, unnecessary and avoidable if the Act and subsequent guidance can be delivered in a more streamlined fashion. Any suggestions made by BBFC so far appear to be divisive, controlling and do not empower individuals to easily make personal choices freely. Conversely, the current methodology under proposal may have a counter-effect of driving readily available foreign VPN's or installing layered network access such as the free TOR Browser to appear from a different country to circumvent controls.

As a result of this behaviour, the suggestions if implemented may have a knock-on effect of making more extreme content not easily found on UK platforms but available globally being available to minors as those who choose to circumvent UK controls. This access to global content can inadvertently effectively leave a back door open to unpoliced global content through TOR Browsers - much has been publicised on this approach on social media and news articles already when discussing this regulation.

Inappropriate data handling has made news headlines on a far too regular basis. Within the pornography industry a massive data breach affecting users of an adult infidelity website caused hugely embarrassing data to be leaked online. Recently the data handling of social media analytics has made world headlines. Attempting to centralise data in the manner BBFC is suggesting will only increase the likelihood of unfriendly sources seeking this data maliciously even when all depersonalisation attempts have been taken.

Relating to the approach of this guidance and consultation, I feel strongly its approach needs a significant review and all current suggestions are too technical and centralised, posing potentially greater risks of accessing inappropriate content through uncontrolled channels and leaving young people at risk whilst creating a digital divide and a lack in data confidence. As such, my suggestion is for BBFC to maintain a high-level enforcement and guidance control but to devolve age verification controls to ISP level. Practically it will still be possible this way for BBFC to flag specific websites with ISP's, and as a result of this an end user can be required to set their control settings to allow all content or filter adult content. In this way it is also possible for content filters to be implemented in a way that the account holder will maintain a PIN that is prompted by the ISP when adult content is sought. Most ISP's have built in age verification of their customers for credit scoring purposes which is likely to be DEA S14(1) compliant.

It is also worthy to note previous Government action to stem streaming of copyright material by blocking websites has failed due to consumer demand and those wishing to obtain such material will simply find a

different way. The suggestions put forward in the BBFC consultation make many assumptions internet access can be tightly regulated in the UK in a way that harks back to a pre-global information era. As a result it appears the practicalities of our global data infrastructure have been forgotten and it is likely to be relatively easy to circumvent country-specific controls on pornography. Far more practical is a solution that empowers end users to take control through ISP PIN verification as an example which is likely to be DEA compliant whilst maintaining public confidence in the safety of young people and avoiding an authoritarian approach.

The spirit of DEA compliance needs to be struck and a balance towards protecting young people and providing ease of access for legal content to be available to adults must be maintained. Guidance material seems to draw a conclusion that tight regulation makes this possible. My spirit towards this consultation reflects tight regulation will drive perverse behaviours to access material from those who should not have access to it, and create situations where adults may unwittingly make access to more extreme content more widely available.

## ANONYMOUS #4

Subject: Age verification consultation

Dear consultation team,

Legislating around internet access, with potentially private companies creating even more detailed troves of extremely personal information tied to British citizens (with the associated security risks of failed technology or intentional hacking) is a privacy risk that should never be taken lightly. Rolling it out to all users, rather than being an option offered by ISPs for those with children who wish to secure their connection (like any other parental controls currently on offer), seems an extreme step which does not correctly weigh the inherent privacy risks (and the lack of regulatory oversight only redoubles this risk).

Why is this not being handled as current mobile and household verification is? A single verification of if the user wants filtered or unfiltered access made by the ISP, not increasing the burden (and creating a privacy risk) on each individual website (which can be served from anywhere on the internet) to verify UK users during every connection to the site.

The underlying concerns in this issue would seem to indicate that mandatory sex and relationship education is required to provide quality understanding by the population about media consumption, not the establishment of a mandatory privacy invasion and internet monitoring. This legislation does not seem capable of actually addressing the issue and the implementation at the website end rather than the ISP end seems both needlessly expensive and massively increasing the privacy risks (something we are already exposed to at the ISP level so adding a new option there would not significantly increase risk, unlike this proposed implementation).

I hope that you rethink the very core implementation details of this proposal as it seems to both create huge risk and not even tackle the underlying issue it is meant to address.

I want my name to remain confidential.

Sincerely,

## ANONYMOUS #5

Subject: age verification

Dear consultation team,

I am just an ordinary person concerned about privacy.

I believe that the current AV framework will do little to prevent underage people from viewing pornographic material. AV does not apply to Twitter, or to erotic literature, and a generation of tech-savvy young people will quickly find ways to bypass age verification systems.

However, age verification presents an enormous risk to privacy. It puts a large amount of very sensitive data into the hands of companies which may not be the most trustworthy and creates a vast blackmail risk which hackers may exploit.

Given the recent cyber attacks on the UK, and the misuse of data by foreign governments, and companies like Cambridge Analytica, a firm which was also engaged in the extensive use of blackmail, I urge you to take a strong line to protect the public's privacy.

Thank you.

I would like my name and address to remain confidential  
Sincerely,

## ANONYMOUS #6

Subject: BBFC consultation

Dear consultation team,

I am against the proposed age verification tools (AV).

I work in IT, and have a very good grasp of technology, and of the limitations of any technology when it comes to keeping information secret.

As can be seen by the many many reports of literally millions of userIDs, passwords, email addresses, postal addresses, and even National Insurance numbers being exposed by either hacking, or incompetence (even from government departments) it should be clear to anyone who looks into it that sooner or later a significant chunk of the AV database will become exposed.

This *\*totally\** ignores the risks of individuals with legitimate access to such a database accessing it for illegal purposes. (such as the cases when police officers are caught using the PNC to investigate their former partners, or former partners new boy-briend. )

So, we are building a system that will hold highly sensitive information about a large number of adults in the UK, and that system will be a high profile target for people seeking to put the information to bad use. We are also building a tool that will allow the state to monitor our access to material that is deemed entirely legal by the courts. (illegal pornography already has methods of being blocked by most ISPs in the UK subject to court oversight)

So the question is, what are we expecting to gain by handing over this level of monitoring (and therefore control) to the state, or risking it falling into the hands of criminals ?

The idea is we protect children from the harm of pornography by instituting AV tools. Considering the very real risk of harm there is to a free society in creating these tools we had better be absolutely sure that they will achieve their goal.

Sadly, the very nature of the internet, and it's de-centralized nature will mean this will fail. The main adult providers with a significant revenue stream in this country will comply, but nothing can compel providers outside of this country to comply.

Making ISPs responsible for blocking content that they cannot confirm is non-adult, will by definition break all forms of Internet privacy, and we've seen in recent months how important that is. Imagine what power Cambridge Analytica would have had if they had access to individuals adult viewing preferences, or web history...

Teenagers being Teenagers, it won't stop most of them seeking out adult material. It will lead to a proliferation of VPN services, anonymising services and technologies such as TOR. It runs a very serious risk of exposing teens to *\*more\** harm through non-mainstream adult sites, into the more exotic, less well known sites.

It will also create an environment that make it impossible for sites that operate to provide real information to under-age teens. An ISP will sooner just block any traffic that might get it into trouble with the law, than risk prosecution, or public shaming. Just look how Apple block any app that has any association with Adult services.



It will also force any small or independent producer of adult material or services, from erotic poems or novels, through to erotic/adult video produces and adult clubs and dating sites off line. Forcing anyone running a small independent, self-empowering business in this area into the hands of large, multinational industrial-scale porn sites.

In summary, this proposal has many many down sides, and does not even have a reasonable prospect of achieving the stated aims.

Please keep my name and address confidential. My comments may be published.  
Sincerely,

## ANONYMOUS #7

Subject: DEA Consultation

I am concerned that the attempt to secure age-verification for online pornography is so vaguely and unrealistically framed that it will be abused to scour British citizens access to open internet content.

Passage 3 about the verification standards lay out no realistic scenario for effective age verification and its hard to envision a solution that wouldn't massively infringe on individual rights to privacy.

Since no viable solution exists, the worry remains that internet sites unable to fulfill the impossible requirements will be subsequently blocked and British citizens will only be able to access sites that the government approves.

Sites that provide news and community for a vast range of non-pornographic means (like for example [www.reddit.com](http://www.reddit.com)) could be blocked for being unable or unwilling to police small pornographic sections to the specification of the British government, or even be abused by bad actors deliberately uploading content to sites in order to get them banned.

It would be better to spend taxpayers money on education for children to understand the dangers of the internet, investment in opportunities in the real world for improved sense of community and mental healthcare people liable to be damaged by access to dangerous content.

The task of policing all pornographic content on the internet is also unrealistic and likely to devolve into a whack-a-mole scenario, which will be unproductive and a complete waste of resources.

Regards

## ANONYMOUS #8

Subject: Consultation on draft age-verification arrangements guidance

Dear BBFC

Regarding chapters 3 and 4 of your DEA draft age-verification guidance consultation, I am very concerned that you have failed to identify any plausible theoretical basis for online age-verification.

I draw your attention to the general comments of the UK Cards Association (UK Finance): [http://www.theukcardsassociation.org.uk/age\\_verification/index.asp](http://www.theukcardsassociation.org.uk/age_verification/index.asp)

"There are a number of options that the merchant may consider which include:

- Not selling age-related goods at all (both online/telephone order/mail order or in a physical shop)
- Sell only age-related goods and services in face-to-face transactions, where certified identification is required from the consumer
- Sell age restricted goods over the internet/telephone order/mail order, and require the signature of an adult upon delivery to an address
- For those with physical shops, enrolling and age-verifying their online customers in-store;
- Allow sales of age-related goods only to customers whose age can be confirmed by age-verification service providers.

...Card companies seek to comply fully with the law, but they have no legal responsibility to check what a young person may try to buy or take a moral position on how cards are used. The onus is on retailers to ensure that their customer is of legal age."

Note that the webpage refers primarily to the use of in-person checks for age-verification and expresses no confidence in the ability of online verification in the absence of subsequent delivery to a named person. They give no indication that payments cards could (let alone should) be used in themselves to confirm age. Indeed, given the multinational nature of online payment card numbers and the multiple laws in different jurisdictions, even a complete card number and security code is insufficient to prove the age of the cardholder, still less prove whether the person submitting the number is actually the cardholder or someone else (such as a younger family member who has had sight of the card).

To the extent that age-verification services purport to be provided by organisations other than payment card providers, the above webpage makes clear that there is no complete register of over-18s against which identities can be confidently matched. And, as you have already identified, lists such as the electoral register are inappropriate as they are public.

Moreover, since verification is not a financial transaction (unlike online purchases), there is no automatic audit trail for a cardholder even to discover subsequently that his or her card number has been used by someone else and report it (in contrast to payment fraud, where cardholders may well spot any fraudulent transactions on the next account statement, and have a strong financial incentive to report it).

Therefore, there is no credible verification scheme yet proposed, unless online submissions are verified against personal presence or postal deliveries to named individuals (which would in practice be likely to reveal the sensitive purpose of its contents from the standard envelope or the high risk of a cohabitant opening it). And you have already rightly declared

that location information, such as a postal address, should not be stored, so this approach is impossible in principle as well as in practice.

The only theoretically risk-worthy system might be one where identity verification is cryptographically separate from website verification (so that neither the verifier knows which adult websites are being used by a given registrant, nor does the website know the identity of the person whose verification has been confirmed and registered). A loose analogy would be ballot paper numbering in UK elections, where it is hard to match the number on a given ballot paper to a given person, since neither list is retained in matching order. But while cryptographically separate matches for registrants and websites would mitigate the disclosure of an individual's specific proclivities, it would still leave the verifying body knowing that an identifiable individual had sought verification from them in the first place, which for many people would still be very sensitive information.

Since EU law overrides domestic law, you have a legal and fiduciary responsibility to ensure that the systems you propose to supervise do not systemically breach the General Data Protection Regulation. It is therefore inadequate for you to act on the naive provisions of the Digital Economy Act alone without actively considering how they may be read down when construed in conjunction with higher privacy principles. This is reinforced by the Human Rights Act requirement that all public bodies comply with the ECHR. In human rights law terms, you and the ICO must give "anxious consideration" to the privacy rights of the individuals whose data you are ultimately regulating. It is not enough for you to ask questions and warn of pitfalls if you have not identified practical and effective mitigations for the problems widely foreseen.

Clearly private sexual preferences are at the high end of sensitive data. For many people, particularly in certain ethnic, religious or sexual minorities, there will be a serious risk of distress, blackmail or suicide if online sexual activities or proclivities are leaked to hackers, foreign powers or the public. Any age-verification database that retains identifying personal information of any kind is therefore a prime target for criminals and nation states. Even if no identifying data were ever stored (a doubtful practicality), identity information in electronic submissions to and from any such database is highly likely to attract interception because of the quantity and value of such sensitive information accessed in one place.

You will be aware that even the most top secret information has been leaked in bulk by Wikileaks and other political and criminal agitators around the world (and presumably a great deal more leaked information is used for blackmail or subterfuge without its theft ever becoming public knowledge). It is therefore inevitable that any nationwide age-verification database will be abused, and probably on an unprecedented scale with a serious likelihood of multiple suicides and violent attacks as well as more general harm to millions of people.

Moreover, websites and service providers of all kinds are increasingly multinational in that servers and ancillary businesses are likely to be located in different jurisdictions from each other, let alone from the prospective end-user. There is a consequently increased magnitude of risk that data protection precautions or enforcement will fail at one or more links in the complex technical chain.

You and the ICO should therefore be extremely precautionary in interpreting the DEA provisions and proactive in ensuring that the GDPR is not set to be systemically breached in the biggest data protection disaster in human history.

In the absence of any plausible verification system (and I have explained above why no current proposal is remotely comprehensive and secure), you should consider whether the UK regulations and policy which you are being asked to apply are fundamentally contradictory or irrational and therefore void.

I want my name and contact details to remain confidential but you may, if you wish, publish the rest of my response.

Yours faithfully

## ANONYMOUS #9

### Age Verification Response

#### Comments on Age-verification Arrangements

*Question: Do you agree with the BBFC's Approach as set out in Chapter 2?*

*Answer: No.*

The approach set out by the BBFC in Chapter 2 is not fit for purpose.

The definition of “commercial” set out in the document is not sufficient to be useful. The BBFC should, in advance of taking any action, set out exacting detailed and specific definitions of commercial, and consult on them. The attempt in both the flawed legislation and this documentation to get out a binary state between commercial and non-commercial does not exist in the real world, where minor advertising surrounds content in many cases by the platform owner or ancillary service provider are used to finance the cost of providing the platform. Nor is there any clarity about a non-commercial blog that might review products in exchange for review samples, nor where someone may discuss their employment as well as their sexuality.

The BBFC claims that it will discharge its responsibilities in a consistent and transparent manner, but it does not set out any direction in how it will do this. There is no useful explanation of how many sites will be investigated, or how that leads to a consistent state of treatment. There is no explanation of any independent regulation of the BBFC's approach or how such consistency or transparency would be measured.

The BBFC is objectively not a transparent organisation. It is not subject to the Freedom of Information Act as it should be, nor does it set out any equivalent publication scheme. It provides poor quality publications about the nature of evidence of harm it claims, and of the independence of its selected experts. The BBFC website was closed on the final weekend before the end date of this publication, which is transparently unprofessional and shows that the consultation itself has not been conducted in a consistent or transparent manner.

The BBFC sets out a perfunctory explanation of its proportionate approach that does not even meet the order of magnitude of detail required. It fails to address –

- That the definition of determining a commercial basis is not made on any useful basis, as set out above.
- The determination if age verification is present does nothing to try and determine harm – for example it stands to reason that a site that provides material behind a paywall and has some samples outside should not be prioritised above sites that are openly available with pirated, advertising funded content where there is no control of what is seen.
- There is no evidence, nor legislative basis for proportionality to look at legal extreme pornography. This section should be removed entirely and shows the discriminatory biases of the BBFC.
- The BBFC does set out any determination of the effects on wider freedom of speech of an action, both in terms of economic or moderation impact nor on other material that might be available on such a site, such as educational or safety material.

- The BBFC does not set out any test to determine the harms caused by any BBFC enforcement actions to the general public or to specific sexual minorities as a result of their actions – for instance by damaging freedom of assembly or increasing internet platform censorship in general of sexual content by creating economic incentives to prevent its publication. It must do if such actions are to have any transparent or consistent approach. The BBFC should produce an annual, independent report that is peer reviewed before publication determining the harm to the general public of its enforcement actions.
- The BBFC proposal does not take in to consideration any of its responsibilities under the Equalities Act in terms of targeting sexual minorities. There is significant concern in this area – for example in terms of evidence of homophobia in the previous DCMS consultations on this legislation which referred to anal sex as a harmful practice.

The BBFC statement on deciding what sites to investigate does not include a workable plan. It claims it will look at the most frequently visited by children, but there are no useful reliable peer reviewed metrics for any such determination. There is no reason for the BBFC to investigate sites with child protection concerns – any such concerns are not within the purview of the BBFC and should be directed immediate to the relevant police services, and to the Internet Watch Foundation who have a much better track record and level of experience than the BBFC. Finally, the BBFC claims it will prioritise sites containing extreme pornography. There is no basis for this determination in the Digital Economy Act legislation, and the BBFC are making an arbitrary judgement that is inappropriate. It should be removed. In all, the entire plan should be fundamentally reworked and a separate consultation carried out on a draft with vastly more detail.

*Question: Do you agree with the BBFC's Age Verification Standards as set out in Chapter 3?*

*Answer: No*

The statement that the use of age verification in relation to the sale of age restricted goods and services online is, at best, dishonest. There is no workable evidence of any success in this area, nor that they achieve a proportional outcome as the BBFC is legally obliged to create.

The BBFC uses the excuse of evolving and fast-moving technology to discharge it's responsibility to produce proper guidance in this area, raising the risk to providers attempting to comply with the legislation. This is not a consistent nor transparent approach.

The BBFC should not be attempting to act in an extra-judicial manner, and should not be referring to any determination that it will assess age verification methods. The BBFC is not qualified nor has made any useful research of harm that overly draconian requirements may cause (including so called "chilling effects" on platforms). This is not a proportionate nor transparent approach and is not fit for purpose.

The BBFC lays out in clause 5a that it will require the usage of data that cannot be reasonably know by another person. This is objectively impossible to achieve, and should be removed as a test. It will not work anyway.

In Clause 6 the BBFC should not be making a determination of compliance with Section 14(1). That is the role of a judge. The BBFC's consideration is damaging and draconian, and these clauses should be removed. The removal of these methods has not been

demonstrated to have any statistical improvement in age verification and causes significant extra harms to sexual minorities and to general public expression. No proportionality test has been carried out on the effects of these methods by the BBFC and should be (and consulted on) prior to rolling out any enforcement regime.

The BBFC states in Clause 8 that it recommends multiple age verification methods, but has not made any cost analysis of a site to provide such methods nor the proportional harm such a recommendation might cause in terms of chilling effects. This is yet another failure by the BBFC to discharge its responsibilities under the legislation.

The BBFC's passing of the buck to the Information Commissioner in clause 10 is a complete abrogation of its responsibilities. The Information Commissioner's office has no useful powers over off-shore sites, so cannot complete its requirements on the vast majority of sites. The Information Commissioner's office does not have sufficient resource to carry out this task, and the BBFC should either provide funding out of its own finances or make this determination itself before providing an even bigger drain on the public finances than it already does.

*Question: Do you have any comments in regards Chapter 4?*

*Answer: Yes*

The section on the good practices in age verification is not fit for purpose. It neither provides enough useful detail, nor makes any test of the financial impact of compliance and the chilling (or real) economic effects of such legislation. The BBFC is not meeting its requirement to be proportional without such tests.

#### Draft Guidance on Ancillary Service Providers

*Question: Do you agree with the BBFC's approach set out in Chapter 2?*

*Answer: No*

The definition of "commercial" set out in Clause 1 is not sufficient to be useful. The BBFC should, in advance of taking any action, set out exacting detailed and specific definitions of commercial, and consult on them. The attempt in both the flawed legislation and this documentation to get out a binary state between commercial and non-commercial does not exist in the real world, where minor advertising surrounds content in many cases by the platform owner or ancillary service provider are used to finance the cost of providing the platform. Nor is there any clarity about a non-commercial blog that might review products in exchange for review samples, nor where someone may discuss their employment as well as their sexuality.

There is considerable concern that the BBFC is not setting out an objective, consistent nor transparent manner as set out in Clause 2. There is no useful explanation of how many sites will be investigated, or how that leads to a consistent state of treatment. There is no explanation of any independent regulation of the BBFC's approach or how such consistency or transparency would be measured. The BBFC's internal leadership and governance arrangements are not fit for purpose for a regulator.



Clauses 3, 4 and 5 sets out that the BBFC will adopt a proportional approach. As noted in the response above on the Age Verification Arrangements, the BBFC's approach there is not fit for purpose, lacking detail and does not fit the legislation or evidence. The BBFC is not performing any test of harm by its actions to determine proportionality. The BBFC is also not meeting its requirements under the Equality Act. The BBFC sites that it will prioritise extreme pornographic material, but has no legislative basis for such an approach, nor any evidence basis. This should be removed, and evidence published of how the BBFC intends to tackle biases in its organisation.

In Clause 9 the BBFC states that it will inform a provider if it considers a person is making extreme pornographic material available to persons within the United Kingdom. The BBFC has no statutory basis for this action under the Digital Economy Act, and should not be undertaking it. There is significant public concern that the BBFC has repeatedly tried to claim extra judicial power in this area based on poor quality research. The laws on extreme pornographic material in the United Kingdom are complex and subject to criminal proceedings and should be left up to the appropriate authorities, especially given the poor track record of successful prosecutions in this area and the threat of political corruption in previous cases such as the Simon Walsh case in 2012.

*Question: Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?*

*Answer: No*

The BBFC claims that it is not possible to even provide an exhaustive list of ancillary service provider categories in Clause 4, but in the event of determining a new category will somehow notify all ancillary service providers, no matter how many millions there may be, what territories they reside in and what languages they speak. It is not even clear the BBFC could ever have enough staff to make such an impossible task happen.

In Clause 6 the BBFC says that it will "request" the Ancillary Services Provider withdraw their services to non-compliant persons. It is not clear on what legal basis the BBFC will do this, it does not have the power to make such a request under the Digital Economy Act, only a notification. This section should make clear no request will be made.

The BBFC appeals process set out in Clause 10 is under specified, and not fit for purpose. No independent regulator of the BBFC's actions is set out. No test of harm of these actions to determine proportionality is set out. No test of discrimination of sexual minorities either under the Equalities Act nor more widely is set out.

### Conclusion

In all, this consultation document is of poor quality and has not been made with sufficient detail, due diligence, legal certainty or evidence to show that the BBFC is remotely up to the task of being age verification regulator. The BBFC should not be undertaking this role, and should step down and notify the Department of Culture, Media and Sport that it is not fit to fulfil it. The BBFC's governance arrangements should be revisited and radically changed, and it's approach to evidence and proportionality subject to expert external review following stakeholder and general public consultation.

| ANONYMOUS #10

Subject: Don't leak my name

Dear consultation team,

Please have name remain confidential because Cambridge Analytica/Facebook just steal it anyway

Sincerely,

## ANONYMOUS #11

To Whom It May Concern,

I am writing to register my concern regarding the draft Guidance on Age-Verification Arrangements, as it seems as if much of the proposals is unnecessary, poorly thought through and ill-advised. My concerns are as follows:

1) Data privacy. At a very simplistic level, the legislation would seem to demand personal information from users in order to access pornography, information that would be stored. In light of recent events, with the Ashley Madison leaks and the ongoing investigations around Facebook and Cambridge Analytica, it would seem ludicrous to talk of privacy or security while requiring users to give such information to a third party company, no matter what supposedly-airtight legislation was put in place to control the use of such data.

2) Discrimination. While larger producers of pornography will be able to cope with these new demands, independent producers will be unable to meet the financial demands. As independent studios are overwhelmingly the producers queer and feminist pornography, it would seem discriminatory to introduce legislation that would drive them out of business.

3) Technical workarounds. While Age-Verification may work for some of the population, there will be many capable of technical workarounds, VPN or making use of the Tor network, who will in turn be able to set up such systems for others. The fact that a higher proportion of people under 18, who have grown up with such technology, will be capable of this themselves seems to be entirely ignored by this legislation. This leads me on to:

4) Protection of children. In section 5 of chapter 2, references is made to services which 'contain potentially indecent images of children or raise other child protection concerns'. In terms of child protection, there is already extensive, effective legislation in place to protect the rights of children, and to criminalise the production and distribution of child pornography. However, if the goal, as seems to be the case with this legislation, is to try and place the genie of online pornography back in an adult-only bottle, then unfortunately it comes far too late. On the other hand, better sex education in schools, and, as has been dramatically proven in the last 6 months, better communication and understanding around consent could go much further in ensuring that under 18s have a fully rounded understanding of sex and intimacy.

In conclusion, I believe that the proposed legislation is both ill-advised and dangerous, and urge the BBFC to abandon it.

Yours faithfully,

## ANONYMOUS #12

Subject: Comments on the consultation on age verification

Dear consultation team,

I am replying as an individual with no special interest other than as a viewer of online pornography, and as a lawyer.

I have little to add to the analysis of the draft proposals produced by Backlash and the Open Rights Group here: <https://stopageverification.org.uk/bbfc-draft-guidance-age-verification-initial-reaction>

I remain against AV on principle, but on the understanding that the BBFC has to implement it, my main concern would be that the highest standards of privacy must be maintained. No AV provider should be approved unless they can demonstrate that they collect no personally identifiable information, and do not store any information beyond what is absolutely necessary. The Standard on Age Verification is an example of the kind of measures that should be required.

The risks to personal privacy involved in AV technology used for accessing pornographic material are extreme. Protecting privacy may not strictly be in the BBFC's remit, but it appears that no other organisation is taking responsibility for it. Allowing an AV provider to operate without ensuring adequate privacy safeguards are in place risks a legal and reputational disaster, for the provider, the BBFC and the system of age verification itself.

For reasons I hope you understand, I would prefer for my name to be kept confidential.

Sincerely,

**Response to the BBFC's Draft Guidance on Age Verification Arrangements**

Paragraphs 1 – 6	Introduction
Paragraphs 7 – 17	Do you agree with the BBFC's Approach as set out in Chapter 2?
Paragraphs 18 – 22	Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?
Paragraphs 23 – 24	Do you have any comments with regards to Chapter 4?

**Introduction**

1. I don't have any particular qualification to write on this matter. I value my privacy, and I prefer that my response will persuade or not only on the basis of what I have written.
2. The advent of the Internet created an unprecedented freedom for anyone to publish anything to anyone else unmediated by rich and powerful corporations and governments who had hitherto controlled publishing and broadcasting. Big business and governments resented this democratisation. Funded by vast amounts of private money, and enabled by misguided legislation, a handful of big corporations have now effectively annexed the entire free Internet. Now that this monopoly stranglehold on the exchange of information and interpersonal communication by unaccountable corporations has resulted in inevitable abuses and undesirable effects, the British Government is responding by creating further legislation to regulate the monster that legislation has produced. This is madness. What is required is not regulatory schemes like that which the BBFC in its Draft Guidelines is to administer, but repeal or refinement of earlier legislation. Instead of introducing censorship through the Digital Economy Act the British Government would have been wiser to have revised the concept of an 'Information Society Service' to exclude all websites. An ISP is a 'mere conduit', Facebook and Pornhub are not.
3. It was inevitable that the freedom created by the Internet would lead to a lot of discussion, depiction or description of sex. Pornography exists only because of the taboo against the free expression of matters to do with sex, and for no other reason. Sexual taboos existed from the earliest times in many societies. They were integral to the development of patriarchal clan societies. (I use the word, 'patriarchal' in its simple dictionary sense not as a trigger word appropriated by radical feminism.) These taboos were central to maintaining hierarchical tyrannies and theocracies especially in Islamic and Judeo-Christian societies up to the Enlightenment and well beyond. Although they aren't universal. The Trobriand Islanders famously have no similar concepts of sexual morality. On the other for them it is taboo to be observed eating. (Malinowski, 1929. *The sexual life of savages in north-western Melanesia*).

Sex taboos existed to suppress the fundamental purpose of humanity, the urge to procreate, and bend the individual to the service of ruling dynasties. They are responsible for widespread sexual neurosis in modern life and human misery throughout history. They have nothing to do with reason, and have no place in a liberal secular democracy.

4. The explosion of freely available commercially produced pornographic videos on the Internet in the last decade has occurred because of the rise of the so-called “tube sites”. These are Internet sites modeled on the ‘YouTube’ website, but featuring exclusively pornographic videos. The business model of these websites is to steal the intellectual property of others and republish it without charge in order to capture a monopolistic hold on the global audience for such content. Then to collect and exploit data about visitors to these sites to make vast amounts of money through nefarious and deceptive means. By far the biggest organisation responsible for these tube sites is the sinisterly named, Mindgeek.
5. Mindgeek, formerly Manwin is the brainchild of one man, Fabian Thylmann. Fabian is an interesting and intelligent youngish man. He made some money initially by developing software to track referrals from hundreds of thousands of little web pages of clickable links created by individuals who would be rewarded with a percentage of subscription charges if a ‘click-through’ resulted in a sign-up. This was how traffic was generated in the days of the Internet before it was taken over by the corporate behemoths who control global Internet traffic today. Thylmann then started to acquire porn sites that he could make more profitable with his insight into Internet traffic. At some point he conceived a plot to capture the entire distribution of pornography throughout the world. He acquired a company in Montreal called Mansef which owned a fledgling website called Pornhub, and secured backing of hundreds of millions of dollars through Wall Street. He went on a buying spree. He acquired other competing ‘tube sites’. As they eviscerated the successful porn studios mostly based in Los Angeles, by giving away their content for free, he was then able to acquire many of these established companies at a discount because the owners could see there was no future and wanted out. Mansef changed its name to Manwin when Thylmann acquired it. It changed again to Mindgeek when he cashed out of it. Mindgeek is not a porn company. Its website, <https://www.mindgeek.com/>, under the slogan “Industry-leading exclusive technologies driving unparalleled performance” boasts 115 million plus daily visitors, 3 billion plus ad impressions. Its business is the same as Facebook’s. Big Data processing. Exploiting and selling data about you acquired surreptitiously when you visit any site it controls, and anywhere else you go on the Internet whilst its cookies remain in your device’s browser.
6. This essentially criminal conspiracy has been enabled and facilitated by legislation itself. It is laws which have granted immunity to website owners for infringing or actionable content posted by third parties, that has enabled larceny on an unheard of scale. The Electronic Commerce (EC Directive) Regulations 2002 in the UK, EU Directive 2000/31/EC, and The Digital Millennium Copyright Act in the United States and a host of smaller legislation in the UK and elsewhere have facilitated piracy and the exploitation of every user of the Internet.

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

7. The first thing that needs to be said is that the ‘contravention’ described in s.14(1) of the Digital Economy Act 2017 (DEA) is a probably a criminal offence in European Convention terms, notwithstanding it’s characterisation as a regulatory contravention in the Act. As you know, how a State characterises an offence is not fully determinative of how it is categorised in Convention Jurisprudence where such matters are said to be ‘autonomous concepts’. The obvious case in the present context is Engel v Netherlands (<http://hudoc.echr.coe.int/eng?i=001-57478>), but the more recent case of Balsyte-Lideikiene v Lithuania (<http://hudoc.echr.coe.int/eng?i=001-89307>) seems to fairly starkly illustrate the point in a case where the applicant was not on the face of things particularly sympathetic.
8. If this is so, then Part 3 of the DEA is incompatible with the Human Rights Act 1998 (HRA). Beyond the statement of the Secretary of State under s.19(1)(a) of the HRA on the face of the Bill, it is not clear that Parliament gave any scrutiny at all to this fundamental issue during the passage of the Bill through both Houses. I could be corrected if they did, I tried to follow the passage of the Bill and I didn’t notice any discussion of this matter. Its important because if I am right that DEA s.14(1) is a criminal offence then Article 6 ECHR (Art 6) as scheduled to HRA applies in its entirety. It follows that the BBFC Draft Guidance is hopelessly inadequate, and any person sanctioned by the BBFC might, if they were inside the United Kingdom, have recourse to apply for judicial review. Or if they were based outside the United Kingdom then ...it gets really complicated.
9. For the moment I’ll put this fatal objection to the provisions of the Act to one side and consider the Draft Guidance as though it were administering civil regulation.
10. The use of the word “determination” throughout this Draft Guidance is inappropriate. Granted it follows from wording in the DEA, but the BBFC cannot make a determination of anyone’s civil rights or obligations without reference to a court. Art 6 states (in part):

*In the determination of his civil rights and obligations ....., everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law.*

The BBFC is not an independent tribunal. In certain circumstances decisions by an official who is not independent can be compatible with the first paragraph of Art 6. But there has to be ultimate recourse to a Court of “full jurisdiction”. Decisions of local authorities in planning or housing for instance - see: Alconbury [2001] UKHL 23 and Bryan v United Kingdom (1995) 21 EHRR 342. Although there is a fundamental difference between long standing regulatory schemes where the regulator is making decisions affecting persons who are participants in the scheme, and a newly invented regulatory system imposed on anyone. Even persons in foreign jurisdictions. Nonetheless the BBFC might be well advised to limit themselves to making ‘decisions’, rather than claiming to make “determinations”.

11. No doubt the DCMS had this in mind when they provided for Appeals from the BBFC by s.16(5) of the DEA

*The Secretary of State must not make a designation under this section unless satisfied that—*

*(a) arrangements will be maintained by the age-verification regulator for appeals to which subsection (6) applies, and*

*(b) any person hearing an appeal under those arrangements sufficiently independent of the age-verification regulator.*

So I must ask, where are the arrangements for appeals in the Draft Guidance ? I can find a reference to publishing outcomes of appeals at paragraph 2.16. There are further references to publishing outcomes in Chapter 3. And eventually in Annex 4 – ‘The Draft memorandum of understanding between the BBFC and the Information Commissioner’ – at paragraph 16, there is this:

*“...A person on whom an enforcement notice has been served may appeal to the Independent Appeals Panel.”*

But who is the Independent Appeals Panel? Is it a tribunal of full jurisdiction? The Draft Guidance fails to mention anything of substance about this essential support for its own legitimacy. It is to be hoped that there will be no attempt to replicate any version of the former ATVOD/OFCOM quangoroo court.

12. Article 10 ECHR is also clearly engaged by the Act and the Draft Guidance:

- 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
- 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

The Right to Freedom of Expression is a qualified right. So if the BBFC were challenged, it might choose perhaps to rely on one of the exemptions contained in the second paragraph, such as that, “*for the protection of health or morals*”. But then the onus would fall on the BBFC to establish that it is “*necessary in a democratic*” state to do any of those things listed in paragraph 2.9 of the Draft Guidance.

13. The BBFC would be hard put to do so. In recent times the DCMS prompted Ofcom to commission exhaustive research into all the academic studies on the question of the effect of exposure to pornography on minors, not once but twice. Presumably they didn’t like the answer the first time and hoped it might



be different if they asked again. Both times however, the answer came back that on the basis of all the research there is as much or more evidence to show that exposure to pornography is beneficial to the moral development of young people than that it would harm them.

*R18 material: its potential impact on people under 18,*  
<http://stakeholders.ofcom.org.uk/binaries/research/radio-research/r18.pdf>

*Sexually Explicit Material and Video On Demand Services - A Report to DCMS by Ofcom*  
<http://stakeholders.ofcom.org.uk/binaries/internet/explicit-material-vod.pdf>

14. In pushing the Bill through Parliament however the DCMS produced two different reports to justify the legislation. One was an enquiry into how young people access pornography on the Internet, which is a totally different question. And the second was a faux academic study of graphs and anecdote produced by the NSPCC (with Middlesex University and the Children's Commissioner) <https://www.nspcc.org.uk/globalassets/documents/research-reports/mdx-nspcc-occ-pornography-report.pdf> . The NSPCC is the same organisation responsible for the satanic abuse scandal of the 1990s following earlier publications by this organisation with a vested interest in finding harm to children in any unlikely place. I am sorry to be hard on this organization in view of its laudable ostensible purpose. Unfortunately it is discredited. The oddest thing about this report is that there is nothing in the responses reportedly given by the young interviewees to justify the insanely alarmist conclusion reached by the grandly named "Report Commissioners" at the very start of the publication. This will not stand scrutiny as justification in a 'necessity' test.
15. Not only must reliance on a permitted Article 10 exemption be necessary, but it must also be proportionate to the allowed aim. As things stand, since the introduction of mandatory Internet porn filters (aka 'family friendly' filters), no young person can *normally* access the unfiltered Internet without the consent or acquiescence of the adult person responsible for purchasing that Internet access, usually the young person's parent. Is it proportionate therefore to require every adult citizen to register their age and identity with some dodgy verification website in order to purport to protect those children whose parents have *exceptionally* allowed their children to go on-line without the filters? Surely it would be much more proportionate to the aim of the DEA to have made regulations requiring parents, and adults with responsibility for under 18s, to ensure that the porn filters were in place for the minors in their charge, for instance. That would have involved a much smaller number of the population. Moreover the only persons whose rights would have been interfered with are the same under 18 year olds who are to be denied the right of free expression anyway. And it would be far more effective since there is already a block in place on all the websites that the little darlings are to be 'protected' from seeing.

16. I have no doubt that the BBFC are sincere in their desire to administer the provisions of the Act proportionately, as they repeated say. Unfortunately they've been handed a poisoned chalice. They cannot administer 'Age Verification' proportionately because the provisions of the Act are manifestly disproportionate. For that reason they are also, at least arguably, unlawful ab initio.
17. On the positive side, paragraph 2.6 of the Draft Guidance appears to describe an approach which gives website publishers the opportunity to make changes before draconian measures are resorted to. The BBFC appears to want to adopt a softer approach to censorship than say the Turkish or Chinese model. That at least is guardedly welcome.

**Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?**

18. Much of what has been said about Chapter 2 is just as applicable to Chapter 3 of the Draft Guidelines.
19. Paragraph 3.4 shows that the BBFC is following the guidance issued by the DCMS in not giving approval to any individual AV scheme. It's to be left to consumer choice. Passing quickly over the little gem of illogicality that is, "...the use of mechanisms that confirm age but not identity", I will point out that effect of this decision is to appoint Mindgeek as the British Government's official 'Age Verifier'. No other AV system has any chance of competing with Mindgeek's Age ID system. This is because Mindgeek already control over 80% of all traffic to adult sites from the UK. All of that traffic is going to have to use Age ID. Further Age ID is being offered for free to small independent sites who simply could not afford to pay anyway. That's a bit more traffic for Mindgeek to process big data on. And that leaves only the minor competition to Mindgeek's empire consisting of the improbably named xhamster and xvideos, both 'tube sites'. Mindgeek won't be offering them free age verification. Probably they'll be looking to marginalise or acquire them.
20. The opportunity offered by AV to Mindgeek is the chance to put their Age ID cookie in the device browsers of 25 million citizens of the UK and to know that every time that relates to a single identifiable individual. Even if a user clears their browser cookies, the very next time they visit any adult site the same unique cookie will be back continuing tracking from exactly the same place it left off before.
21. There are other AV systems being developed with completely opaque business models. Suffice it to say that none of these, no doubt otherwise perfectly respectable, businessmen are doing this for any reason but personal profit. However I have to say that I don't give much for their chances of survival against Mindgeek's Age ID system.
22. I might also mention s.14(5) of the DEA:

*Regulations 17 to 20 and 22 of the Electronic Commerce (EC Directive) Regulations 2002 (S.I. 2002/2013) apply in relation to this Part, despite regulation 3(2) of those Regulations.*

By virtue of this the 'tube' sites, will be able to claim status as "Information Society Services". Thus they won't be regulated under Chapter 2, but under Chapter 3. If the BBFC sends take down notices from now until the next Millennium they will be no further forward. They might send a notice in the morning, which will probably be complied with, but the same video will be posted again in the afternoon with a different title from a different user account.

If on the other hand Mindgeek et al accept that they are publishers and not information society services and are liable to be regulated under Chapter 2, then I look forward to years worth of pent up copyright infringement cases being brought to the UK courts.

#### **Do you have any comments with regards to Chapter 4?**

23. Let's assume that Age Verification companies are all honest, diligent, totally competent and keep confidential data in impregnable vaults that will never be hacked. Will that ensure that no one is going to be tracked on the basis that they have verified their identity ? Of course not. Everyone who uses the Internet is being tracked all the time. You aren't being tracked by your name and address and date of birth although such information might well be in your file somewhere. Everyone is tracked by a user identification number. You are identified by cookies and "browser finger printing" and other techniques. No one is (hopefully) scrutinising your every move exactly. But every move you make is being collected and sorted and aggregated until it finds it's way into unique folders linked to you as an individual. The data is anonymous, but it is used to target you personally. And if it came to it, it is trivial to de-anonymise such data.
24. Apart from the legitimate Age Verification enterprises vying for a piece of the action. There are 50 zillion (approx.) businesses located in such places as Donetsk, St Petersburg, Guangzhou, Beijing, Islamabad, Bangalore, Freetown, Lagos, and Miami who are gearing up to provide their own AV systems. I think they will let you access any site you like if you fill out a form giving the long card number, the expiry date, the CV number, and your postcode. What's to stop them? If the ICO and the BBFC are going to attempt to police the flood of fraud that they have invited, what time will they have to do anything else? And if they aren't going to police it, why not?

## Response to BBFC consultation on Age Verification

I have many concerns with the wording and intention both of the Digital Economies Act and the BBFC proposals for how they should be implemented. I have attempted to cover the major concerns here in brief.

### Privacy

The privacy protections in the act and the consultation appear wholly inadequate. We are speaking here of creating a nation-scale database of people's entirely **legal**, but also entirely **private**, viewing habits. Suicides in the aftermath of the Ashley Madison hack <http://www.bbc.co.uk/news/technology-34044506> and the concerns about subversion of electoral processes by data collected by Facebook and Cambridge Analytica should surely serve as stark warnings that this aspect of the regulations must be looked at again. This is especially true given that the business model of some of the providers implementing large-scale age verification solutions is based on advertising, and therefore relies heavily on correlating and tracking visitors as they navigate online to target those adverts. I believe most people have a reasonable expectation of privacy when they visit a legal adult entertainment website. How is that expectation to be met if a secondary service provider (the age verifier) is correlating their porn viewing habits with their other online activity in order to cover their costs and make a profit?

### Right To Appeal

Little mention is made in the proposals of rights of appeal. This procedure needs to be laid out in detail, with an independent appeals authority, and a light-weight system for quick response to prevent unwarranted censorship and the closure of businesses pending appeal.

Previous attempts at internet regulation in the UK included ATVOD deciding that a one-man-band operation was somehow operating a television on demand service in competition with Sky and the BBC. The appeals procedure was unfair in that the service was required to be taken down pending appeal, ensuring complete loss of customers so that even once a successful appeal was made a year later, the business in question had already collapsed. (The ATVOD procedure was so flawed that the organisation was wound up).

Given that the new regulations treat the digital equivalent of the local corner store on the same footing as Pornhub and Playboy, what will the appeals procedure be? What consideration will be given to allowing the continued existence of the disputed website pending appeal? What guarantees will be made on the independence of the appeals panel and the speed of the process?

### The Scale of the Operation

There are 1.8 billion websites in the world (<http://www.internetlivestats.com/total-number-of-websites/>) of which 200 million are claimed to be currently active. In principle, each of these must be at least visited by BBFC inspectors to ensure that they are either non-adult in nature, non-commercial (presumably including any advertising), or if they do contain some commercial adult material, hold them behind a compliant age verification wall.

No serious consideration seems to have been given as to how a small organisation like the BBFC will be able to apply these regulations in anything like an even-handed manner given the scale of what is proposed.

Will automated or semi-automated searches be used to locate potentially infringing websites? This immediately falls foul of the Scunthorpe Problem (named after automated blocking by AOL's profanity filter prevented people from sCUNThorpe from making accounts on AOL, [https://en.wikipedia.org/wiki/Scunthorpe\\_problem](https://en.wikipedia.org/wiki/Scunthorpe_problem) ).

The BBFC propose to start with sites which are “most frequently-visited, especially by children”, which seems at face value to be sensible. Unfortunately, on reflection, both halves of the sentence are problematic. It is hard to establish traffic levels robustly, and how on earth are the BBFC proposing to identify sites visited by children in an ethical manner? And **all** websites are available worldwide, unless blocked by national level firewalls.

All websites serve British customers and there is no reliable way of a small business in (say) Nevada choosing to disallow visitors from Britain. They can decline to admit customers into paid areas on the basis of credit card address details, but that's never been any sort of problem anyway. At worst they may need to disallow the tiny fraction of payments made by debit card rather than credit card. This may be an issue to sites in Germany where credit cards are less used, but in the English-speaking world, credit card payment is almost universal and age verification to access the paywalled area is already the de facto standard (and has been for two decades).

The problem is trailers and the free area. There is no way for the Nevada producer to show legal-in-the-USA preview material to US customers but require UK customers to age verify first. Indeed, age verification systems required for UK compliance may be illegal in other jurisdictions given the lack of privacy protections. How can a small business obey mutually contradictory regulations coming from different countries?

Geotagging methods are haphazard and unreliable at best, and are also immediately defeated by any form of redirection ranging from simply telnetting to a machine in Spain and popping up a window back on your local machine, through virtual private networks (often used for legitimate purposes such as logging into commercially-sensitive corporate intranets while an employee is off site) to freely-available tools like TOR.

How is a small business operator in Nevada meant to comply with local and UK regulations if they cannot adjudicate the country of origin of an incoming HTML request? Doing so is beyond the capabilities of Netflix and the BBC, so what hope does a Swedish webmaster or a part-time performer in Amsterdam have of complying?

And why should one small business in Nevada have to endure the commercial burden of obeying UK regulations and paying to age-verify his potential customers so they can view his previews when his neighbour, whose site the BBFC have decided does not qualify as “frequently visited” and therefore do not propose to inspect, does not? Both will very likely be doing their best to comply with their local regulations already, but one is suddenly landed with a disproportionate foreign regulatory burden and the other is not.

They cannot even choose to age-verify only potential customers coming from the UK, since there is no robust method of geo-tagging by IP address that is not trivially defeated by redirection.

What in fact is likely to happen is what happened with ATVOD- site operators will keep their heads down in order to try to avoid notice, the regulator will pick on a small fraction of

operators essentially at random, and impose regulatory burdens on them which are not suffered by their competitors, putting the unlucky few at a serious competitive disadvantage, likely putting them out of business pending appeal.

The largest players who can afford to handle the requirements of verification on an industrial scale will rub their hands together in glee at the hope of putting their competitors- the small, diverse, boutique adult producers we'd presumably like to encourage- out of business.

The BBFC document simply fails to appreciate that the scale of the problem- 200,000,000+ active websites in the world- is out of all proportion to anything the organisation has ever dealt with before.

For example, in 2016 the BBFC classified 1075 cinema films, 8201 videos and 74 music videos. That's of order of 30 classifications a day. Websites are currently being created at the rate of 1 per second- 86,400 a day.

To enforce the regulations in an even-handed manner, every single one of these really ought to be inspected. And revisited regularly to prevent change of use, since unlike cinema films which are static objects (a film is not re-edited on a daily basis) websites can and do change dynamically all the time. Otherwise unscrupulous operators can just register "[www.MySewingWebsite.com](http://www.MySewingWebsite.com)" and use it to distribute porn- and if the regulators do chance upon it, will just switch domains to "[www.OurHillwalkingWebsite.com](http://www.OurHillwalkingWebsite.com)".

Estimates vary, but as many as 4% of websites might include adult entertainment, and therefore need more than a cursory inspection.

How do the BBFC proposed to organise the inspection of websites in a consistent and fair manner? At the very least, thresholds should be placed to exclude micro-businesses from unwarranted burden on the basis of hypothetical risk. It's not clear what a good and robust set of metrics for those standards would be, but excluding businesses below a certain number of employees, a certain turnover threshold, or some metric based on unique visitors per day would be a start.

We need something more rigorous and even-handed than "most frequently-visited" as a criterion and the BBFC needs to set this out publicly and transparently.

### **Metrics And Proportionality**

The act and the BBFC document appear to treat it as a given that viewing human nudity and human procreation when under the age of 18 is inherently harmful. Studies in this area are limited, with small sample sizes, questionable methodologies and contradictory results.

What steps are being taken to survey the extent of the problem in an impartial and rigorous way? We need data on the current extent of the problem, then we need metrics to quantify the reduction in harm as the regulations are rolled out, in order that we can evaluate their effectiveness. What metrics are proposed?

Since the UK's proposed solution is the imposition of ISP-level censorship, financial censorship, and potentially large fines, hadn't we better ensure that our approach is actually working, and that the harm caused to freedom of speech and the chilling effect of

self-censorship on already marginalised sexual minorities like the LGBT community and consensual BDSM practitioners sharing best practices online is actually accompanied by a positive effect on the problem the regulations are seeking to tackle?

Indeed, what steps are being taken to monitor the negative consequences of the regulations on freedom of expression and the provision of educational material by sexual minorities? Educational material is often made widely available on sites which also generate their income by sales of adult entertainment. “How to tie safely” videos on bondage websites, for example, and safe sex advice on gay sites. What attempt has been made to assess the chilling effect of regulation on these sources of information? Will they need to be placed behind age verification walls? A highly retrograde step if so, surely?

In short- what metrics are to be used to assess success, and to assess predicted negative consequences? How will it be determined whether these regulations are disproportionate or not?

### **Accountability**

The BBFC annual report mentions that the organisation regularly conducts public consultations to ensure its guidelines stay up to date with public expectations. However, recent legal cases such as that of Michael Peacock ([https://en.wikipedia.org/wiki/R\\_v\\_Peacock](https://en.wikipedia.org/wiki/R_v_Peacock)) show that at least as far as obscenity goes, the public’s view is significantly different from that of the authorities.

Given that the BBFC is now to be given sweeping powers to block free speech in the UK on the basis of subjective determinations of what constitutes 18-rated material or 18-R material, there needs to be a much more wide-ranging, active, ongoing and **transparent** procedure to keep these regulations up to date. What is the BBFC proposing to do in this area?

Remember that the scale of the operation is MANY orders of magnitude greater than anything the BBFC has previous tackled. The potential impact on free speech is therefore also much more severe, and it seems doubtful that current consultation structures will be adequate for the scale of the new endeavor.

If the BBFC is going to become the arbiter of free speech in the UK, are they to come within the remit of laws such as those governing freedom of information requests?

### **Specificity of Rules**

In the past, the BBFC has issued broad guidelines on what is likely to be considered at each level of classification, but the final classification of any work has always been made after viewing by human beings at the BBFC.

Detailed guidelines as to precisely what can and cannot be shown have never been issued.

Unless the BBFC is to recruit tens of thousands of new staff, they are going to be unable to inspect any meaningful fraction of adult websites. Given the typical scale of releases in the adult industry (many producers release a new product every day) it will not be possible for the BBFC to act in any advisory role in a meaningful way either.

Producers are left to guess what is and isn’t acceptable for publication on any given distribution channel. The most critical point where this matters is in knowing what material

is acceptable to distribute outside the age verification wall, and what must be restricted to within the wall.

For example, here are two still frames, drawn from trailers whose contents are rather similar.





Given a copy of the BBFC guidelines, can one determine if it is acceptable for the producer of an adult entertainment product to show the above stills on their free area or for publicity on public platforms such as Twitter? Or for the trailers from whence they come?

One cannot.

I chose these two examples with care to illustrate a problem caused by the lack of specificity in guidelines. Both show an attractive actress being tied up, against the will of the character they are playing (but of course consensually and professionally in a safe working environment in reality).

The top still is from an American bondage producer, and would presumably be rated 18, or possibly 18R, or possibly characterised as extreme porn because the actress has all four limbs bound and is gagged... even though no actual sexual activity takes place, and as far as I know no nudity is featured either (I haven't purchased the full film, just watched the trailer).

The bottom still is from the movie RED, rated 12 by the BBFC.

Which rating would apply to the trailer for the American bondage film? Extreme porn (illegal and banned), 18, 18R or rated 12? Would publishing it be permissible for advertising, and for publication on a website in a free preview area outside the age verification area?

If not, why not, since the above clip for RED is freely available on YouTube, and in any case was drawn from a movie which was only rated 12?

More critically, how could any producer possibly follow the rules and only publish acceptable material on their free preview area and publicity, if the rules are not detailed enough that one cannot make this determination given the above two images and a copy of the rules?

Given that a producer must make this decision for EACH new release, on a daily basis, how can they possibly attempt to ensure that their adverts, trailers and free preview areas are compliant with the laws without extremely detailed, unambiguous guidelines?

It is not a solution to require that all advertising or previews or trailers be behind age verification walls. The cost of age-verifying a viewer will either be non-zero (for a reputable age verification company making its money from providing a service) or zero, but with a stiff cost to the end consumer in terms of loss of privacy and risk of exposure of intimate details.

The average ratio of customers to viewers in any industry is high. Typical sales of fetish videos are in the tens to hundreds of units; typical followings on Twitter are in the tens of thousands. If it costs £1 to verify the age of each of 10,000 viewers to sell to 100 customers at £10 a unit, all small producers will be put out of business- the cost of age verification will rapidly exceed their turnover, by a factor of 10. Or they must turn their potential customers over to the mercy of advertising-based age verification operators, a dubious and unappealing proposition at best.

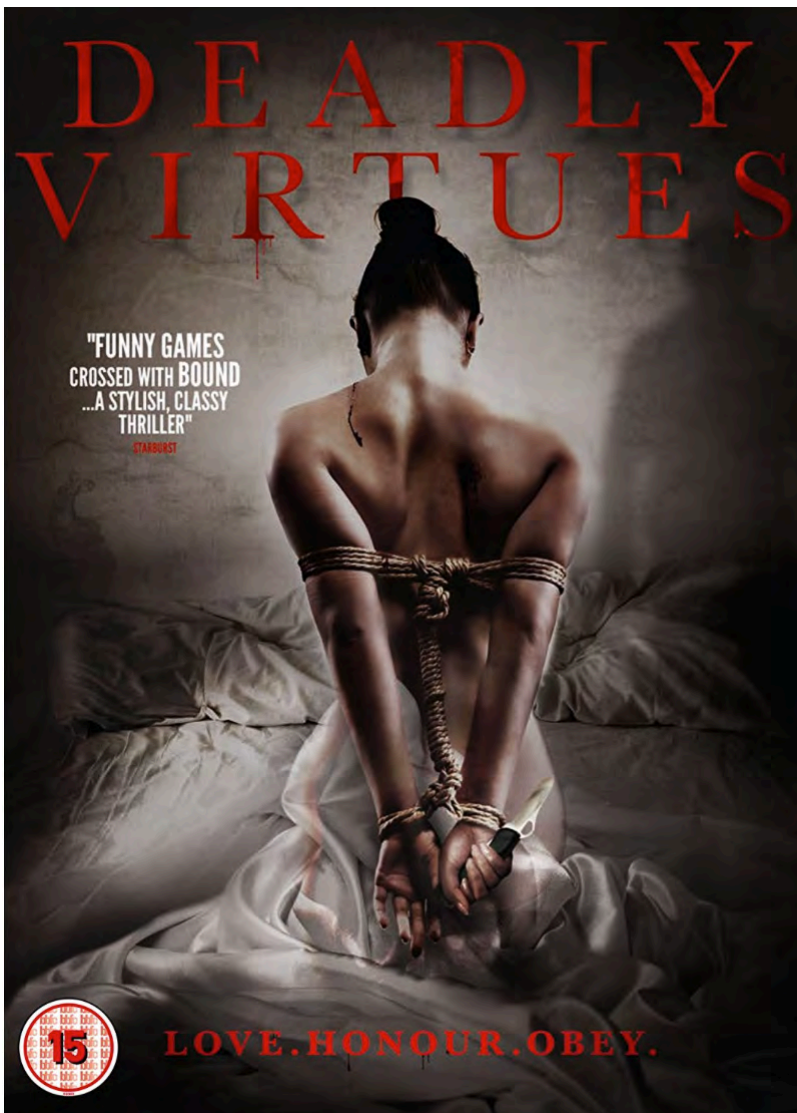


Society acknowledges this in mainstream films- we allow 12-rated trailers for 18-rated films, and sell 18-rated films in supermarkets with suggestive but allowable photographs on the cover.

To take a second example, the photograph above would be considered pretty extreme on a lot of BDSM websites- especially the knife held in the girl's hand, and what looks like a trail of blood on her shoulder.

The implication of violence, the blood, the (non-revealing, but clear) nudity... all would suggest an extreme porn image.

The producer of such an image might certainly consider keeping it behind an age verification wall, rather than putting it on the free area as a preview. And they might even self-censor, being unable to be sure whether or not it counts as extreme porn.



Actually, this image was on display at my local Tesco... at knee height.

It's the cover for a 15-rated movie, and was visible to passing toddlers.

As far as I know, there was no harm caused to anyone by its publication.

So if we are happy with this on the shelves at Tesco (which we should be), surely we should be happy with images like this on social media and as posters and previews for adult sites?

I defy anyone to classify the image according to BBFC guidelines and tell me whether or not it would be acceptable outside the age verification wall on an adult website, with reasoning that an impartial observer would be able to follow and verify.

## **The Difference Between Producers And Tube Sites**

Finally, I would just like to address the implicit idea that producers of adult entertainment are in any way targeting their products towards minors, as this seems to be an area of great misunderstanding.

Adult producers are also parents, carers, citizens, tax-payers and consumers. They have moral standards every bit as high - and occasionally of course as low- as everyone else's. From a moral point of view, few want minors to be consuming their wares, any more than the producers of "Deadly Virtues" want toddlers to watch their horror film. But, like the producers of "Deadly Virtues", they must showcase their wares in their shop windows in order to generate sales and make a living. "Deadly Virtues" did so in Tesco. Producers do so online on their websites in free areas and with trailers.

All reasonable producers would be willing to abide by sensible, consistent restrictions as to what they can display in their shop windows. They'd even do their best to do so country-by-country, despite the impossibility of verifying the geographical location of an incoming HTML request. (No such guidelines exist, certainly not for the UK). They keep the full versions of their products behind paywalls because that is how they make their money.

Payment for access to adult entertainment is overwhelmingly made by credit card, not debit card. Consumers are mostly savvy enough to know that all online purchases should be made via credit card, because of the greater consumer protection they provide. Existing paywalls are probably not perfect, but I would suggest that they already exclude almost all minors and could be tightened up if studies were to reveal that payment by minors using debit cards was actually a significant factor.

But note that minors would make extremely poor customers for adult producers. They have little disposable income, any payment methods they have are either illicit (stealing Dad's credit card) or of limited use online (debit cards), and they likely don't have the privacy at home to be able to consume adult entertainment. And since the vast majority of producers are reasonable human beings, the idea of kids watching their products is anathema.

The idea that producers are actually TRYING to sell to minors is far-fetched from both a moral and financial point of view. No producer has the slightest interest in minors viewing their material. They accept that some children may happen to view their preview material, as is the case for the extreme porn BDSM and blood image on the cover of Deadly Virtues and would be willing to work within a reasonable framework of restrictions on trailers, were any to be produced.

So how are kids going to view the full versions of these producers' adult entertainment products? What exactly is the problem here? Where does all this free porn come from?

- 1) By stealing Dad's credit card. Not likely to last long, and surely a parental issue not a governmental one. Age verification is of no help here, since if a card can be stolen, so can age verification credentials.
- 2) By getting access to material already legitimately purchased by an adult in the household. Again, a purely parental matter, and one which age verification online does not address.
- 3) By using their own debit card on the small number of sites which accept them. Possible, but are there any studies which indicate that this happens in significant numbers? Age verification would help here, but it is using a sledgehammer to crack a nut.

4) By viewing the material stolen and uploaded to a "Tube" site where it is made available for free to anyone.

This is the elephant in the room. Producers have been fighting an ongoing war against the tube sites for a decade or more, trying to stop copyright violation and piracy. Pirates post copies of a producer's material to tube sites without authorisation, giving away free what was previously only available behind a paywall.

THAT is how children access porn. All other channels are insignificant.

Perhaps if existing laws regarding copyright violation were used to prosecute those who operate and distribute stolen material from legitimate producers, tube sites would not be able to continue to steal traffic from paywalled sites by giving away their copyrighted material for free.

These sites have grown large on the backs of pirated material, so large that some of them are now in fact also legitimate producers. But their business model still revolves around advertising, selling visitor's eyeballs to advertisers.

It is they who have an incentive to display material to minors, because more visitors means more ad clicks which means more money. Unlike the original producer, their business model depends only on attracting more visits, not on convincing someone to pay for an adult entertainment product behind a paywall.

It is they who have an incentive to steal material, sucking in more visitors who previously would have had no option but to go behind the legitimate original producer's pay wall to view the products. They put cosmetic "complain and we'll take it down" measures in place so they can claim to be resisting piracy, but all adult entertainment producers know this is a sham. Videos get taken down on a complaint but are back up within hours. Many original producers are forced to hire specialist firms to try to combat the flood of piracy, and are losing the battle.

These sites are parasites on the legitimate industry of producing legal adult entertainment and it is they, not the original producers, who have created whatever problems might result from the free availability of adult entertainment online.

If one were to level the playing field by prosecuting the copyright infringement, removing all the stolen material from tube sites so it once again becomes available only behind existing pay walls, the problem of free porn would largely go away.

If one is serious about tackling minors viewing porn, prosecuting the pirates who make copyrighted material illegally available online would be a good start.

And being wary of allowing the most egregious example of a Tube site company built on piracy, MindGeek, to perform age verification and collect data on the private and intimate habits of a third of the UK population would probably be a wise second step.

## **CONCLUSION**

If we are going to insist on these ill-considered and draconian censorship measures to combat a problem whose existence is questionable, the least we can do is to come up with some reasonable and consistent guidelines for producers of legal adult entertainment to follow in order to know that they are within the law.

Furthermore, we must put in place swift and fair appeals procedures (to avoid putting legitimate small businesses out of business whilst enduring bureaucratic delays). We must insist upon transparent and wide-ranging public consultations on the standards, and produce rigorous, unambiguous guidelines for what is acceptable outside age verification walls and what has to be placed inside.

We must ensure the privacy of the estimated 20 million UK citizens who are likely to avail themselves of age verification systems. We must institute proper scientific studies into the harm caused to children by viewing different sorts of adult entertainment, and studies to assess any possible negative impacts on free speech and the chilling effects of the regulations on minority communities.

None of these concerns are adequately addressed by the recent BBFC proposals.

## Guidance on Age-Verification Arrangements

- *Do you agree with the BBFC's Approach as set out in Chapter 2?*

No.

I have fundamental concerns about privacy and utility. I also have concerns about scope.

I do not see any meaningful way in which the 'commercial basis' definition does not include any website or internet service. The phrase "overwhelming majority" invites questions about measurement and use of services with multiple uses and queries about times at which entities were measured.

Enforcement and verification seem to be being imposed upon ISPs and other service providers with opportunities for breach of privacy, consolidation of risk, and though the intent is laudable these proposals create risks for consenting adults accessing legal material that did not previously exist, without any meaningful or obvious safeguards for them.

The phrase "Although not a requirement" is concerning, not least with reference to "*adopt good practice in the design and implementation of their solutions*" and "*offer a choice of age-verification solutions*". Minimal requirements risks minimal compliance and creates new risks.

I am also concerned about scope – the BBFC already seem pressed to cope with physical media, and the panoply of platforms for pornography to be provided is likely to stretch any capacity made available. Overstretched services make mistakes, and with no explicit consideration of user privacy it seems even more likely that there will be compromises that affect the rights of consenting adults making use of legal services.

*Do you agree with the BBFC's Age-verification Standards set out in Chapter 3?*

No.

In particular the "*use of age verification data that cannot be reasonably known by another person, without theft of data or identification documents or readily predicted by another person*". Passwords can be changed, but people have a finite number of such 'secrets'. The opportunities for violations of privacy and attendant risks are significant and alarming.

- *Do you have any comments with regards to Chapter 4?*

There are insufficient reassurances within these proposals that privacy will be protected.

The Open Rights Group had the following to say (italicised)

*Age Verification tools may create a sensitive record of the public's porn watching habits. The consequences of a breach would be catastrophic for millions of UK citizens. Privacy must be a priority.*

The presence of a login for an Age Verification tool is in and of itself potentially something private. The concern is also that material may be classed as pornography, or spaces where LGBTQIA content is found may be classed as pornographic, not least because of some of the seeming broad categorisations. The proposals on privacy do not go far enough.

*Between the BBFC and the ICO, there is a regulatory gap where nobody is assigned to oversee privacy. This is inviting disaster.*

*In light of the Cambridge Analytica scandal, a failure to take privacy concerns seriously is unconscionable. Private companies are clearly capable of disregarding user privacy, so they require strict privacy guidelines.*

Prior research has shown that it is sometimes trivial to deanonymise browsing or other content. If the intent is to dissuade consenting adults from making use of legal services this is a convoluted way to do it. There is frequent reference made to content that is already illegal, these proposals don't address those issues directly.

*It is in the BBFC's interest to make sure AV tools protect the public's privacy. If a breach occurs, people will see both the BBFC and the Government as responsible.*

I have retained their text in its entirety because I agree with it.

The BBFC will refer any comments regarding Chapter 4 to the Information Commissioner's Office for further consideration.

### **Draft Guidance on Ancillary Service Providers**

- Do you agree with the BBFC's Approach as set out in Chapter 2?
- Do you agree with the classes of Ancillary Service Provider set out in Chapter 3?

No.

Ancillary Service Provider is so broad and the "no direct commercial relationship" element so far reaching in an age of shared services, cloud hosting, and so forth that this effectively forces the BBFC into the point where they come close to being a regulator for the entire Internet as it connects to the UK. I do not think any organisation is capable of achieving that task fairly, evenly, or successfully, and certainly not as proposed here.



## ANONYMOUS #16

Subject: Protection against abuse of age verification data

Dear consultation team,

I am alarmed at the legislation apparently proposed around mandatory age verification.

I consider it vital that we have a credible and cast-iron guarantee that any data submitted will never be used for any purpose other than strict age verification and will never be passed to any third parties for any reason at all. To be credible, there needs to be provision to enforce that guarantee and the public need to have sight of it being enforced!

It also needs to be very clear exactly what kind of content is covered by this provision. Otherwise, non-pornographic material which may contain images or text taken out of context, might be caught up in the restriction. Examples - fine art nudes, medical texts, discussion venues where topics may sometimes include 'sensitive' issues.

Without that guarantee, I will not be taking part in any age verification. But while I have no interest in pornography, I do not want to be denied access to discussion and information sites because of legislation that is ambiguous or interpreted too loosely, and which do not truly need this protection!

I would like to keep my name to remain confidential please. Do what you like with my response!

Sincerely,

## ANONYMOUS #17

Subject: Age Verification

Dear consultation team,

Making people verify their age when watching porn will not help stop people under 18 watching such material. In fact like all prudent measures is will only push this activity to the darker areas on the internet. Not only will kids under 18 just watch porn on unregulated sites but also, so will adults who want to keep their habits a secret. These such sites which are unregulated could contain some material that is illegal (without them knowing) etc. Also regulated ethical sites will go out of business. So basically all you are doing is pushing kids and some adults to watch unregulated sometimes illegal porn. How is that a step forward. The only reason I can see you are doing this is to collect further data on what consenting responsible adults are doing with their lives. If Facebook and do then I'm sure government sites will do the same and sell are data to the highest bidder. Some people may be fooled, but i am not, and it's just a further step to big brothers watching you.

I want my name to remain confidential.

Sincerely,

## ANONYMOUS #18

Subject:

Dear consultation team,

I am unlikely to sign up to any age verification to be able to access porn sites, so age verification per se does not bother me.

However, I am very concerned that any age verification technology is being left to private companies to develop and provide. What motivation would any such company have re: safeguarding any data about users that is collected? On the contrary, they would have an incentive to collect and sell information about user viewing habits, especially if this involves pornography. The recent revelations about Facebook, and the Cambridge Analytica scandal in particular, is a reminder that private companies are not reliable guardians of personal data. There is no excuse why the Government should not be prioritising privacy for AV technology.

In any case, any person with much technical savvy will find a way round any need for authorisation, although I fear that some of the means for this may be banned, as some now are in Russia.

I am happy to be counted, and hope that my views are taken into account, but I want my name to remain confidential please.