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 laywer specialising in obscenity law, who obtained Not Guilty verdicts in two landmark obscenity trials in 2012, R v Walsh and R v 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[1] in November 2015, and Ofcom's own overview of the potential impact of R18 material[2] 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.[3] 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".[4]

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

---

1https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/500701/Report_of_DCMS_Expert_Panel__Autumn_2015__FINAL_.pdf
2http://stakeholders.ofcom.org.uk/binaries/research/radio-research/r18.pdf
3https://bishtraining.com/does-porn-harm-young-people
4http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf

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 of websites each year, especially since he only anticipates taking on "one or two extra people"[5]. 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[6]. 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 "sadomasochistic 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

---

5 https://hansard.parliament.uk/Commons/2016-10-11/debates/5da6f418-b687-41aa-9418-449cf52d598e/DigitalEconomyBill(SecondSitting)

6https://www.cps.gov.uk/legal-guidance/obscene-publications

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."[7]

7http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

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.

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".[8] 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

8http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

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 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 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 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.[9] In 2012 a YouPorn data breach revealed the email addresses, usernames and passwords of a million porn viewers.[10] The same year hackers romped through Digital Playground, leaking 73,000 user details and numbers,

9https://www.theinquirer.net/inquirer/news/3018894/pornhub-hack-hackers-hijacked-ads-with-malware-in-year-long-attack

10https://www.pcworld.com/article/250532/youporn_data_breach_exposes_1_million_user_logins.html

expiry dates and security codes for 40,000 credit cards;[11] "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.[12] 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.

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[13] 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

11https://www.theregister.co.uk/2012/03/12/smut_site_hacked/
12https://www.cnbc.com/2016/09/07/alleged-data-breach-exposes-almost-800k-brazzers-porn-site-users.html
13https://digitalguardian.com/blog/timeline-ashley-madison-hack

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.

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.[14] 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.

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.

14https://medium.com/@alecmuffett/a-sequence-of-spankingly-bad-ideas-483cecf4ba89

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.

Regulatory oversight

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 responsibly 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.