Society for Civil Rights—supplementary written evidence (FEO0113)

House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online

Written evidence following the hearing on 9 March 2021

1. Preface

The author of this statement was invited by the House of Lords to give oral evidence in the Select Committee on Communications and Digital on 9 March 2021 on the question whether the United Kingdom should adopt national legislation similar to Article 17 of the EU-Directive on Copyright in the Digital Single Market (CDSMD). The statement is based on a study that the author of this statement co-authored for the German Society for Civil Rights (Gesellschaft für Freiheitsrechte e.V.) on the compatibility of Article 17 CDSMD with European fundamental rights.[1]

The following excerpt of the study outlines why Article 17 CDSMD is incompatible with the fundamental right to freedom of expression and information laid down in Article 10 of the European Convention of Fundamental Rights (ECHR). The UK Human Rights Act 1998 gives effect to the Convention in UK law and requires UK courts, including the Supreme Court, to take into account the decisions of the European Court of Human Rights (ECtHR). The ECHR and the ECtHR exist separately from the European Union. The UK's obligations under the ECHR are therefore not changed by the UK's exit from the European Union.

2. Platform liability in the DSM-Directive

Article 17 of Directive 2019/790 on Copyright in the Digital Single Market (CDSMD) constitutes a paradigm shift not just for copyright law, but also for intermediary liability in Europe more generally. Whereas up until now protected content was available unless shown to be infringing, now materials that are detected by algorithms will be removed from public circulation unless demonstrated to be legitimate.[2]

Article 17 CDSMD makes a subset of hosting service providers directly liable for copyright infringements of their users and is widely considered to require the use of upload filters, which would place ex-ante restrictions on the ability of users to communicate via these platforms. Its adoption was accompanied by widespread protests by citizens[3], as well as criticism from academics[4] and fundamental

---

1 *Reda* et al., Article 17 of the Directive on Copyright in the Digital Single Market: A Fundamental Rights Assessment, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3732223.

2 *Elkin-Koren*, Fair Use by Design, UCLA Law Review 64 (2017), p 1093; *Schwemer/Shovsbo*, What is Left of User Rights? Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime, Forthcoming in Paul Torremans (ed), Intellectual Property Law and Human Rights, 4th edition, 2020, p. 15. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3507542.

rights advocates.[5] While Member States are in the process of implementing Article 17 CDSMD into their national laws, the European institutions are deliberating additional sector-specific legislation that raises similar questions about the fundamental rights implications of filtering technologies.[6] The controversy around Article 17 CDSMD has led the European Parliament to view these technologies much more critically than in the past, and express strong reservations against their use.[7]

3. The Impact of Automatized Content Filtering on the Freedom of Expression and Information

Automatized content filtering leads to potential interferences with the internet users' freedom of expression and information, protected by Art. 10 (1) of the European Convention on Human Rights (ECHR). Art. 10 ECHR protects two dimensions of the freedom of expression and information: The freedom to impart as well as to receive information. With regard to the material scope of Art. 10 of the ECHR, the ECtHR has emphasised that this provision is to apply to communication on the Internet, whatever the type of message being conveyed.[8]

State of the art filtering technologies are not suitable for assessing the lawfulness of user- generated content. Automated tools are unable to distinguish between lawful and unlawful content, because they cannot judge the context in which content appears.[9] Especially in the field of copyright, context is crucial to determine whether a particular use of a protected work is lawful. Not all uses of copyrighted works are infringing. The use of protected material in

---

3 Approximately 170,000 people participated in street protests against the adoption of the DSM Directive on 23.03.2020. Cf. *Reuter,* Demos gegen Uploadfilter: Alle Zahlen, alle Städte. https://netzpolitik.org/2019/demos-gegen-uploadfilter-alle-zahlen-alle-staedte/. Over five million signed a petition against Article 17 CDSMD called "Stop the censorship-machinery! SavetheInternet!" on the public participation platform change.org. https://www.change.org/p/european-parliament-stop-the-censorship-machinery-save-the-internet.

4 Numerous open letters from academics and European research institutes to the legislators at different stages of the legislative process, criticizing Article 17 CDSMD (then Article 13), are available at: EU Copyright Reform, Evidence on the Copyright in the Digital Single Market Directive. UK Copyright and Creative Economy Centre, University of Glasgow.https://www.create.ac.uk/policy-responses/eu-copyright-reform/.

5 Cf. United Nations. Office of the High Commissioner on Human Rights. Letter of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the European Commission of 13.06.2020. OL OTH 41/2018. https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf.

6 Cf. Proposal for a Regulation of the European Parliament and the Council on preventing the dissemination of terrorist content online. COM(2018) 640 final. Article 6.

7 *"The European Parliament […] 5. Stresses that the responsibility for enforcing the law must rest withpublic authorities; considers that the final decision on the legality of user-generated content must be made byan independent judiciary and not a private commercial entity; […] 12. Takes the firm position that the Digital Services Act must not oblige content hosting platforms to employ any form of fully automated ex-antecontrols of content unless otherwise specified in existing Union law, and considers that mechanisms voluntarily employed by platforms must not lead to ex-ante control measures based on automated tools orupload-filtering of content and must be subject to audits by the European entity to ensure that there is compliance withthe Digital Services Act"*, European Parliament. Report with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online. (2020/2019(INL))

8 https://www.echr.coe.int/Documents/Guide_Art_10_ENG.pdf, p. 101.

9 *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 346.

user-generated content can be lawful under limitations and exceptions to copyright, such as parody or quotation, or on the basis of a license. The identification of a match between an upload and the information provided by a rightsholder is therefore only the first step in determining if the uploaded content infringes copyright laws.

Filtering technologies do not go beyond that first step, they are not capable of the complex legal and factual examination that is required to determine if the content falls under an exception or limitation.[10] The European Commission, after having heard from a variety of stakeholders including the manufacturers of filtering technologies, concluded in its guidance consultation document on the implementation of Article 17 CDSMD that "in the current state of the art, content recognition technology cannot assess whether the uploaded content is infringing or covered by a legitimate use."[11]

This fundamental shortcoming is unlikely to be solved through technological development, as even the most sophisticated filtering technologies that employ machine learning still operate on the basis of recognizing patterns in the data. These tools do not understand the contents of the patterns they detect, hence they are unlikely to perform the qualitative assessments required to determine the presence of humour, or criticism, which are necessary to determine whether a use falls under an exception or limitation. Advanced filtering technologies are capable of making quantitative distinctions regarding the amount of protected material that is used, at least with regard to some types of protected works and other subject-matter. However, these quantitative distinctions fail to align with the legal realities of copyright law. On the one hand, the use of an extremely short extract of a work can constitute an infringement,[12] whereas, on the other hand, the use of an entire work may be permissible, for example in the context of a quotation.

Furthermore, automated filtering systems cannot detect false claims of exclusive rights, including over public domain material or material that is published under a Creative Commons license (overclaiming), nor can they detect whether particular material qualifies for copyright or related rights protection in the first place. The use of automated filtering systems relies entirely upon the veracity of the information provided by presumed rightsholders. The experience with existing automated filtering systems that some large platforms have been using on a voluntary basis has provided empirical evidence for both collateral overblocking and overclaiming by negligent rightsholders.[13] This problem is exacerbated by rightsholders increasingly automating the provision of information about their repertoires to platforms. Those automated schemes are based on the assumption that those rightsholders hold *exclusive* rights in all parts of their repertoires, routinely leading to erroneous requests for the removal of content that is in the

---

10 *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 346.

11 European Commission, 2020. Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market, p. 15.

12 CJEU, C-476/17, ECLI:EU:C:2019:624 – *Pelham*, para. 29.

13 *Bridy,* The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform, Vanderbilt Journal of Entertainment & Technology Law, volume 22 (2020), p. 347.

public domain or for which rightsholders only hold a non- exclusive usage license.[14]

Collateral overblocking, meaning the over-removal of lawful content, because the content was either falsely blocked for technical reasons or because of overcompliance with copyright laws, is inherent to the context-blindness of filtering systems. Overblocking constitutes a severe interference with the right to freedom of expression of the affected user whose content is blocked, as well as the right to freedom of information of the general public, who are denied access to lawful pieces of information.

In addition to the impact on the freedom of expression caused by blocking of lawful content, overblocking also has an indirect negative effect on the freedom of expression of users by causing behavioural changes. These *chilling effects* have been empirically demonstrated in several studies, which showed a drop in individual users' activity on social media platforms after those users had received an automated copyright infringement notice.[15]

The interference with fundamental rights that is caused by automated filtering under Art. 17 CDSMD is especially severe because it leads to an ex-ante restriction of the users' freedom of expression and information. Potentially lawful content can be blocked or removed before a court or independent judicial body has assessed its lawfulness. This shift in the balance of copyright enforcement caused by the mandatory introduction of automated filtering systems undermines the essence of the fundamental rights to freedom of expression and information, because it can cause information to be prevented from publication altogether,[16] rather than being initially made available and blocked at a later point, once its illegality has been determined.

3.1 ECtHR Case Law on Overblocking and ex-ante Restrictions of Freedom of Expression and Information

The meaning and the scope of the fundamental right to freedom of expression within the ECHR can be further clarified by the ECtHR case law. The ECtHR has an extensive case law on the impacts of website blocking on the freedom of expression. In determining the severity of the interference with the freedom of expression, the ECtHR notes that overblocking constitutes a type of prior restraint, because an information is blocked before a judicial decision on the lawfulness of the content was issued.[17] The Court reiterates in this connection that prior restraints are not prohibited by Article 10 ECHR as such, but the dangers inherent in prior restraints '*call for the most careful scrutiny on*

---

14 For an example of this phenomenon, German TV station accidentally blocking a political activist group's YouTube video, after having shown it on its TV programme on the basis of a non-exclusive license, see: PinkStinks, RTL hat uns mal kurz gekillt. https://pinkstinks.de/rtl-hat-uns-mal-kurz-gekillt/.

15 Cf. *Matias et al.*, Do Automated Legal Threats Reduce Freedom of Expression Online? Preliminary Results from a Natural Experiment. https://osf.io/nc7e2/; *Penney*, Privacy and Legal Automation: The DMCA as a Case Study. 22 Stan. Tech. L. Rev. 412. https://www-cdn.law.stanford.edu/wp-content/uploads/2019/09/Penney_20190923_Clean.pdf.

16 This issue is discussed in detail below in light of the ECtHR case-law regarding prior restraint.

17 ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 90.

the part of the Court and are justified only in exceptional circumstances'.[18] This is especially relevant when the access to information on the internet is restricted, as:

> *"in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general."*[19]

The Court adds that preventive restrictions on the freedom of expression and information require a legal framework establishing precise and specific rules regarding the application of preventive restrictions.[20] The ECtHR's case law makes it therefore clear that ex-ante restrictions of the freedom of expression constitute an especially severe interference that can only be justified in exceptional circumstances.

In *Ahmet Yildirim v Turkey*, the ECtHR also addressed the issue of collateral overblocking. The Court ruled that the injunction in question violated Article 10 ECHR, because it led to a significant collateral blocking of lawful websites.[21] The ECtHR in *Kharitonov v Russia*[22] ruled that the Russian website blocking scheme that led to blocking of websites that shared the same IP address was a violation of Article 10 ECHR because it led to arbitrary and excessive blocking of lawful websites. The Court argues that any measure that renders large quantities of information inaccessible substantially restricts the rights of Internet users. Whenever a measure interferes with lawful content or websites as a collateral effect, the legal framework must establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures. When exceptional circumstances justify the blocking of unlawful content,

> *"a State agency making the blocking order must ensure that the measure strictly targets the illegal content and has no arbitrary or excessive effects, irrespective of the manner of its implementation*".[23]

The ECtHR has so far not approved of a single blocking system. Even in hate speech cases, where the ECtHR gives the Member States greater latitude, it did not approve of pre- publication restraints.[24] The ECtHR case law on blocking systems shows that the Court regards ex-ante restrictions of the right to freedom of expression and information as an especially severe interference. This interference can only be justified in exceptional circumstances and require a precise and specific legal framework. Even if an ex-ante restriction is justified to block unlawful content, the Court clearly spells out that this must not lead to overblocking.

---

18 ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* para.47.
19 ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* para.48.
20 ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 92.
21 ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey,* paras. 66–68.
22 ECtHR, Application no. 10795/14 – *Kharitonov v Russia*.
23 ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, paras. 45 f.
24 In *Delfi AS v. Estonia,* Application no. 64569/09 – *Delfi AS v. Estonia*, the ECtHR accepted that states may impose liability if the portals fail to remove certain kinds of hate speech, however, *Delfi AS v Estonia* only referred to certain kinds of hate speech for which the ECtHR accepted ex-post removal (para. 159), and didnot approve of preventive filtering of content before its publication.

Although the ECtHR's cases dealt with the blocking of websites, the same analysis applies to service providers hosting user-generated content. In *Kablis v Russia,* the ECtHR confirmed that the blocking of individual content falls under the same category of interferences, that is prior restraints, because it amounts to a limitation of the freedom of expression and information prior to judicial determination of lawfulness.[25]

In conclusion, the interference with the freedom of opinion which automated content filtering in the copyright context causes is of particular severity under the European Convention of Human Rights. The blocking of content before its publication and before a court has assessed its lawfulness is a prior restraint according to the ECtHR's case law that can only be justified in exceptional circumstances. The ECtHR places great importance on the fact that filtering systems may lead to the collateral overblocking of lawful content. In the ECtHR's case law on website blocking, it is well established that ex-ante restrictions of the freedom of expression and information on the internet can only be justified in exceptional circumstances and require a precise and specific legal framework. As will be shown below, Article 17 CDSMD fails to meet this standard.

3.2 ECtHR Case Law on Filtering Systems and Procedural Safeguards

As outlined above, the ECtHR has ruled on the admissibility of website blocking schemes in various cases and has not yet accepted a single blocking system. All of the ECtHR's case law finds violations of the freedom of expression and information due to insufficient safeguards. The starting point in all these cases is that the blocking of content before its unlawfulness has been established is a type of prior restraint.[26] The ECtHR explicitly states that "a legal framework is required to ensure both tight control over the scope of bans and an effective Convention-compliant judicial review".[27] According to the ECtHR, legislation must "provide safeguards against abuse (...) in respect of incidental blocking measures".[28] Legislation that leads to preventive restrictions of the fundamental right to freedom of expression and information must itself contain a precise and specific framework regarding the application of these restrictions.[29]

In the decisions of *Kharitonov v Russia, OOO Flavus v Russia and Engels v Russia*, the ECtHR found that website blocking schemes violated Article 10 ECHR for not including the following safeguards: (i) an impact assessment of the blocking measure prior to its implementation, (ii) an obligation to proactively notify and educate those who might be impacted by overblocking, (iii) the blocking measures had not been sanctioned by a court or other independent adjucatory body, (iv) they lacked effective transparency with respect to grounds and possibilities to challenge already implemented blocking

---

25 ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 90.

26 *Husovec*, Overblocking: When is the EU Legislator Responsible? p. 11, https://ssrn.com/abstract=3784149; ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, para. 43.

27 ECtHR, Application no. 3111/10 – *Ahmet Yildirim v Turkey* para.64.

28 ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, para. 43.

29 ECtHR, Applications nos. 48310/16 and 59663/17 – *Kablis v. Russia*, para. 92.

measures, (v) and did not provide for judicial recourse for the parties.[30]

Ultimately, the safeguards in Article 17 CDSMD do not meet the strict requirements of the ECtHR's case law. Article 17 CDSMD does not lay down clear and precise minimal procedural safeguards. With regard to the 'specific' safeguards, the Directive leaves the design of the complaint and redress mechanisms entirely to the Member States. The text of the Directive does not provide for basic information rights of users, nor for state oversight or transparency. In addition, the directive contains no provisions on how Member States should ensure that the decisions of the in-platform redress mechanisms are effectively enforced. In particular, it fails to ensure that service providers cannot evade their obligations toward users by resorting to the blocking of user uploads on the basis of their terms and conditions, rather than on the basis of Article 17 CDSMD.[31] The general safeguards are not suitable to mitigate the interferences with the fundamental rights of users. They do not provide sufficient guarantees to effectively protect their rights from the prior restraint imposed by the Article 17- mechanism.

26 March 2021

30 ECtHR, Application no. 10795/14 – *Kharitonov v Russia*, paras. 43–45, 55.

31 The experience with the German Network Enforcement Act shows that this is not merely a theoretical concern. Cf. *Wagner et al.*. Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act, FAT 2020.