AGE VERIFICATION - RISKS & RECOMMENDATIONS

Introduction

Age verification for pornographic content, as required by the Digital Economy Act 2017 (DEA), represents a grave threat to users' online privacy. The age verification requirement creates substantial new risks for users, and these risks cannot be adequately curtailed by data protection law alone.

The risks of age verification

Age verification services must at some stage directly identify users in order to accurately verify age. Users will be viewing pornographic content, and the data about what specific content a user views is highly personal and sensitive. This has potentially disastrous consequences for individuals and families if the data is lost, leaked, or stolen.

Until now, most porn viewing would have been anonymous to the extent that no user ID is required in most free services of that kind. Age verification will fundamentally change the nature of online pornography, enabling the detailed tracking of all habits - what people watch, when, where and for how long - and linking these to a unique identifier, creating a new and unique privacy risk.

Once this data is in the public domain, there is no going back. Highly sensitive data about a person's private sexuality cannot simply be revoked in the way that leaked credit cards or billing data can.

Following a hack affecting Ashley Madison – a dating website for extramarital affairs – a number of the site's users took their own lives as a result of the public exposure of their sexual activities and interests (1). Suicide cannot be rectified or compensated for. It is imperative that the DCMS consider the potential consequences of age verification data, as the blame for future data breaches and leaks will lie squarely at the Government's door.

Members of the LGBTQ+ community may be forced to deal with the fact that they are 'outed' by the leaking of such data. This could have devastating consequences, particularly those who are dependent on family members or who are members of religious faiths which are less accepting of LGBTQ+ identities.

(1) http://www.bbc.co.uk/news/technology-34044506

Impacts on professional reputations could also be severe; for instance teachers may find it impossible to maintain discipline if perfectly legal sexual preferences become the object of school gossip.

Data protection law does not suffice

GDPR offers a number of positive improvements for data protection, but does not go far enough for data protection law to be considered sufficient to protect information that is as potentially revealing as a person's pornographic viewing history.

It is possible for a porn company to legitimately re-use data – for example with consent, claiming anonymisation, or through some other legitimate interests. Users may be required to agree to Terms of Service documents they have not fully comprehended, or may be incentivised to consent to further processing of their data with the promise of free content or additional features.

Data breaches must be reported to the ICO, but only in some cases to the data subjects involved. The fines from regulators and courts may be substantial, but these do not provide financial compensation to individuals affected, who must seek redress separately. It seems unlikely that many users of adult websites will choose to further expose themselves by suing.

Further risks relate to the detail of tool design. For instance account log-ins could be (inadvertently) accessed, leading to sexual histories being shared, dependent on tool design. Tool design cannot be regulated without new legal powers.

The need for extra protections

The remedies found in GDPR are focused on deterrence through the use of fines, but the evidence from sectors handling sensitive data is that mere deterrents are not sufficient. Where risks are high, it is appropriate to mandate a tighter approach to privacy.

Payment card information, for example, is protected by the contractually-enforced Payment Card Industry Data Security Standard (PCI DSS) (2). Similarly, European Union legislation ensures the confidentiality of communications data through specific ePrivacy laws, which contains a number of enforceable provisions for telecoms providers.

(2) https://www.pcisecuritystandards.org/

We need specific protections of this type for the highly sensitive data that will be created by these proposals.

Potential Approaches

GDPR Codes of Conduct

One potential system that could be taken advantage of to increase the security and safety of age verification data would be to enforce a requirement for all age verification providers to sign up to an "approved code of conduct" uinde GDPR provisions (3)

As such codes of conduct are voluntary, Parliament would need to take action to amend the Digital Economy Act to grant the BBFC the power to issue binding requirements for age verification providers that specifically take user privacy into account. The BBFC could then indicate in their guidance that they will judge an operator to be compliant only if they signed up to a specific GDPR code of conduct for age verification.

Contractually-enforced standards

One prime example of a contractually-enforced standard for data protection is the previously mentioned PCI DSS standard maintained by the Payment Card Industry Security Standards Council – a coalition of payment card brands which includes members such as MasterCard, Visa, and American Express. This builds a mandatory baseline level of security that merchants must adhere to when storing, processing, or transmitting card data.

In this model, a statutory instrument would require the new scheme to be used, but would let the scheme's operators provide the detailed framework and enforcement mechanisms, which would be provided for by contract, as with PCI DSS. A new industry body would be needed to govern and enforce the standard.

Sectoral legislation

Statutory restrictions on age verification providers could be used to outline rules that strictly enforce the user privacy protection. These could create a statutory duty for age verification providers to prioritise privacy, and could enforce penalties in the event that such a duty is breached.

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

AGE VERIFICATION - RISKS & RECOMMENDATIONS

Generally, sectoral legislation tends to be less detailed than contracts or GDPR codes of practice, because it is intended to last a long time and apply to many situations. More specific guidance would need to be issued more flexibly by the BBFC and evolved where necessary.

Recommendations

Ensure regulatory guidance is binding and enforceable

Irrespective of the method chosen to safeguard the privacy of users of age verification systems, it is of critical importance that the guidance given to providers for doing so is mandatory and enforceable.

Voluntary guidance is not sufficient to protect users, and this is especially true where the motives of some age verification providers potentially lie in direct conflict with a desire to protect user privacy (4).

Ensure that a clear enforcement mechanism exists

As well as ensuring that user privacy protections are mandatory, it is essential that a clear and transparent system of enforcement exists for noncompliance by age verification providers.

Noncompliant providers must be forced to suspend the collection of any and all user data until such a time as they can be assessed as compliant. This must be strictly enforced with strong penalties for providers who continue to collect any form of data after being judged not to be complying.

Act before the implementation of age verification

As the intended time period for the commencement of age verification is rapidly approaching, the DCMS should not allow time to lapse. Waiting until age verification services are 'switched on' and already collecting user data before taking steps to protect user privacy is not an acceptable course of action. In this time period, all of the risks to users which have been highlighted in this submission would be present, and users would be put at risk unnecessarily.

(4) For example, the AgeID age verification tool operated by pornographic media giant MindGeek. For MindGeek, the mining and profiling of user data would be an exceptionally useful source of business and market intelligence, and could be used to facilitate targeted advertising.

AGE VERIFICATION - RISKS & RECOMMENDATIONS

Swift action must be taken to ensure that user privacy is adequately protected by strictly enforced standards before the Secretary of State chooses to trigger the commencement of Part 3 of the Digital Economy Act 2017.