Open Rights Group briefing on the Digital Economy Bill

Open Rights Group is the UK's only digital campaigning organisation working to protect the rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

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 and tech projects.

ORG has concerns about the following areas of the Digital Economy Bill (DE Bill):

- Age verification (Part 3)
- Web blocking (Part 3)
- Online copyright infringement (Part 4)
- Data sharing (Part 5)

1. Age Verification (Part 3 of the Bill)

Since July, there have been **two major hacks** on porn websites affecting more than 400 million people (xHamster - 380,000 people and FriendFinder 412 million accounts). People's personal details including their email addresses and usernames have been traded on the dark web. Another public exposé of people's names, addresses and phone numbers in the Ashley Madison case, reportedly resulted in two suicides. [1]

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

Age verification proposals in the Bill could create similar databases of data to those that have already been hacked. The proposals demand that people give up a part of their privacy and trust age verification systems with their personal information potentially being connected to some of their most sensitive activity online.

Age verification systems will operate in an **extremely insecure** environment.

The age-verification regulator would be able to make sites verify age and issue penalties, but they have **no specific duties** to protect people's privacy, security or defend against cyber security risks that may emerge[2] from the age verification systems.

1.1 Recommendations:
Insert privacy safeguards onto the face of the Bill.

The Digital Economy Bill's impact on privacy of users should, in human rights law, be properly spelled out ("in accordance with the law"). Reducing some of the aforementioned privacy (and free expression) concerns can be achieved if the age-verification **regulator has specific duties** to ensure that:

- Age verification systems are low security risk.
- Age verification systems do not create wider security risks for third parties, for instance to credit card systems.
- Users' data is kept anonymous. Age verification systems should not disclose the identity of individuals verifying their age to persons making pornography available on the internet.
- Users of adult websites are able to **choose** which age verification system they want to use as opposed to being given only one prescribed method by the website.

[2] Evidence to the Public Bill Committee on the Digital Economy Bill submitted by Alec Muffett outlining security risks of proposed age verification systems.
http://www.publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB39.htm

- Users of adult websites have clarity on the liability of data breaches and what personal data is at risk.
- Age verification methods are easy to operate and cheap to implement.

ORG's proposed amendment is here:
https://wiki.openrightsgroup.org/wiki/Age_Verification_amendment

2. Web-blocking (Part 3 of the Bill)

Government plans to enforce age verification on adult websites by blocking them have raised concerns[3] that **legal adult content** will be **censored**.

The proposals to web block non-complying adult websites have been hastily drafted and inserted at the last moment during the Commons debate. Their possible impacts are not yet known and have not been assessed.

Route of appeal

The age-verification regulator will be issuing blocking notices without going through a legal process (e.g. a court order) first. There is **no external route of appeal** in the Bill for incorrectly blocked websites, although an internal appeal is allowed for. Adult (and non-adult) website owners will be left with the only opportunity to challenge the regulator via judicial review. This is a highly **burdensome approach**.

Costs

Website blocking will impose costs from the technical deployment and maintenance of censorship systems. Internet service providers (ISPs) are particularly worried about the lack of consultation and disregard for costs.[4] It would be **unreasonable** to demand Internet service providers (ISPs) are **financially responsible** for these costs. In some circumstances, the costs could be prohibitive, as not all ISPs have the means to implement blocking.

---

[3] Nearly **15,000 people** have expressed in ORG's petition their disagreement with the Government plans to enforce age verification on adult websites by blocking them.

[4] Internet Service Providers' Association: "*We are concerned and disappointed it has gone down this path … this change in direction has been agreed without any consultation, with no assessment of costs nor is there any certainty that it will comply with judicial rulings on interference with fundamental rights.*"

Proportionality

The proposal needs to assess the impacts of blocking of non-complying adult websites in each case. It might be disproportionate to block websites that have a very low number of UK visitors. A particular ISP might only supply businesses, so an order asking them to apply blocks may be disproportionate. Blocking a particular website may not be proportionate if it will deprive a specific minority of their only way of expressing their sexuality. An assessment of the harms needs to be made in each case.

2.1 Recommendations:

- A process of **external appeals** should be included in the Bill so that judicial review is only one of the options.
- The Bill should provide safeguards to ensure that **small ISPs are compensated** if they are required to take action which they are are unable to implement without significant resources.
- Web blocking needs a **proportionality assessment**. Possible harms to free expression caused by blocking a website to its audience should be assessed in relation to the objectives in each case.

More detailed analysis of the web blocking proposals can be found here: https://www.openrightsgroup.org/ourwork/reports/digital-economy-bill-briefing-to-house-of-commons-at-report-stage

3. Online copyright infringement

There are a number of companies, often referred to as “copyright trolls", that look for evidence of copyright infringement online, in order to send threats to individuals in the UK. The process of detection is vulnerable to error.[5]

The process relies matching the unreliable detections with personal data from Internet Service Providers through a court order. Despite the obvious problems, the practice cannot be stopped due to international commitments to combat online copyright infringement.

Letters can therefore be sent on the basis of this unreliable evidence to accuse the recipient of copyright infringement and asking them for payment. The alleged infringements often relate to niche pornography. This is chosen by the “copyright trolls” as this is not something most people would want to become public knowledge and therefore may persuade recipients of the threats that they should pay up. (See Golden Eye[6], TCYK LLP[7] for examples).

Our advice to people who receive these letters is to contact their Citizens Advice Bureau for guidance.

Clause 27 aids these companies by empowering them to threaten any online infringer with the much stronger criminal sanctions, which include ten years in prison. Even as a general comment within a letter, this could have a powerful persuasive effect on innocent people that they should pay the sums mentioned in the threatening letters.

---

[5] For instance, the account holder may not be the infringer. The infringer might be a family member or someone else using the Internet connection. Wifi connections are not always secured by password, allowing neighbours to use the connection. Other errors include incorrect logging of Internet address connections to customers, as these vary over time.

[6] ISP customers were accused of illegally downloading a porn movie and the company demanded they pay £700.

[7] 83-year old pensioner was accused by TCYK LLP of illegally downloading a movie. The company demanded that the pensioner pays £600 to settle the case.

The courts can supervise the companies issuing the threatening letters. We believe the courts will be helped in this supervision if the new offence is clear about the criminal sanctions relating to serious losses and serious risks, that are properly regarded as criminal.

Currently, Clause 27 states that criminal liability is to be determined by ***"causing loss"*** and ***"risk of loss"*** to the owner of the copyright.

3.1 Recommendation

Clause 27 can be improved by **adding thresholds of seriousness** to the "risk of loss" and "causing loss".

This change will ensure that individuals infringing copyright are normally dealt with through civil courts and civil copyright action. It will help deliver the *"expected outcome"*[8] of the Clause, that is to criminally prosecute only commercial copyright infringers.

Proposed amendment:
https://wiki.openrightsgroup.org/wiki/Category:Proposed_DEBill_amendments

[8] Matt Hancock stated that *"A person who accidentally shares a single file without the appropriate licence, particularly when the copyright owner cannot demonstrate any loss or risk of loss, is not expected to be caught by this offence."*

4. Data sharing (Part 5)

Part 5 contains a broad range of new powers for public bodies to disclose information – also known as data sharing – mainly among each other but in some cases with the private sector.

ORG has been involved in extensive discussions about these measures. Part 5 of the Bill has serious deficiencies that need to be amended.

4.1 Lack of sufficient privacy safeguards

Chapter 1 on public services correctly attempts to restrict the scope of sharing to government activities that improve citizens' well-being. Parliament should test that the definition employed is robust. However, the safeguards in the Bill are certainly not strong enough. There are similar concerns for chapters 3 and 4 on fraud and debt.

This could lead to abuses or risks for individuals as data may end up being used for purposes very different from those originally intended in the power. For example, onwards disclosure is not allowed unless “required or permitted by any enactment” (s 33(2)(a) page 31 line 19), which can be very broad and impossible to foresee.

We therefore recommend that the bill is fixed by including key privacy safeguards in the face of the Bill through the amendments found here: https://wiki.openrightsgroup.org/wiki/Data_Sharing_amendments

4.2 Non-enforceable codes of practice

Some added safeguards are contained in the code of practice. This is not adequate because the code is not legally enforceable.

We therefore recommend that the bill is fixed by including the amendments that can be found at here: https://wiki.openrightsgroup.org/wiki/Category:Proposed_DEBill_amendments

4.3 Unconstrained sharing of bulk civil registration data

Chapter 2 provides for the sharing of civil registration – births, deaths and marriages – for any public body's functions without restrictions other than those expressly provided in other legislation. Ministers have presented this chapter as a way of improving electronic government transactions by avoiding the need for paper certificates to be circulated, which indeed is a good thing. However we have been told unequivocally that the power is intended for bulk data sharing of the full civil register across government.

This case for the power for bulk sharing of civil registration has not been made, but it appears to be more about convenience for administrators instead of a clear social purpose. There are few safeguards on how the power is used and broad purposes for which data can be shared wholesale.

We recommend that the Bill should contain a consent based power, where citizens can request the sharing of electronic individual records in order to improve e-government.

The following amendment would implement these restrictions: https://wiki.openrightsgroup.org/wiki/Category:Proposed_DEBill_amendments