International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

'Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market

Felipe Romero Moreno

To cite this article: Felipe Romero Moreno (2020) 'Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market, International Review of Law, Computers & Technology, 34:2, 153-182, DOI: 10.1080/13600869.2020.1733760

To link to this article: https://doi.org/10.1080/13600869.2020.1733760

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
2020, VOL. 34, NO. 2, 153–182
https://doi.org/10.1080/13600869.2020.1733760

Routledge
Taylor & Francis Group

'Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market

Felipe Romero Moreno

Hertfordshire Law School, Hertfordshire University, Hertfordshire, UK

ABSTRACT

This paper critically examines to what extent Article 17 of the EU Directive on Copyright in the Digital Single Market (CDSM) could be implemented in a way which complies with the right of online content-sharing service providers and uploaders to a fair trial, privacy and freedom of expression under Articles 6, 8 and 10 of the European Convention on Human Rights (ECHR), the E-Commerce Directive 2000/31 and the General Data Protection Regulation 2016/679. The analysis draws upon Article 17 CDSM Directive, the case-law of the Strasbourg and Luxembourg courts, and academic literature. It assesses the compliance of 'upload filters' with the European Court of Human Rights' (ECtHR) three-part, non-cumulative test to determine whether the obligations laid down in Article 17 can be implemented: firstly, that it is 'in accordance with the law'; secondly, that it pursues one or more legitimate aims contained in Article 8(2) and 10(2) Convention; and thirdly, that it is 'necessary' and 'proportionate'. The paper also evaluates the compatibility of upload filters with the ECtHR principle of presumption of innocence under Article 6 ECHR. It proposes that for Article 17 to be a human rights-compliant response, upload filters must be targeted specifically at online infringement of copyright on a commercial-scale.

KEYWORDS

Upload filters; notice and staydown; human rights

1. Introduction

The European Union Directive on Copyright in the Digital Single Market (the CDSM Directive) aims to strengthen the hand of rightholders to enabling them to better negotiate and be compensated for the use of copyrighted material. Article 17 of the CDSM Directive permits rightholders to negotiate with user-generated content (UGC) services the way in which rightholder content is shared and utilised (EC 2019). This obligation affects online content-sharing service providers (OCSSPs), which have become the predominant way for users to access large amounts of copyrighted material that OCSSPs economically benefit from through ad revenue, generally without the rightholder's permission (EC 2019).

Specifically, Article 17 of the CDSM Directive requires specific types of OCSSPs to enter into licensing agreements with rightholders for the use of works, for instance, songs and

CONTACT Felipe Romero Moreno f.romero-moreno@herts.ac.uk University of Hertfordshire, de Havilland Campus, Hatfield AL10 9EU, UK

This article has been republished with minor changes. These changes do not impact the academic content of the article.

videos. If a licence is not concluded (perhaps because rightholders are unwilling to do so), OCSSPs must make 'best efforts' to guarantee that unauthorised content for which rightholders have given the 'relevant and necessary information' is inaccessible (EC 2019). Furthermore, after receiving a notice from rightholders, such OCSSPs must remove or disable access to the uploaded content (EC 2019). There is a general agreement in the literature that what this 'best effort' obligation means in practice is the adoption of notice and staydown or 'upload filters'. This is where a rightholder takedown notice for a specific unlawful copyrighted work triggers an OCSSP's duty to proactively detect and remove all instances of infringing content and prevent future uploads (Engstrom and Feamster 2017, 10; Romero-Moreno 2019, 2; Urban, Karaganis, and Schofield 2016, 60). This is notwithstanding the fact that the European Commission (EC) neither requires any upload filters nor compels OCSSPs to utilise any specific technology or means (EU 2019) following implementation of the CDSM Directive. As the literature suggests, however, the problem remains that in the EU internet governance decisions are gradually moving from intermediary liability to intermediary responsibility (Frosio and Mendis 2019, 17; Kuczerawy 2019, 2; Montagnani and Yordanova-Trapova 2018, 295, 297).

The E-Commerce Directive 2000/31 (the E-Commerce Directive), which is currently under review, is the legislative framework for intermediary service providers in the Single Market. This Directive aims to eliminate barriers to cross-border services within Europe, as well as provide legal certainty to individuals and companies. The E-Commerce Directive provides intermediary service providers which offer mere conduit, caching and hosting functions with a specific exemption from secondary liability due to unlawful users' activity. More specifically, Article 14 of the E-Commerce Directive shields hosting service providers against liability for content stored by uploaders if services have no actual knowledge of the unlawful action/content and are unaware of facts and circumstances from which unlawful action/content has appeared. If the service gains knowledge/awareness, it is still exempted if it acts expeditiously to disable or remove access to the content by implementing a notice and takedown procedure. Similarly, the literature seems to identify an existing research gap in that the Court of Justice of the EU (CJEU) has yet to fully clarify the boundary between general and specific monitoring (Frosio and Mendis 2019, 4, 24; Husovec 2019, 25; Kuczerawy 2019, 14–15; Riordan 2016, 422). Article 15 of the E-Commerce Directive prohibits Member State courts from imposing on service providers a general obligation to monitor stored or transmitted information or actively look for facts or circumstances denoting unlawful action, such as uploading unauthorised copyrighted material. However, importantly, under the E-Commerce Directive, the prohibition of monitoring duties exclusively concerns monitoring of a general character. Recital 47 of the E-Commerce Directive also allows Member States to require services to perform a monitoring obligation in a specifically targeted situation.

Moreover, pursuant to Recital 48 of the same Directive, such services can also adopt 'duties of care' to identify and prevent unlawful activities, specified by domestic legislation. In this context, it is worth stressing that in *Glawischnig-Piesczek v Facebook* the CJEU explained that, pursuant to Article 15 of the E-Commerce Directive, a duty extending to information with equivalent content did not result in a general monitoring obligation being imposed upon hosting services. The CJEU found that this was particularly the

case provided that the monitoring and examination of information required were limited to the information including the details set out in the staydown injunction, and the services were not required to undertake an independent evaluation since they could use 'automated search tools and technologies'.[1] Furthermore, in view of *Google France v Louis Vuitton*[2] and *L'Oréal v eBay*,[3] the literature elaborates that the CJEU also needs to shed more light on the scope of the E-Commerce Directive's safe harbour regime as per its Article 14 (Angelopoulos and Quintais 2019, 6, 13; Bridy 2019, 9–12; Visser 2019, 11). As of 22 August 2019, TorrentFreak explains on its blog that in several pending cases[4] the Luxembourg Court was requested to address some important questions regarding upload filters. For example, one was whether hosting services such as Google's YouTube, under Article 14 E-Commerce Directive, played an 'active role' when classifying footage, making topic suggestions and targeting ads, and another was whether these services should remove copyrighted material based simply upon metadata (to prevent recurrent uploads), rather than identifying specific unlawful material.

Building on the author's previous research (Romero-Moreno 2019), the purpose of this paper is twofold. The first is to critically assess the extent to which Article 17 of the CDSM Directive can be implemented in a way which is compatible with the right of OCSSPs and uploaders to a fair trial, privacy and freedom of expression under the European Convention on Human Rights (ECHR), the E-Commerce Directive and the General Data Protection Regulation (EU) 2016/679 (GDPR). The second is to suggest and appraise some procedural safeguards to ensure the CDSM Directive's compatibility with the ECHR, the E-Commerce Directive and the GDPR. Importantly, the paper seeks to fill a major gap in the literature by proposing that, in order for Article 17 to be a human rights-compliant response, upload filters must be specifically targeted at infringement of copyright on a commercial-scale. I conclude that unless, pursuant to the stakeholder discussions requirement contained in Article 17(10) of the CDSM Directive, the procedural safeguards suggested in this paper are heeded, the implementation of Article 17 will violate Articles 6, 8 and 10 of the Convention, the E-Commerce Directive and the GDPR.

2. The substantive law

Article 17(1) of the CDSM Directive states that Member States must set out clearly in national legislation that an OCSSP carries out an act of making available to the public or an act of communication to the public if it grants the public access to uploaded copyrighted works or other subject matter. Thus, Article 17(1) of the CDSM Directive requires OCSSPs to gain authorisation from rightholders under Article 3(1) and (2) of Information Society Directive 2001/29 by concluding licensing agreements. Article 17(2) of the CDSM Directive explains that such authorisation not only covers non-commercial activities of users but also those user actions which do not generate substantial revenues. Importantly, however, Article 17(3) of the CDSM Directive alerts that if an OCSSP carries out an act of communication or making available to the public, it cannot benefit from the liability exemption enshrined in Article 14(1) of the E-Commerce Directive. Accordingly, Article 17(4) of the CDSM Directive elaborates that if a licensing agreement is not concluded, the OCSSP is liable unless it shows that it has:

(a) 'made best efforts to obtain an authorisation, and

(b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event
(c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).'

Put differently, Recital 66 of the CDSM Directive sums up that if rightholders neither provide the OCSSP with the 'relevant and necessary information' nor notify the OCSSP regarding the removal or disabling of uploaded copyrighted material, the OCSSP is exempt from liability.

In terms of the principle of proportionality, Article 17(5) of the CDSM Directive recognises that, in establishing whether the OCSSP satisfies the above obligations, there are several factors to consider, such as (a) the type, audience and size of the OCSSP, and the type of uploaded copyrighted content; and (b) the existence of effective and suitable means, and their cost for OCSSPs. Recital 66 of the CDSM Directive stresses that depending on the type of work, different means to prevent unlawful material could be appropriate and proportionate. Thus, when assessing proportionality, the evolving state of the art regarding current means must also be considered, including possible future developments.

However, Article 17(6) of the CDSM Directive subjects start-ups and small OCSSPs which have existed for less than 3 years with a turnover below 10 million euros to simpler obligations. According to Article 17(6), if these small OCSSPs fail to conclude an agreement with rightholders, following a rightholder notice, they must respond expeditiously to remove or disable access to the unlawful content by implementing notice and takedown. Notwithstanding, if at a later stage the audience surpasses 5 million visitors monthly, upon receiving a rightholder notice, such small OCSSPs must also make best efforts to prevent future uploads by adopting notice and staydown. Furthermore, the EC has stressed that uploading GIFS, memes or similar UGC is expressly permitted (EC 2019) as under Article 17(7) the CDSM Directive must in no way impact lawful uses, thereby allowing uploaders to rely on exceptions or limitations to copyright for the purposes of review, quotation, criticism, pastiche, caricature or parody. However, this contrasts with Cambridge Consultants' warning that these types of UGC cannot easily be determined using content analysis alone but require knowledge of the context surrounding it to establish whether it is copyright infringing. In fact, understanding such context consistently raises significant issues for both AI and humans. It demands a wider appreciation of cultural, societal, political and historical aspects, thus requiring a mixture of contextual and cultural awareness to be effective (Ofcom 2019, 4, 33).

Pursuant to Article 17(9) of the CDSM Directive, OCSSPs must also inform users in their terms and conditions about these exceptions or limitations. Recital 70 of the CDSM Directive therefore points out that legally obliging Member States to permit such uses is vital to strike a balance between the right to freedom of expression, freedom of the arts, and IP under the EU Charter of Fundamental Rights (the Charter). Although not specifically referring to Article 15 of the E-Commerce Directive, importantly, Article 17(8) of the CDSM

Directive expressly prohibits Member States from implementing Article 17 in a way which could lead to the imposition on OCSSPs of a general monitoring obligation of UGC. Recital 84 states that the CDSM Directive complies with the fundamental rights and principles enshrined in the EU Charter. Therefore, it should be applied and interpreted by observing such rights and principles. Moreover, crucially, Article 17(9) also compels Member States to implement the above obligations in compliance with data protection and privacy laws since the CDSM Directive must neither result in any disclosure of users nor in the processing of personal data, except pursuant to the GDPR and E-Privacy Directive 2002/58. Indeed, echoing Article 28 of the CDSM Directive, Recital 85 CDSM Directive stresses that any personal data processing must also respect the right to privacy and protection of personal data under Articles 7 and 8 of the Charter.

Furthermore, Article 17(9) asserts that Member States must also require OCSSPs to provide for an expeditious and effective complaint and redress mechanism for users who contest the unjustified removal or disabling of access to uploaded content. Specifically, Article 17(9) of the CDSM Directive indicates that if rightholders request removal or disabling of access, they must provide solid grounds for such a request. It further explains that user complaints must be handled without excessive delay and removal or disabling decisions should be subject to human review. Additionally, under Article 17(9), Member States must establish alternative dispute resolution or out-of-court redress systems, thus allowing disputes to be decided independently, without affecting users' right to go to domestic courts and rely on copyright exceptions or limitations.

Lastly, and of particular relevance here, Article 17(10) of the CDSM Directive adds that the EC, in collaboration with the Member States, must arrange stakeholder discussions to consider best practices for collaboration among rightholders and OCSSPs. Thus, vitally, Article 17(10) requires the EC, in cooperation with rightholders, OCSSPs, user groups and others, to discuss potential practical solutions for the implementation of Article 17, emphasising the importance of striking the right balance between fundamental rights and copyright exceptions and limitations. Article 17(10) concludes that, regarding these stakeholder dialogues, user groups must also have access to appropriate data from OCSSPs on the operation of the cooperation procedures. In this context, it is important to reiterate that unless, following the stakeholder discussions requirement included in Article 17(10) of the CDSM Directive, the procedural safeguards proposed below are taken on board, the adoption of Article 17 will infringe the rights of OCSSPs and uploaders under Articles 6, 8 and 10 of the ECHR, the E-Commerce Directive and the GDPR. Moreover, in order for Article 17 to be a lawful response to the problem of online copyright infringement, upload filters must be targeted specifically at commercial-scale cases.

3. Completing the upload filter puzzle

For the upload filter puzzle to be complete, it requires several pieces to be in place: firstly, the algorithm needed for detecting a specific fragment of material; secondly, a database of copyrighted works against which every uploaded fragment of material can be checked; and lastly, arrangements with rightholders as to what steps to take if a match is identified. Importantly, for the successful implementation of Article 17 of the CDSM Directive, content recognition and filtering technologies must exist for every type of uploaded content. Therefore, the algorithms used should detect all types of material – audio, video and

images. Then, once uploaded content is detected, an infringement can be flagged by checking it against a database that must be managed and constantly updated in cooperation with rightholders (Gann and Abecassis 2018, 4).

3.1. Types of filtering technology: OCSSPs make 'best efforts to prevent future uploads'

3.1.1. Metadata

The simplest form of content recognition and filtering system relies upon a content metadata query which examines data surrounding the content (Engstrom and Feamster 2017, 11). This 'metadata' might include information concerning the file, for instance, in respect of a film, its title and duration (Gann and Abecassis 2018, 5). The metadata of a fragment of file can be compared against a database of copyrighted content without having to examine the content. However, this technique has obvious drawbacks since metadata can easily be manipulated by users and is frequently unreliable or incorrect (Gann and Abecassis 2018, 5).

3.1.2. Hashing

With hashing, a fragment of material is depicted numerically using a content hash. The file size of such a numerical depiction is considerably lower than the one of the initial file, making it more effective when comparing the hash value of an uploaded fragment of content against databases of hash tasks (Gann and Abecassis 2018, 5). This technology has been criticised for only allowing strictly same files to the original files to be identified. However, for instance, Google's YouTube uses hashing to prevent an identical file to the original file already removed after a notice and takedown process from being reuploaded (Japiot 2017, 17). It is worth noting that in *Glawischnig-Piesczek v Facebook* the CJEU found that, following a complaint notification, hosting services could be compelled to remove and/or block access to 'identical' and 'equivalent' information previously found to be illegal by Member State courts, even worldwide, provided that the staydown injunction respected international law.[5] Therefore, importantly, considering the CJEU's finding, this means that YouTube's use of hashing would respect Article 15 E-Commerce Directive as it would constitute a monitoring obligation in a 'specific' case, something which is permitted under Recital 47. However, one of the problems with this technique is that any file modification also leads to alteration of the hash value (Gann and Abecassis 2018, 6).

3.1.3. Watermarking

This technique is normally in the form of a hidden barcode individually incorporated into the file, which is used to detect sounds, videos or images. It is frequently employed within the film industry to identify the source of copyright infringement, such as unlawful recordings made in film theatres. In practice, any watermarked duplicate is instantly detected, whilst a duplicate without a watermark, for instance, if it was made before the watermarking operation, cannot be identified. Thus, it can only be utilised to protect new copyrighted works but not content already disseminated. However, as with metadata and hashing, this technology also has its challenges since it is unable to detect the use of works within content that is exclusively created by others, such as cover songs (Japiot 2017, 17).

3.1.4. Fingerprinting

Although the CDSM Directive does not expressly refer to content recognition and filtering using fingerprints, the EC Impact Assessment appears to indicate that the intention of the EC was to deploy these systems (EC 2016, 164–165). Content-based fingerprinting is a more advanced technique which examines a specific piece of material to establish its unique features. It identifies original content even if modifications are carried out, since the technology detects the content instead of the file (Gann and Abecassis 2018, 6). For instance, Google's YouTube ContentID can detect endeavours to avoid identification like slowing down or speeding up the audio, modifying a video's aspect ratio or flipping images horizontally. Similarly, with developments in machine learning, it can also recognise audio, music and video in remixes, remakes or reuploads rightholders decide to claim, track or block from YouTube (Google 2018, 27). In practice, relying on a European patent from the self-proclaimed leading content recognition and filtering solution Audible Magic, a fingerprint can be created to help detect copyrighted content. The created fingerprint is subsequently contrasted with an archived fingerprint from 'registered copyrighted works' (European Patent Office 2014, 4). If there is a match, thereby indicating the sending of a registered work, transmission data are then logged. It is important to stress that multiple data values for detecting the transmission of a copyrighted work can be logged, which are part of Audible Magic's dataset. These can include one or more of the following:

(a) Sender IP address from which the detected material was sent;
(b) Receiver IP address to which the detected material was sent;
(c) The date the identified content was disseminated;
(d) The time the identified content was disseminated;
(e) The title or name of the work, whether video, image, audio or other type;
(f) Artist name, if appropriate, when the work is copyrighted content already registered with the service provider;
(g) Album name, if applicable, linked to a registered copyrighted content;
(h) Record company, if applicable, linked to a registered copyrighted content;
(i) Different metadata, such as producer name, distributor name, studio name, etc.;
(j) The count of unlawful downloads arranged in different ways, such as by IP address, location, day, week, month etc.;
(k) The count of redirected tried downloads arranged in different ways, such as by IP address, location, day, week, month, etc. (European Patent Office 2014, 4–5)

As noted before, software used in upload filters is limited to the type of material it is designed to detect. This means that whilst an OCSSP which exclusively permits the supply of audio content would only need to examine UGC utilising software designed for audio file recognition, a service provider utilising UGC for audio, images and video would need to employ different filters for all the different content types (Gann and Abecassis 2018, 6). Article 17(4)(b) of the CDSM requires OCSSPs to make best efforts to guarantee the absence of 'specific works and other subject matter'. However, this broadly written passage appears to ignore the fact that currently no upload filter exists which can recognise both 'specific works and other subject matter', such as software code, 3D printing files or written text (Gann and Abecassis 2018, 4, 7, 8, 9).

3.1.5. Other technologies

In addition to content recognition and filtering systems using fingerprints, other technologies are also being employed in beta releases or in conjunction with those previously explained. Technology may well emerge soon that improves efficiency and decreases the amount of computer performance required (Japiot 2017, 18). Indeed, as stated before, Recital 66 of the CDSM Directive explains that to assess proportionality the evolving state of the art concerning current means, including possible future developments, to prevent the existence of distinct types of material and the cost for OCSSPs, must be considered. For instance, in order to gain contextual understanding, Cambridge Consultants argues that by utilising AI, machine learning and deep learning it may be possible to carry out a targeted search based on metadata supplied by the user to identify and classify repeat copyright infringers into commercial-scale uploaders. This user metadata, which is similar to the Audible Magic's dataset above, could include information related to uploaded content such as uploader IP address, uploader previous content history, uploader location, time on platform, connection type and uploader earlier content removals and appeals (Ofcom 2019, 6, 32, 52).

As set out in Audible Magic's European patent mentioned above, and consistent with the CJEU rulings in *Sabam v Netlog*[6] and *Sabam v Scarlet*[7], it might not be reasonable to apply content-based fingerprinting to 'all' files carried through the network due to the usually processor-exhaustive character of fingerprint creation and comparison. Therefore, it is arguable that utilising a hierarchical technique to examine the possible copyright protected work being sent – for example, as this paper suggests, content of high commercial value – might be preferable to guarantee adequate speed with limited processing resources. Respecting the European Court of Human Rights (ECtHR)[8] and CJEU[9] case-law, a fundamental principle of such a technique is to begin with less processor-exhaustive stages to establish whether the transfer includes a registered copyrighted file, and accordingly to move to more processor-exhaustive stages only if previous stages do not return a match (European Patent Office 2014, 8).

The initial assessment step could be a comparison of the file name and file size. If there is a match in the database for both the file name and file size, then the probability is elevated that the digital sample includes a specific registered and copyrighted file. Comparing file names and file sizes is normally an easy task and does not deplete significant processing resources (European Patent Office 2014, 8). If the file name and file size do not match, the second assessment step entails registering the source and destination IP addresses, the type of copyrighted files, and the frequency and number of transmissions or tried transmissions. Asking a database for suspect source IP addresses involved in a history of unlawful transmissions is normally less processing-demanding than creating and comparing fingerprints (European Patent Office 2014, 9).

On the other hand, if analysis of the source IP address and file size and/or type do not match a registered copyrighted file, then the next assessment step is detection through a watermark or metadata. Searching a database for the existence of a watermark or metadata information is done prior to content-based fingerprinting to attain good speed features when processing resources are restricted (European Patent Office 2014, 9).

A fingerprint test is performed if none of these assessment steps establish the existence of a registered and copyrighted file. In order to assess the effectiveness of any hierarchical identification technique, even if one or more of the above assessment steps returns a

match, it is preferable to compare at least a fragment of the matched findings with a fingerprint for confirmation purposes (European Patent Office 2014, 9).

3.2. Databases: rightholders provide 'relevant and necessary information'

As noted before, in the upload filter the presence of algorithms is essential but only one part of what is required since rightholders also need to register fingerprints and metadata in databases. Content recognition and filtering systems permit a portion of unidentified material to be compared with a database of files that include reproductions of registered works. To establish whether a song is copyrighted, upload filters must be applied to the file to assess it and subsequently compare it against a database of registered songs (Gann and Abecassis 2018, 4). To do so, as required under Article 17(4)(b) of the CDSM Directive, rightholders must provide OCSSPs with 'relevant and necessary information' on their catalogues of specific works that must then be kept in databases which can be scanned by such filters.

It is worth pointing out that, in a welcome move, Google's YouTube has updated its ContentID algorithm for creators. As of 16 August 2019, TorrentFreak explains on its blog that YouTube also permits specific rightholders to make 'manual' infringement claims. Whilst this allows rightholders to identify material, which is not detected by ContentID, it is significant that such claims are reviewed by a human. This is because the automated ContentID is not a 100-percent foolproof system and sometimes makes mistakes. To prevent dishonest behaviour, rightholders manually submitting claims are required to provide 'relevant and necessary information' for the specific portion of the video they report. Moreover, rightholders are prohibited from manually claiming content which utilises short or random music pieces such as a three-second music video in a longer piece of footage, or a track which happens to be playing in the background. Notably, TorrentFreak concludes that those rightholders who repeatedly infringe such a policy will have their manual ContentID claiming rights terminated.

There is the additional problem that the volume of UGC and the presence of numerous rightholders raises significant technical, legal and commercial issues. For each kind of work, rightholders must cooperate to create a database and provide their copyrighted material in an upload filter-compatible form. Indeed, as flagged above, in industries such as text, software or 3D printing, centralised databases simply do not exist. It can be noted that this coordination challenge might be more easily addressed within the music industry where, unlike the world of images, there are few major rightholders (Gann and Abecassis 2018, 4, 7, 8, 9).

As the CDSM Directive recognises,[10] in the EU each Member State is free to adopt its individual copyright legislation and infringements are tackled at a domestic level. This is set to cause further problems when it comes to creating pan-European databases since the specific definitions of copyrighted material will differ between countries. Databases of material would need to reflect domestic legislation, which could potentially lead to different databases for each Member State against which OCSSPs functioning in that country would need to do their checks (Gann and Abecassis 2018, 8).

Therefore, as will be discussed in greater detail later, unless copyright databases are centralised and targeted exclusively at music and video with high-commercial value content, arguably the implementation of upload filters will mean that fragmentation

could be a real problem. On the one hand, major rightholders who have already invested in the establishment of databases may not be willing to enlist other databases and exchange their copyrighted material due to costs. On the other, OCSSPs would have to check uploaded content against different platforms. The result would be that the cost of implementing Article 17 of the CDSM would increase with every supplementary database against which UGC must be compared (Gann and Abecassis 2018, 9, 11).

3.3. Business rules: rightholders design business instructions considering 'availability of suitable and effective means' and 'cost' for OCSSPs

Arrangements with rightholders in terms of what actions to take if a copyright match is detected constitute a significant part of the upload filter and are needed to implement Article 17 of the CDSM (Gann and Abecassis 2018, 4). For instance, according to Google, by using YouTube's ContentID rightholders can be automatically informed of uploaded UGC which includes their copyrighted work and choose between three actions or so-called business rules: first, monetise the upload; second, leave it up and analyse viewing figures; or third, block it (Google 2018, 25).

Importantly, business rules must also be registered by rightholders in databases and, as Google reveals, those rules can be 'flexibly' adopted based on how the work has been reused (Google 2018, 25), for example, pursuant to Article 17(7) of the CDSM Directive, for the purposes of review, quotation, criticism, pastiche, caricature or parody. The search engine further explains that rightholders can also design business rules according to the amount of their work utilised in a piece of footage or the percentage of the footage their work accounts for (Google 2018, 25). Similarly, Audible Magic acknowledges that such rules can be adopted either independently or in combination based on the frequency, number and/or timing of transmissions of specific content (European Patent Office 2014, 9).

Additionally, Audible Magic elaborates further business rules that include sending a message, preferably giving clear instructions to the sender and/or receiver IP addresses participating in the transmission of unlawful copyrighted content, and sending a message alerting a receiver IP address of, or redirecting a receiver IP address to, a commercial website where the wanted copyrighted content can be bought. If the receiver decides to challenge the blocking, a return message is sent, thus allowing the immediate transmission of content to the receiver (European Patent Office 2014, 6).

Article 17(5) of the CDSM Directive states that, in order to satisfy the principle of proportionality, the existence of 'suitable and effective means' and the 'cost' for OCSSPs must be considered. However, although omitted from the CDSM Directive, it should also be noted that to implement upload filters the use of Deep Packet Inspection (DPI) technology is essential. DPI blocking requires information or signature, but it is computationally quite complex and therefore expensive as all copyrighted material needs to be assessed against blocking rules. In practice, DPI has a list of information to block, for example, filenames, keywords, traffic features such as transmission rates or packet sizes, or other content-specific data. This means that any endeavour to download unencrypted copyrighted material which matches one on the list would be stopped (Internet Society 2017, 14).

Referring back to the 'suitable and effective means' test above, DPI would be very ineffective for generic rules such as 'block inadequate content' or against multiple

encryption. Moreover, with this technology both false positives (blocking material erroneously) and false negatives (being unable to block material as expected) are frequent. Indeed, the false positive percentage varies from remarkably low to significantly high. Importantly, ensuring compliance with the 'suitable and effective means' test would all depend on the quality of the blocking rules, for instance, rules specifically targeting commercial-scale online copyright infringement. Whilst it is hard to draft high-quality business rules, if the filtering rules are improperly drafted minor modifications to text can easily circumvent blocking efforts (Internet Society 2017, 21). Additionally, consistent with the AG warning in *Sabam v Scarlet*, since DPI inspects all traffic to users it would also invade a user's privacy, personal data protection and confidentiality of communications.[11]

4. Proposal

For rightholders, whether to permit, monetise or block copyrighted content is frequently determined by the advertising revenue that could be received for the video or audio. Thus, to satisfy the stakeholder discussions requirement under Article 17(10) of the CDSM Directive, it is arguable that rightholders should always be encouraged to favour monetisation over blocking (Japiot 2017, 20). However, perhaps rightholders might fail to reach an agreement concerning this matter. Accordingly, as noted before, consistent with ECtHR[12] and CJEU[13] case-law, it is possible to utilise a hierarchical identification technique as well as design databases of 'relevant and necessary information', and business rules specifically targeting commercial scale copyright infringement.

The hierarchical technique begins with less processor-exhaustive stages before moving to more processor-exhaustive ones, but only if previous stages do not return a match (European Patent Office 2014, 8). However, importantly, whether or not a match is found, when copyrighted material is detected upload filters can always return a response, which can itself unlock a registered business rule (Audible Magic 2017, 28). Therefore, the first step of the suggested proposal is to assess whether the uploaded content contains a registered work of high commercial value and, if that returns a match, permitting or monetising (not blocking) it. A database could then be interrogated to determine commercial-scale copyright infringement before blocking it (European Patent Office 2014, 8–9).

While most attempts to upload content are identified and stopped when uploading, some cannot be detected by upload filters, for instance, because the uploaded copyrighted work is not registered in a database (Audible Magic 2017, 51). Thus, the proposal's suggestion for an initial stage would be for rightholders to exclusively register in a database content of high commercial value. Since upload filters cannot recognise all types of content, only video and audio metadata values like those included in Audible Magic's dataset above should be registered in a database (European Patent Office 2014, 4–5).

Moreover, although the most commonly used business rules include permitting, monetising or blocking, such actions can be 'flexibly' adopted (Google 2018, 25). Thus, the proposal's second stage would be for rightholders to register in a database rules which fully comply with the case-law of the Strasbourg and Luxembourg courts. In particular, there should be the following business rules: first, assessing whether the uploaded material contains a registered work of high commercial value;[14] then, checking the frequency and number of unlawful uploads[15] that is, asking a database for suspected repeat infringement IP addresses; next, sending a message alerting[16] of potential commercial-scale

infringement or redirecting to a commercial website; and lastly, giving the opportunity to alleged commercial-scale uploaders to challenge[17] the blocking before actually implementing it (European Patent Office 2014, 6, 8, 9).

Taken together, the suggested parts of the proposal would involve a two-prong non-cumulative test: first, a qualitative assessment depending on the nature of the registered and copyrighted content, and second, a quantitative assessment based on whether a source IP address creates a history of unlawful uploads and, if so, whether the file type is consistent with past unlawful uploads (European Patent Office 2014, 9), thereby reaching the commercial-scale threshold. Crucially, implementing this proposal would mean that, for upload filters, respecting ECtHR[18] and CJEU[19] case-law and observing Recitals 47 and 48 E-Commerce Directive would become lawful 'duties of care' constituting a monitoring obligation in a specific case exclusively targeting high commercial value content and previously notified and identified commercial-scale uploaders. The suggested proposal would further support the CJEU's finding in *Glawischnig-Piesczek v Facebook* that Article 15 E-Commerce Directive required staydown injunctions allowing upload filters' monitoring and analysis of user information to be limited to specific content. The CJEU found that hosting services were not compelled to conduct an independent evaluation to detect content of an equivalent character since they could deploy automated analysis methods and technologies.[20]

5. Compatibility of Article 17 of the CDSM Directive with the GDPR

Article 17(9) CDSM states that its implementation must not result in any disclosure of user information or in the processing of personal data, except pursuant to the GDPR and the E-Privacy Directive 2002/58. It is useful that the GDPR includes regulations on both automated individual decision-making, that is, making a decision based solely on automated means without any human participation (Article 22(1) GDPR) and on profiling (namely, any form of automated personal data processing, which involves the use of personal data to assess individual aspects) as per Article 4(4) GDPR. It is not uncommon for profiling to be part of an automated decision-making process under the GDPR (ICO 2018a).

Article 4(4) GDPR states that profiling is any type of automated personal data processing which comprises the usage of personal data to assess specific individual factors concerning a natural person, particularly to examine or predict factors regarding that natural person's behaviour and/or location. As noted above, relying on Audible Magic's dataset, the suggested proposal would require OCSSPs to collect both uploader personal and sensitive data, such as IP addresses and content media name. Subsequently, as required by Article 4(4), utilising AI and machine-learning such data would be examined to categorise repeat copyright infringers into commercial-scale uploaders and establish links between uploader behaviour and location (ICO 2018a).

Moreover, under the GDPR, pursuant to Article 22(1), service providers can exclusively perform solely automated decision-making with lawful or equally important effects including those premised upon uploader profiling when the decision is: (a) required for the performance of contracts; (b) allowed by EU law, such as for implementing the obligations laid down in Article 17 of the CDSM Directive; (c) or based on uploader's express consent. Moreover, whilst Article 22(3) GDPR compels services to adopt suitable means to safeguard uploader's rights and freedoms, Article 22(4) GDPR additionally requires that

uploader's sensitive data only be processed where it is necessary on substantial public interest grounds (ICO 2018a). Notably, when assessing whether services can rely upon legitimate interest as a lawful basis for uploader data processing, Article 6(1)(f) GDPR does not expressly specify what factors to consider. However, in *Rigas*[21] the CJEU suggested a three-part test. Firstly, is there a legitimate interest for processing? Here, OCSSPs would seem to have a legitimate interest in uploader data processing, specifically for implementing Article 17 of the CDSM. Secondly, is processing necessary to pursue a legitimate interest? This would also appear to be the case since Article 17 can only be implemented if uploader data is processed. Lastly, does the legitimate interest prevail over users' rights and freedoms? (ICO 2018a).

Engeler has correctly argued that in order for Article 17(4) of the CDSM Directive to be proportionate to the legitimate aim sought under Article 6(3) GDPR, upload filters must be compatible with the three parts of the CJEU's non-cumulative test contained in Article 52 (1) Charter (Engeler 2019). However, when it comes to the relationship between the ECHR and the Charter, it is worth noting that in *Tele2/Watson* the AG stressed that, to ascertain if human rights violations had taken place, it would not be legally adequate to impose a different test upon Member States based on whether the Convention or the Charter was being considered.[22]

Thus, arguably, whether the implementation of Article 17 of the CDSM Directive is lawful is largely determined by the compatibility of upload filters with the three parts of the ECtHR 's non-cumulative test. In sum, under the Convention, any interference with Articles 8 and 10 must firstly be 'in accordance with the law', secondly pursue one or more of the legitimate aims set out in Articles 8(2) and 10(2), and thirdly be 'necessary' and 'proportionate'. Importantly, a failure to comply with one part of the test constitutes an infringement regardless of whether the other two parts are satisfied (Cameron 2006, 105).

6. Assessment of applicability and compliance with Articles 8 and 10 of the ECHR

6.1. 'In accordance with the law'

Strasbourg Court case-law indicates that for any interference with the right to privacy and freedom of expression under Articles 8 and 10 ECHR to be 'in accordance with the law', three requirements must be met: firstly, it has to be based in domestic law; secondly, this law should be accessible; and lastly, it must also comply with the ECtHR's principles of foreseeability and rule of law.[23] The basis in domestic law requirement is easy to meet since Article 17 of the CDSM (written legislation) and the ECtHR's *Big Brother* case,[24] which examines filtering technology, provide this. However, regarding the second and third requirements, this section will argue that unless upload filters are targeted specifically at commercial-scale infringement, the implementation of Article 17 could fail to comply with the Court's accessibility, foreseeability and rule of law principles, thereby infringing the non-cumulative test's first-prong under Articles 8(2) and 10(2).

As far as the accessibility principle is concerned, it is well-settled Strasbourg Court case-law that the quality of the law requirement under Articles 8 and 10 of the Convention compels that legislation to be published, and thus it is sufficiently accessible to the

concerned individuals.[25] As noted above, Article 17(4)(b) of the CDSM states that if a licensing agreement is not concluded the OCSSP is liable unless it has made best efforts to guarantee the non-existence of specific content and 'other subject matter'. However, it is concerning that in conflict with *Big Brother*,[26] the CJEU's *Planet49*[27] decision and the transparency condition enshrined in Article 5(1)(a) GDPR, the description of the specific types of copyrightable works covered by Article 17 is neither sufficiently clear nor recognised in the CDSM Directive, thereby being inaccessible to the public. It is true that in *Sabam v Netlog*,[28] *Sabam v Scarlet*[29] and *McFadden*[30] the CJEU found that upload filters could monitor, filter and block copyrighted content such as audio-visual and music files. Worryingly, however, the CDSM Directive appears to ignore the fact that even if a registered audio or video of high commercial value might be detected, as explicitly required by Article 17(4)(b), it is not always possible for OCSSPs to uniquely identify all 'other' types of 'subject matter'. This is due to the difficulty of adapting content recognition and filtering to the content and the vast volume of material created that makes the production of a database of copyrighted content very troublesome. Indeed, a UGC service which permits users to upload written text, software code, images or files, including designs for 3D printing, has no technological capability to examine each upload for its unique features. Neither does there exist a database of tangible items against which it might compare such content (Gann and Abecassis 2018, 7, 9). Thus, since the vague text of the CDSM Directive does not specify in a form accessible to OCSSPs and uploaders the types of copyrightable works that Article 17 of the CDSM covers, it arguably fails to satisfy the ECtHR accessibility principle under Articles 8(2) and 10(2) ECHR.

In applying the foreseeability principle, the ECtHR case-law indicates that it requires a sufficiently precise formulation of the provision to allow any individual to adjust his conduct, as guaranteed by Articles 8 and 10.[31] As set out above, the CDSM Directive states that pursuant to Article 17(9) OCSSPs must inform users in their terms and conditions about copyright exceptions and limitations. Problematically, however, disregarding ECtHR[32] and CJEU[33] case-law and at odds with Article 14 and 15 GDPR, the CDSM Directive fails to mention, much less expressly safeguard, the uploaders' right to be informed and to access their personal data. Arguably, therefore, to ensure the CDSM Directive's compliance with Articles 14 and 15 GDPR, following *Planet49*,[34] OCSSPs should give uploaders specific 'privacy information' through clear and comprehensible just-in-time notices (ICO 2018b, 92, 97).

In addition to explaining the purpose for using upload filters (implementation of Article 17 of the CDSM Directive), these notices should clearly specify what type of uploader data OCSSPs collect and utilise before automated decisions are made about them and they end up being profiled as commercial-scale uploaders (ICO 2018b, 92, 98). For instance, based on Audible Magic's dataset above, this information would involve content data (media name), uploader traffic data (IP addresses and location) and metadata (distributor, producer and studio name, etc.) (European Patent Office 2014, 4–5). Furthermore, as per *Big Brother*[35] and *Planet49*,[36] these just-in-time notices should also clearly state what the likely impact of upload filters is, such as uploaders being profiled as commercial-scale infringers, being suspended and having all their uploaded content deleted. Lastly, according to Article 15 GDPR, such notices should additionally inform of, among other things,[37] the existence of the uploaders' right to request restriction, deletion or rectification, to object to data processing, and to lodge a complaint with a supervisory authority (ICO

2018b, 102). Indeed, in *Fashion ID* the CJEU held that for filtering technology to be lawful it was crucial to notify the audience target likely to become the subject of data collection, processing and profiling.[38] Thus, since Article 17 of the CDSM does not safeguard uploaders' right to be informed and to access their personal data, it arguably fails to satisfy the ECtHR foreseeability principle under Articles 8(2) and 10(2).

In terms of the rule of law principle, the Strasbourg Court case-law indicates that surveillance and technical measures must be subject to robust independent supervision and appropriate safeguards.[39] As mentioned above, Article 17(10) of the CDSM states that the EC must organise stakeholder discussions to consider best practices for collaboration among rightholders and OCSSPs. However, regrettably, ignoring ECtHR[40] and CJEU[41] case-law, the CDSM Directive neither provides independent oversight of upload filters nor gives uploaders effective safeguards against abuse. In *Sabam v Netlog*[42] and *Sabam v Scarlet*[43], the CJEU found that upload filters could detrimentally affect not only uploaders in terms of their right to protection of personal data and freedom of expression due to overbroad monitoring, filtering and blocking (under Articles 8 and 11 EU Charter), but also the freedom of hosting services such as, OCSSPs to conduct their business because of the computational complexity and costs of these filters (under Article 16 EU Charter). Thus, since the implementation of Article 17 might inevitably lead to legal problems, such as IP, data protection, free speech and competition issues, the CDSM Directive should explicitly require the cooperation of all concerned state authorities and regulators.[44]

Moreover, in agreement with the European Data Protection Supervisor (EDPS 2010, 8), UN Special Rapporteur David Kaye stressed that, in addition to conducting human rights impact assessments and public consultations on upload filters, developers such as Audible Magic should make all filtering criteria fully auditable, allowing regular external and independent auditing and the publishing of results (UNHRC 2018, 19–20). Importantly, this is consistent with Article 35 GDPR which requires services to complete Data Protection Impact Assessments (DPIAs). Indeed, these DPIAs show that appropriate safeguards are in place regarding data processing operations, which are 'likely to result in high risk', such as the tracking of uploaders' behaviour and location to establish commercial-scale online copyright infringement (ICO 2018c). Thus, given that in contrast to requiring cross-sector state authority cooperation and appropriate safeguards the CDSM Directive only requires stakeholder dialogues to consider best practices for cooperation, it is arguable that it fails to satisfy the ECtHR rule of law principle under Articles 8(2) and 10(2).

6.2. Legitimate aim

According to Articles 8(2) and 10(2), state authorities can rely on several expressly set out legitimate interests as a basis for interfering with the right to privacy and freedom of expression under the Convention. These include domestic security, public safety or the economic well-being of the country, the prevention of crime or disorder, and the protection of the reputation or rights and freedoms of others.[45] States normally have no difficulty in satisfying the legitimate aim test, thus complying with the second-prong of the Court of Strasbourg's non-cumulative test. It is arguable that the deployment of technology, such as notice and staydown or upload filters systems, could potentially achieve the prevention of crime or disorder and the protection of the reputation or rights and freedoms of others.

Indeed, the ECtHR explicitly recognised this in its ruling involving the Pirate Bay administrators in *Sunde v Sweden*.[46]

6.3. 'Necessary' and 'proportionate'

The next matter to be assessed in this paper is whether the implementation of Article 17 of the CDSM Directive would comply with the third prong of the Court of Strasbourg's test. The ECtHR's case-law indicates that under Articles 8(2) and 10(2) of the Convention monitoring, filtering and blocking means are 'necessary' in a democratic society if they respond to a 'pressing social need' and are proportionate to the legitimate aim pursued.[47] Moreover, the Court has noted that the grounds given by the state to justify such means need to be 'relevant and sufficient'.[48] Yet, whilst state authorities enjoy a margin of appreciation, the ultimate assessment as to whether these means remain necessary and proportionate is subject to judicial review in Strasbourg.[49] This section will argue that the use of upload filters does not comply with the principles of necessity and proportionality.

In terms of the first principle, it is well-settled ECtHR case-law that under Articles 8(2) and 10(2) ECHR the degree of intrusion of a measure is one key consideration when evaluating whether the means adopted might be considered necessary to achieve the legitimate aim sought.[50] As noted above, the CDSM Directive states that the implementation of Article 17 must not result in Member States imposing on OCSSPs a general monitoring obligation. Alarmingly, however, the CDSM Directive fails spectacularly to explain how Article 17 could be implemented in a less data processor-intrusive way for OCSSPs and minimally impact uploaders' rights. In *Sabam v Netlog*[51] and *Sabam v Scarlet*[52] the CJEU held that, pursuant to Article 15 E-Commerce Directive, in order to assess whether upload filters led to general monitoring obligations being imposed on services, it was necessary to evaluate whether such services were required to actively monitor 'all the data' of 'all users' to prevent 'any' future copyright violation. Therefore, while this is the most common way to implement upload filters, it remains legally questionable to apply such a method to 'all' files because of the data processor-invasive nature of these filters. Consequently, consistent with the CJEU decision in *Glawischnig-Piesczek v Facebook*,[53] for general monitoring obligations to become lawful 'duties of care' and 'specific' enough to comply with Recitals 47 and 48 E-Commerce Directive, OCSSPs should deploy a hierarchical identification technique. Moreover, rightholders should create databases of 'relevant and necessary information' along with business rules that exclusively tackle commercial-scale copyright infringement. This would also support further case-law of the Strasbourg[54] and Luxembourg[55] courts.

Accordingly, the suggested proposal would entail first a qualitative assessment based on the nature of the registered content, and second a quantitative assessment depending upon whether a source IP address creates a history of unlawful uploads, and, if so, whether the file type is consistent with past unlawful uploads (European Patent Office 2014, 9), thereby reaching the commercial-scale threshold. Therefore, since the suggested specifically targeted uploader monitoring obligation aimed at commercial-scale infringers would have significantly less impact on OCSSPs and uploader rights, arguably the CDSM Directive fails to satisfy the ECtHR necessity principle under Articles 8(2) and 10(2).

Regarding the proportionality principle, it is also well-established in ECtHR case-law that the scope and application of monitoring, filtering and blocking measures must be appropriate under Articles 8(2) and 10(2) ECHR.[56] As set out above, the CDSM Directive states that when assessing proportionality, the evolving state of the art regarding current means should also be considered, including possible future developments. Controversially, however, ignoring the ECtHR[57] and CJEU[58] case-law, Article 17 of the CDSM Directive is neither limited in scope, nor in time nor in the specific type of uploaders being profiled. Importantly, DPI technology filters content based on, for example, keywords and/or traffic features (Internet Society 2017, 14). Therefore, consistent with Article 15 E-Commerce Directive, the suggested hierarchical identification technique would require OCSSPs to detect through passive monitoring and then filter, first, keywords, that is, registered titles of high-value commercial copyrighted content, second, suspect source IP addresses and, lastly, traffic features, specifically, the number and frequency of unlawful downloads. Thus, the CDSM Directive should only target DPI devices at the proposed keywords and traffic features.

Moreover, Audible Magic explicitly acknowledges that its upload filter's process launches automatically and runs in the background '24 hours a day, seven days a week' (Audible Magic 2017, 51). However, in addition to *Planet49*[59], this also notably conflicts with Strasbourg Court case-law which stresses that the use of never-ending surveillance and technical measures constitute prior restraint, thereby contravening the ECHR.[60] The CDSM Directive should also expressly limit the duration of these measures. Lastly, according to Article 22(1) GDPR, the deployment of upload filters simply based on evidence of copyright infringement is an automated decision-making process which does not necessarily entail profiling. However, under Article 4(4) GDPR, it would become a decision based on profiling if, as suggested above, uploading behaviour is monitored over time to establish commercial-scale copyright infringement (Working Party 2018, 8). The CDSM Directive should also expressly recognise the type of users being subjected to profiling, such as commercial-scale uploaders. Thus, since the CDSM Directive does not set out explicitly the scope and application of the measures, it arguably fails to satisfy the ECtHR proportionality principle under Articles 8(2) and 10(2).

In applying the principle of proportionality, the Strasbourg Court has elaborated that the evaluation of the legality of surveillance and technical measures must also take into consideration the seriousness of the infringement.[61] As flagged above, the CDSM Directive states that, depending on the type of work, distinct means to prevent unlawful material could be adequate and proportionate.[62] However, it is concerning that in conflict with the ECtHR[63] and CJEU[64] case-law the CDSM Directive fails to address, much less explicitly detail, the type of content and number and frequency of uploads that result in commercial-scale copyright infringement. Referring to the suggested proposal above, the identification of commercial-scale uploaders would involve the sum of qualitative and quantitative parts. First, the initial prong of the test would originally require rightholders to exclusively register in a database content of high commercial value. This would consider both 'production value', namely, whether the content was generated with low or high production cost, and 'expected sales rank', that is, based on past duration and position in top-100 charts (Erickson and Kretschmer 2018, 83–84). Subsequently, concerning the quantitative assessment or test's second prong, this entails interrogating a database for suspect source IP addresses involved in past unlawful uploads (European Patent Office 2014, 9).

Moreover, importantly, following CJEU *L'Oréal v eBay*,[65] it involves recording their number and frequency. The assumption is that if a specific source IP address creates a history of similar past unlawful uploads (at least three infringements in one month as suggested by Sawicki), then there is a high probability that uploads originating from that source IP address include unlawful material (European Patent Office 2014, 9). The rationale behind this suggested commercial-scale threshold is that uploaders flagged as repeat infringers would be automatically notified[66] at least three times by their OCSSPs concerning the risks of further infringement (Sawicki 2006, 1483). Arguably, this by itself is sufficient to reach the commercial-scale threshold, thus blocking the upload. As such, as the CDSM Directive does not require the exclusive targeting of high commercial value content and previously notified and identified commercial scale uploaders, a case can be made that it fails to satisfy the ECtHR proportionality principle under Articles 8(2) and 10(2).

7. Assessment of applicability and compliance with Article 6 of the ECHR

Having found that, as currently drafted, Article 17 of the CDSM Directive may neither be 'in accordance with the law' nor 'necessary' nor 'proportionate' under Articles 8 and 10 of the Convention, the last issue to be examined in this paper is whether the deployment of upload filters would also infringe the Strasbourg Court's principle of presumption of innocence under Article 6 ECHR. In *Engel v the Netherlands*, the ECtHR set out a three-prong, non-cumulative test for examining the applicability of the criminal head of Article 6 ECHR, which entailed interrogating the classification of an alleged offence in the domestic law, the nature of the offence and the nature and degree of gravity of the sanction.[67] The CDSM Directive does not expressly refer to criminal penalties for copyright infringement as such. However, the EC's Recommendation on measures to effectively tackle illegal content online suggests a collective response to proactively identify, eliminate and prevent the reuploading of unlawful material. It warns that if there is proof of a grave criminal offence, services should quickly notify law enforcement authorities (EC 2018). Thus, upload filter deployment would also cover criminal cases.

7.1. Compatibility of Article 17 of the CDSM Directive with the ECtHR principle of presumption of innocence

Article 6(2) ECHR states that a defendant must be presumed innocent of a criminal offence until proven guilty according to law. The ECtHR's case-law indicates that this means that the defendant is given the benefit of doubt and the burden of showing his guilt rests with the prosecution.[68] In *Salabiaku v France*, the ECtHR stressed that under the Convention the burden of proof could shift to the defendant. However, regarding criminal law, it set out a three-prong test to assess the compliance of such reverse onus provisions with Article 6(2) Convention. Specifically, it required Member States to: remain within reasonable limits; consider the importance of what was at stake; and, protect the rights of the defence.[69]

In terms of the test's first prong, the Strasbourg Court initially explained that for reverse onus provisions to satisfy Article 6(2) ECHR, Member States had to remain within reasonable limits.[70] As noted above, the CDSM Directive states that allowing copyright exceptions and limitations is key to striking a balance between freedom of expression, IP and

freedom of the arts under the Charter.[71] However, troublingly, disregarding ECtHR[72] and CJEU[73] case-law, the CDSM Directive seems to overlook the fact that the balancing test must always be conducted fairly, due regard being had to 'all' competing interests at stake including uploaders' Article 7 and 8 Charter rights. Importantly, when evaluating the likely content being transmitted and asking databases for suspect source IP addresses, that is, repeat copyright infringers, the suggested proposal entails an element of prediction. Therefore, this would increase the risk of false positives as the input data (the personal data utilised to generate the commercial-scale uploader profile) and the output data (the profile itself) could be flawed. For example, in addition to content identification mistakes linked to algorithmic design, concerns with data quality, and the lack of a mechanism for evaluating whether the alleged infringing content is a parody, review or criticism, it is also worrisome the way in which services publish metrics to assess upload filters' effectiveness (Lester and Pachamanova 2017, 63–66). Indeed, the CJEU case-law strongly indicates that to ensure a fair balance between competing fundamental rights, while 'clear evidence' of copyright infringement was critical (*Bonnier Audio*[74]), upload filters should not prevent users from legally accessing content (*UPC Telekabel*[75]). Thus, arguably, to achieve GDPR compliance uploaders should not only be able to exercise their right to rectification, erasure and restriction of processing under Articles 16, 17 and 18 GDPR, but also, pursuant to Article 21(1) GDPR, additionally object to erroneous profiling[76] and receive compensation as provided in Article 82 GDPR. Thus, since when conducting the balancing test the CDSM Directive does not appreciate that uploaders' GDPR rights are also crucial, it is debatable whether it could infringe the ECtHR's presumption of innocence principle under Article 6(1) ECHR.

As far as the second prong of the test is concerned, the ECtHR observed that for reverse onus provisions to satisfy Article 6(2) ECHR, Member States also had to consider the importance of what was at stake.[77] As mentioned above, Article 17(9) of the CDSM Directive states that Member States must require OCSSPs to provide for an expeditious and effective complaint and redress mechanism for users to challenge rightholders' requests to remove or disable access to content. Controversially, however, the CDSM Directive fails to address, much less expressly recognise, that to enable matching of content the creation of centralised databases of copyrighted material is critical to successful upload filter performance (Gann and Abecassis 2018, 4). In *Sabam v Netlog*[78] and *Sabam v Scarlet*[79], the CJEU held that as staydown injunctions compelled services to deploy costly, complex, permanent upload filters at their own expense, this violated the freedom to conduct their business under Article 16 Charter. Therefore, one might argue that unless databases were centralised and exclusively targeted music and video with high-commercial value content, the implementation costs of Article 17 could dramatically increase. This is because it would be essential to compare every fingerprint against numerous databases for numerous rightholders[80] and numerous types of material.

Within industries where fragmentation is reduced, such as in the music industry, rightholders are generally able to combine efforts to create centralised databases. However, for most other types of content, such as images, databases tend to be rightholder-specific and fragmented. Moreover, since the OCSSP would need to deploy multiple upload filters to individually detect every work, the use of each supplementary database would thus duplicate Article 17 implementation expenses (Gann and Abecassis 2018, 7, 9, 11, 12). Indeed, this notably conflicts with *United v Commission*[81] and *NV v Commission*[82] where the CJEU

found that Article 86 of the Treaty on the Functioning of the EU (TFEU) reflected the main goal of Article 3(f) TFEU, namely, adopting a framework which ensured that common market competition was never distorted.[83] Thus, since Article 17 of the CDSM would harm competition and stifle innovation, arguably it could contravene the ECtHR's principle of presumption of innocence under Article 6(2) ECHR.

In applying the test's third prong, the ECtHR added that for reverse onus provisions to satisfy Article 6(2) ECHR, Member States also had to safeguard the rights of the accused.[84] As stated above, Article 17(9) of the CDSM asserts that Member States must establish out-of-court redress systems that allow disputes to be decided independently, but without affecting uploaders' rights to go to domestic courts to use copyright exceptions or limitations. However, alarmingly, in conflict with ECtHR[85] and CJEU[86] case-law, the CDSM Directive does not afford uploaders an effective remedy since it lacks the supervisory authorities' power to investigate complaints regarding human rights violations. Notably, following the legitimate interest test for data processing in the CJEU's *Rigas* case,[87] under Article 6(1)(f) GDPR uploader profiling would be necessary if the OCSSP's interests were to prevail over the uploader's fundamental rights (Working Party 2018, 14).

The initial aspect to examine in the balancing exercise is the level of detail of the profile, such as whether an uploader is being broadly categorised as alleged copyright infringer or instead being specifically labelled a commercial-scale uploader. A further step is to assess the comprehensiveness of the profile. This can be done, for example, by considering whether the profile is based on a narrow feature of the uploader, such as repeatedly uploading registered titles of high commercial value, or more problematically – as expressly recognised in the EC Impact Assessment – the profile reflects a more comprehensive view based on 'real-time' statistics of what uploaders browse, how they watch films or listen to music, so that all this data are analysed and then utilised for targeted display advertising (EC 2016, 164–165). Additionally, the next step is to assess the profiling's impact. Considering the Facebook-Cambridge Analytica scandal, examining the above 'real-time' statistics to create the profile means that the impact on uploaders would be significant. Lastly, the balancing test ultimately requires there to be appropriate safeguards against abuse (Working Party 2018, 14), such as uploader profiling being subject to cross-sector state authority oversight.[88] Thus, since the CDSM Directive fails to protect the defence's rights, a case can be made that it could infringe the ECtHR's presumption of innocence principle under Article 6(1).

8. Discussion of findings

In the internet era the impact of upload filters on human rights has become a central issue for legal scholarship. A growing body of research has investigated whether, relying on human rights as a benchmark, Article 17 of the CDSM Directive is a lawful response to the problem of online copyright infringement (Frosio and Mendis 2019; Geiger and Izyumenko 2019; Grisse 2019; Husovec 2019; Quintais et al. 2019; Senftleben 2019). Surprisingly, however, little research has been conducted on the compatibility of Article 17 of the CDSM Directive with Articles 6, 8 and 10 ECHR, the E-Commerce Directive and the GDPR. This paper has sought to fill an existing gap in the literature, suggesting that, in order for Article 17 to respect these instruments, upload filters must be targeted specifically at commercial-scale infringement. The findings of this paper are consistent with

the case-law of the Strasbourg and Luxembourg courts. In *Mouvement v Switzerland*, the ECtHR emphasised that while there was hardly room under the right to freedom of expression for interferences with political speech or debate, if Article 10 Convention involved 'commercial speech', domestic courts were given a specially broad margin of appreciation in determining whether a fair balance had been struck.[89] Similarly, in *Coöperatieve v Deepak*, the CJEU confirmed that if services were exempted from liability, they could, pursuant to Article 14(3) E-Commerce Directive, target at the individual concerned, where infringements of IP rights had been demonstrated to the required legal standard, action aimed at stopping those infringements or preventing that possibility.[90]

Moreover, the paper's findings might also have an economic and societal impact. But before this impact is considered, the question remains as to whether specifically targeting uploader monitoring obligations at infringement of copyright on a commercial-scale is worth the cost. Since the size of a fingerprint database generally increases as time passes, it may not be necessary to compare newly uploaded material against 'all' fingerprints, which could be expensive as all uses would exclusively involve registered content of high commercial value (Japiot 2017, 21). In satisfying the stakeholder discussions requirement contained in Article 17(10) of the CDSM Directive, a potential practical solution for the implementation of Article 17 would be to design an 'active' fingerprint database that omits the copyrighted material, which is no longer expected to be the origin of a sufficient number of matches (Japiot 2017, 21). Accordingly, to optimise the use of the means, anticipated performance might be determined by OCSSPs and rightholders, thereby helping the standardisation of best practices for cooperation. Moreover, Article 17(10) of the CDSM additionally requires bearing in mind the interests of all relevant stakeholders and user safeguards. Therefore, since the OCSSP would obtain a percentage of the ad revenue, it would also have a reason to encourage rightholders to favour monetisation over blocking. In practice, costs might be negotiated on a case-by-case basis depending upon the number of matches made against the fingerprint database and its size (Japiot 2017, 21). An upload filter of this nature that could specifically target the most widely shared high commercial value content could potentially be introduced into the EC's advice on the adoption of Article 17, expressly laid down in the CDSM Directive.

Furthermore, in terms of societal impact, apart from tackling copyright infringement, Audible Magic has shown how notice and staydown systems can also be designed to monitor, filter and block matters such as pornography, terrorism, questionable content, terms of use infringements, hate speech and so on (Audible Magic 2017, 32). Thus, as flagged above, rather unsurprisingly, the literature warns of the EC's intention to increase the adoption of upload filters by addressing these specific content-related concerns (Frosio and Mendis 2019, 17; Heldt 2019, 4–9; Kuczerawy 2019, 2). However, caution should be taken not to use upload filters for multiple purposes, since arguably the deployment of DPI not only to filter but also alter content might well result in worrisome unintended consequences. Yet, whilst it is evident that the process of filtering and changing content as the packets travel across the network has been employed for behavioural advertising,[91] it is a concern that packet modification could take internet censorship into a whole new dimension. For instance, in a hypothetical scenario, by deploying a DPI device the EC could alter any packets passing through EU networks. The EC could even create a signature for TorrentFreak posts which included views it deemed censorable and utilise DPI to rewrite such posts while passing over these networks. Either including

some fabricated statements in a TorrentFreak news article, such as 'UN Human Rights Rapporteur: upload filters "disproportionate response" to copyright infringement', or simply deleting its most controversial details, would be significantly more powerful than even blocking https://torrentfreak.com/ itself.

In fact, any such alterations could just be realised within EU networks and could even be set up to take place exclusively in specific areas of Europe. Worryingly, this sophisticated process of filtering and altering information as the packets travel across the network would be immensely hard to uncover and would equally make it remarkably difficult to differentiate between the authentic and the censored European variation (Wagner 2009, 9–10). Yet, this is the fundamental reason why the designers of the futuristic OpenAI system, which can create limitless deepfakes for text including negative and positive customer reviews, spam and fake news that are sufficiently persuasive to be plausible as human creations, decided to raise the alarm. Indeed, perhaps not surprisingly, the public has already been alerted to the fact that the technology is too dangerous to release for fear of its potential abuse (*The Guardian News*, February 14, 2019).

9. Conclusion

This paper has critically evaluated the extent to which Article 17 of the CDSM Directive could be implemented in a way which is compatible with the right of OCSSPs and uploaders to a fair trial, privacy and freedom of expression under Articles 6, 8 and 10 of the ECHR, the E-Commerce Directive and the GDPR. I conclude that unless, pursuant to the stakeholder discussions provision laid down in Article 17(10) of the CDSM Directive, the procedural safeguards suggested below are considered, the adoption of upload filters will violate OCSSPs and uploaders' Articles 6, 8 and 10 Convention rights, the E-Commerce Directive and the GDPR. Thus, it is suggested that, in addition to the invaluable user freedoms proposed by the literature (Quintais et al. 2019), a human rights-compliant response to future Article 17 implementation, which can potentially help the standardisation of the EC's best practices guidance for cooperation, would be for the EC to take on board the following recommended safeguards.

- Since it is in conflict with the ECtHR principle of accessibility, the description of the specific types of copyrightable works covered by Article 17 is neither sufficiently clear nor acknowledged in the CDSM Directive. The first procedural safeguard should therefore be for the different types of works to be protected to be specifically set out, thereby being made accessible to the public.
- By disregarding the ECtHR principle of foreseeability, Article 17 fails to mention, much less explicitly safeguard, uploaders' Article 8 EU Charter rights. The second procedural safeguard should be that uploaders have the right to be informed about the gathering and use of their personal and sensitive data and also access their data under Articles 14 and 15 GDPR.
- At odds with the ECtHR principle of rule of law, Article 17 neither provides independent oversight of upload filters nor gives uploaders effective safeguards against abuse. The third procedural safeguard should be for the use of upload filters to be subject to

independent supervision and appropriate safeguards, such as conducting human rights impact assessments, public consultations and regular audits.

- In conflict with the ECtHR principle of necessity, the CDSM Directive fails spectacularly to explain how Article 17 could be implemented in a less data processor-intrusive way for OCSSPs and minimally impact uploaders' rights. The fourth procedural safeguard should be for OCSSPs to deploy a hierarchical identification technique, have rightholders' design databases of 'relevant and necessary information', and include business rules that exclusively tackle commercial-scale online copyright infringement.
- In the way it ignores the ECtHR principle of proportionality, Article 17 is neither limited in scope, nor in time nor in the specific type of uploaders to be profiled. The fifth procedural safeguard should be for upload filters to only target DPI devices at the suggested keywords and traffic features. Moreover, the duration of its surveillance and blocking measures should be limited as well as the types of users being subjected to profiling, such as commercial-scale uploaders.
- At odds with the ECtHR principle of proportionality, Article 17 fails to address, much less explicitly detail, the type of content and number and frequency of uploads, and this without taking due account of the commercial-scale threshold. The sixth procedural safeguard to be implemented is that the deployment of upload filters should exclusively target high commercial value content and previously identified and notified commercial-scale uploaders.
- In conflict with the first prong of the ECtHR *Salabiaku v France* test, Article 17 disregards the fact that the balancing test must always be carried out fairly, with due regard being given to 'all' competing interests at stake. A further procedural safeguard to be adopted is that uploaders should exercise their right to rectification, erasure, restriction of processing, and so object to erroneous profiling and receive compensation under the GDPR.
- In ignoring the second prong of the ECtHR *Salabiaku v France* test, Article 17 fails to consider, much less explicitly acknowledge, that to enable matching of content the creation of centralised databases of copyrighted material is crucial. An additional procedural safeguard to be applied is that copyright databases should be centralised and made to exclusively target music and video with high-commercial value content.
- Finally, at odds with the third prong of the *Salabiaku v France* test, Article 17 of the CDSM Directive lacks the supervisory authorities' power to investigate complaints regarding human rights abuses. The last procedural safeguard should be for the profiling of uploaders to be made compatible with the legitimate interest test for data processing in the CJEU's *Rigas* case.[92]

At a time when Article 17(10) is the most carefully thought-out provision laid down in the CDSM Directive, which might ensure that a fair balance is struck between all the fundamental rights at stake concerning rightholders, OCSSPs, uploaders, as well as customers and human rights organisations, the EC would be ill-advised not to take on board these recommended safeguards. In my view, if these are not introduced into the EC's best practice guidance for the implementation of Article 17, no other position it could take would have a more incendiary effect since the CDSM Directive would be violating the rights of OCSSPs and uploaders under Articles 6, 8 and 10 of the Convention, the E-Commerce Directive and the GDPR.

Notes

1. C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458 [46].
2. Joined cases C-236/08 C-237/08 and C-238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL* [2010].
3. C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000.
4. C-401/19 *Poland v Parliament and Council* case being referred to CJEU (pending); C-682/18 *YouTube* case being referred to CJEU (pending); C-683/18 *Elsevier* case being referred to CJEU (pending).
5. C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458 [53].
6. C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000.
7. C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4.
8. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [121]; *James and Others v the United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) [51]; *Uzun v Germany* App no 35623/05 (2010) 53 EHRR 852 [78]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [64].
9. C-287/11 *Aalberts Industries NV and Others v European Commission* [2013] EUECJ [54]-[57]; C-443/13 *Ute Reindl v Bezirkshauptmannschaft Innsbruck* [2014] EUECJ [39]; C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] EUECJ [120]-[122].
10. Recital 53 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance) PE/51/2019/REV/1 OJ L 130, 17.5.2019, p. 92–125.
11. Advocate General's Opinion in C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [AG footnote 31].
12. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [121]; *James and Others v the United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) [51]; *Uzun v Germany* App no 35623/05 (2010) 53 EHRR 852 [78]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [64].
13. C-287/11 *Aalberts Industries NV and Others v European Commission* [2013] EUECJ [54]-[57]; C-443/13 *Ute Reindl v Bezirkshauptmannschaft Innsbruck* [2014] EUECJ [39]; C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] EUECJ [120]-[122].
14. For case-law concerning the harm caused to the rightholder see for instance *Neij and Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013); C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB* [2012] 2 CMLR 42 [49], [58].
15. For case-law concerning the gravity of the offence see for instance *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [137]; *Neij and Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013); C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [33]–[34]; see also C-70/10 *Scarlet Extended SA v Société´ belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [35]–[48].
16. For case-law concerning the user notification requirement see for instance *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [133]; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [121].
17. For case-law concerning users' right to challenge see for instance *Dombo Beheer BV v The Netherlands* App no 14448/88 (1993) 18 EHRR 213 [33]; *Ankerl v Switzerland* App no 17748/91 (1996) ECHR 45 [38]; *Bulut v Austria* App no 17358/90 (1996) ECHR 10 [47]; *Niderost-Huber v*

Switzerland App no 18990/91 (1997) ECHR [23]; C-314/12 *UPC Telekabel Wien GmbH v Constantin FilmVerleih GmbH and Wega Filmproduktionsgesellschaft GmbH* [2013] [66].

18. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [121]; *James and Others v the United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) [51]; *Uzun v Germany* App no 35623/05 (2010) 53 EHRR 852 [78]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [64].
19. C-287/11 *Aalberts Industries NV and Others v European Commission* [2013] EUECJ [54]-[57]; C-443/13 *Ute Reindl v Bezirkshauptmannschaft Innsbruck* [2014] EUECJ [39]; C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] EUECJ [120]-[122].
20. C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458 [46].
21. C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme* [2017] 4 WLR 97 [28]-[32].
22. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [AG 142].
23. *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [52]; *Kennedy v the United Kingdom* App no 26839/05 (2010) 52 EHRR [151]; *Liberty and others v the United Kingdom* App no 58243/00 (2008) 48 EHRR 1 [59]; *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [120]–[122];*Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [57].
24. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [329], [346], [387].
25. *Liberty and others v the United Kingdom* App no 58243/00 (2008) 48 EHRR 1 [59]; *Kennedy v the United Kingdom* App no 26839/05 (2010) 52 EHRR [151]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [57].
26. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [305], [313]; see also *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [52]; *S and Marper v the United Kingdom* (2009) 48 EHRR 50 [95].
27. C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] EU:C:2019:246 [74], [75].
28. C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [53].
29. C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [55].
30. C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] [25], [87].
31. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [204].
32. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [133].
33. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [121].
34. C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] EU:C:2019:246 [74], [75].
35. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [310].
36. C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] EU:C:2019:246 [74], [75].
37. Also (i) the purpose of processing that is, being necessary for compliance with a legal obligation, namely, the implementation of Article 17; (ii) the categories of personal data concerned, for example, uploaders' personal data such as, source and destination IP addresses and location, along with sensitive data such as, content/media name; (iii) the storage period for retaining uploader's personal data.
38. C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] [36]; see also AG Opinion in the same case [AG 57].

39. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110], [122]; *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59]; see also *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60].
40. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [318]; *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110]; *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59], [122]; see also *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60].
41. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123]; C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] [17].
42. C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [46]-[51].
43. C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [48]-[53].
44. On 24 January 2020, the UK Government decided not to implement the CDSM Directive into UK domestic law including its Article 17. However, in a hypothetical scenario, supposing that Article 17 had already been implemented in the UK, this would probably have been required cross-sector cooperation between four authorities. Specifically, the Intellectual Property Office (intellectual property authority), the Information Commissioner's Officer (data protection authority), Ofcom (communications regulator), and the Competition and Markets Authority (competition authority).
45. *Golder v the United Kingdom* App no 4451/70 (1979) 1 EHRR 524 [44].
46. *Neij and Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013).
47. *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [78]; *Cenzig and others v Turkey* App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015) [58]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [56]; *S and Marper v the United Kingdom* App no 30562/04 and 30566/04 (2008) ECHR 1581 [101]; *Peck v the United Kingdom* App no 44647/98 (2003) 36 EHRR 41 [76]; *Khurshid Mustafa and Tarzibachi v Sweden* App no 23883/06 (ECtHR, 16 March 2009) [42].
48. *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [78]; *S and Marper v the United Kingdom* App no 30562/04 and 30566/04 (2008) ECHR 1581 [101]; *Peck v the United Kingdom* App no 44647/98 (2003) 36 EHRR 41 [76]; *Khurshid Mustafa and Tarzibachi v Sweden* App no 23883/06 (ECtHR, 16 March 2009) [42].
49. *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [78]; *S and Marper v the United Kingdom* App no 30562/04 and 30566/04 (2008) ECHR 1581 [101]; *Coster v the United Kingdom* App no 24876/94 (2001) 33 EHRR 20 [104]; *Khurshid Mustafa and Tarzibachi v Sweden* App no 23883/06 (ECtHR, 16 March 2009) [43].
50. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [121]; *James and Others v the United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) [51]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [64]; *Uzun v Germany* App no 35623/05 (2010) 53 EHRR 852 [78].
51. C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [33]-[38].
52. C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [35]-[40].
53. C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* [2019] EU:C:2019:458 [34], [42].
54. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [121]; *James and Others v the United Kingdom* App no 8793/79 (ECtHR, 21 February 1986) [51]; *Uzun v Germany* App no 35623/05 (2010) 53 EHRR 852 [78]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [64].
55. C-287/11 *Aalberts Industries NV and Others v European Commission* [2013] EUECJ [54]-[57]; C-443/13 *Ute Reindl v Bezirkshauptmannschaft Innsbruck* [2014] EUECJ [39]; C-83/14 *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia* [2015] EUECJ [120]-[122].

56. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [140]–[141]; Concurring Opinion in *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) page 29; see also *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [159].
57. *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [59]; see also Concurring Opinion in *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013), 27–28.
58. C-70/10 *Scarlet Extended SA v* Société belge des auteurs, *compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 see final holding; see also Advocate General's Opinion in C-70/10 *Scarlet Extended SA v* Société belge des auteurs, *compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [AG 53]–[AG 59].
59. C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019] EU:C:2019:246 [78], [81].
60. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [140]–[141]; see also Concurring Opinion in *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) page 28.
61. *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [137]; *Neij and Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013); *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [115]; *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [159]; *Uzun v Germany* (App no 35623/05) (2010) 53 EHRR 852 [80].
62. Recital 66 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) PE/51/2019/REV/1 OJ L 130, 17.5.2019, p. 92–125.
63. *Akdeniz v Turkey* App no 20877/10 (ECtHR, 11 March 2014) [25]-[26]; *Mouvement* raëlien suisse *v Switzerland* App no 16354/06 (2012) ECHR 1598 [61]-[62]; *Neij and Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013).
64. Advocate General's Opinion in C-275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 119]; C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000 [55].
65. C-324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000 [55].
66. For case-law concerning the user notification requirement see for instance *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [133]; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [121].
67. *Engel and others v the Netherlands* (App no 5100/71, 5101/71, 5102/71, 5354/72, 5370/72) (1976) 1 EHRR 647 [82].
68. *Barberà, Messegue and Jabardo v Spain* (App no10590/83) (1988) 11 EHRR 360 [77].
69. *Salabiaku v France* App no 10519/83 (1988) 13 EHRR 379 [28].
70. *Ibid*.
71. Recital 70 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) PE/51/2019/REV/1 OJ L 130, 17.5.2019, p. 92–125.
72. *Ashby Donald and others v France* App no 36769/08 (2013) ECHR 287 [40]; *Chassagnou and Others v France* App nos 25088/94, 28331/95 and 28443/95 (1999) 29 EHRR 615 [113].
73. C-275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [68]; C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [42], [47], [48]; C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [46], [49], [50].
74. C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB* [2012] 2 CMLR 42 [49], [58].
75. C-314/12 *UPC Telekabel Wien GmbH v Constantin FilmVerleih GmbH and Wega Filmproduktionsgesellschaft GmbH* [2013] [66].
76. Based on Article 6(1)(e) or (f) of the GDPR.

77. *Salabiaku v France* App no 10519/83 (1988) 13 EHRR 379 [28].
78. C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECR I-0000 [46], [47].
79. C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [48], [49].
80. For instance there can be multiple rightholders engaged in the same portion of material such as, in video content, the producer, the director, the script writer and music suppliers all have rights; also there can be multiple concurrent non-exclusive licensees: crucially, it is only possible to filter based on an exclusive right such as, if a broadcaster has concluded a music licence agreement for phono rights from the PPL, which does not enable it to block content page – see (Gann and Abecassis 2018, 4).
81. C-27/76 *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* [1978] ECR 207 [24].
82. C-322/81 *NV Nederlandsche Banden Industrie Michelin v Commission of the European* Communities [1983] ECR 3461 [29].
83. See also C-52/09 *Konkurrensverket v TeliaSonera Sverige AB* [2011] [2011] ECR I-527 [20]-[22].
84. *Salabiaku v France* App no 10519/83 (1988) 13 EHRR 379 [510].
85. *Big Brother Watch and others v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (2018) ECHR 299 [510].
86. C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] [44], [58]; C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy* [2017] EUECJ [54]-[55]; C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] EUECJ [47].
87. C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme* [2017] 4 WLR 97 [28]-[32].
88. In this context, state authorities should take into account the UN Special Rapporteur on freedom of expression, which recommends that information be published frequently on the regularity at which upload filter decisions are subject to complaints, and the types, requests and effectiveness of remedies available. Specifically, how much content upload filters remove, how frequently human moderators authorise upload filter removals, how often these removals are disputed and how regularly challenges are approved. David Kaye concludes that developers should lastly be transparent about the reliability of metrics to evaluate upload filters' effectiveness, well-known failure scenarios such as, false positives in fair dealing cases and content identification problems associated with data quality and algorithmic design. See UNHRC (2018).
89. *Mouvement raëlien suisse v Switzerland* App no 16354/06 (2012) ECHR 1598 [61]-[62].
90. C-521/17 *Coöperatieve Vereniging SNB-REACT U.A. v Deepak Mehta* [2018] EUECJ [51]; see also C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* [2016] [77], [78], [94]; equally, the EDPS agrees that following the commercial scale rule included within Article 8 of Directive 2004/48/EC, the random monitoring of a user's behaviour, concerning not-for-profit, minor and small-scale infringement, is disproportionate and in violation of Article 8, of the Convention, Articles 7 and 8 of the Charter, and the Data Protection Directive – see (EDPS 2012, 7).
91. Since content recognition and filtering technology also allows, among other things, the gathering of user personal data, the placement of synchronised ads on smart devices as well as the tracking of advertising broadcasts (Japiot 2017, 18), this arguably had a detrimental impact on both, the Brexit referendum and the US presidential election. For instance, in 2017 it was reported that relying on Facebook big data analytics, it is possible to model target specific groups of users and predict their behaviour, by ensuring the right political advertising messages are targeted to the right voters – see (Romero-Moreno 2019, 204).
92. C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme* [2017] 4 WLR 97 [28]-[32].

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Angelopoulos, C., and J.-P. Quintais. 2019. "Fixing Copyright Reform: A Better Solution to Online Infringement." *Journal of Intellectual Property, Information Technology and E-Commerce Law*. https://www.jipitec.eu/issues/jipitec-10-2-2019/4913.

Audible Magic. 2017. "Annex 1- Gestdem 2017/4050." https://www.asktheeu.org/en/request/4465/response/14429/attach/5/Annex%20I%20Gestdem%202017%204050%20v3.pdf.

Bridy, A. 2019. "The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3412249.

Cameron, Iain. 2006. *An Introduction to the European Convention on Human Rights*. 5th ed. Uppsala: Iustus Förlag.

EC (European Commission). 2016. "Commission Staff Working Document Impact Assessment on the Modernisation of EU Copyright Rules." https://ec.europa.eu/digital-single-market/en/news/impact-assessment-modernisation-eu-copyright-rules.

EC (European Commission). 2018. "Recommendation on Measures to Effectively Tackle Illegal Content Online." https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms.

EC (European Commission). 2019. "Frequently Asked Questions on Copyright Reform."https://ec.europa.eu/digital-single-market/en/faq/frequently-asked-questions-copyright-reform.

EDPS. 2010. "Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)." https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf.

EDPS. 2012. "Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America." https://edps.europa.eu/sites/edp/files/publication/12-04-24_acta_en.pdf.

Engeler, M. 2019. "Copyright Directive: Does the Best Effort Principle Comply with GDPR." https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html.

Engstrom, O., and N. Feamster. 2017. "The Limits of Filtering: A Look at the Functionality and Shortcomings of Content Detection Tools." *Engine* 1–32. http://www.engine.is/the-limits-of-filtering/.

Erickson, K., and M. Kretschmer. 2018. "'This Video is Unavailable' Analyzing Copyright Takedown of User-Generated Content on YouTube." *Journal of Intellectual Property, Information Technology and E-Commerce Law*. https://www.jipitec.eu/issues/jipitec-9-1-2018/4680/.

European Patent Office. 2014. "European Patent Specification." https://www.audiblemagic.com/wp-content/uploads/2014/10/EP1490767B1-1.pdf.

Frosio, G., and S. Mendis. 2019. "Monitoring and Filtering: European Reform or Global Trend?" In *The Oxford Handbook of Online Intermediary Liability*, edited by Giancarlo Frosio. OUP (forthcoming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411615.

Gann, A., and D. Abecassis. 2018. "The Impact of a Content Filtering Mandate on Online Service Providers." https://www.analysysmason.com/Consulting/content/reports/the-impact-of-a-content-filtering-June2018/.

Geiger, C., and E. Izyumenko. 2019. "Blocking Orders: Assessing Tensions with Human Rights." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3392253.

Google. 2018. "How Google Fights Piracy." https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/How_Google_Fights_Piracy_2018.pdf.

Grisse, K. 2019. "After the Storm – Examining the Final Version of Article 17 of the New Directive (EU) 2019/790." *Journal of Intellectual Property Law and Practice*. https://academic.oup.com/jiplp/article/14/11/887/5588517.

Heldt, A.-P. 2019. "Upload-Filters – Bypassing Classical Concepts of Censorship." https://www.jipitec.eu/issues/jipitec-10-1-2019/4877.

Husovec, M. 2019. "How Europe Wants to Redefine Global Online Copyright Enforcement." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372230.

ICO. 2018a. "Automated Decision-Making and Profiling." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/.

ICO. 2018b. "Guide to the General Data Protection Regulation (GDPR)." https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

ICO. 2018c. "Data Protection Impact Assessments." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

Internet Society. 2017. "Internet Society Perspectives on Internet Content Blocking: An Overview." https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf.

Japiot, O. 2017. "Copyright Protection on Digital Platforms: Existing Tools, Good Practice and Limitations." http://www.culture.gouv.fr/content/download/185905/2020626/version/2/file/CSPLA%20report-%20Copyright%20protection%20on%20digital%20platforms%20.pdf.

Kuczerawy, A. 2019. "From 'Notice and Take Down' to 'Notice and Staydown': Risks and Safeguards for Freedom of Expression." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305153.

Lester, T., and D. Pachamanova. 2017. "The Dilemma of False Positives: Making Content ID Algorithms More Conducive to Fostering Innovative Fair Use in Music Creation." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083080.

Montagnani, M. L., and A. Yordanova-Trapova. 2018. "Safe Harbours in Deep Waters: A New Emerging Liability Regime for Internet Intermediaries in the Digital Single Market." *International Journal of Law and Information Technology*. https://academic.oup.com/ijlit/article/26/4/294/5126431.

Ofcom. 2019. "Use of AI in Online Content Moderation." https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

Quintais, J., Giancarlo Frosio, Stef van Gompel, Bernt P. Hugenholtz, Martin Husovec, Bernd Justin Jütte, and Martin Senftleben. 2019. "Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484968.

Riordan, Jaani. 2016. *The Liability of Internet Intermediaries*. Oxford: Oxford University Press.

Romero-Moreno, F. 2019. "Notice and Staydown and Social Media: Amending Article 13 of the Proposed Directive on Copyright." *International Review of Law, Computers and Technology*. https://www.tandfonline.com/doi/full/10.1080/13600869.2018.1475906.

Sawicki, A. 2006. "Repeat Infringement in the Digital Millennium Copyright Act." *The University of Chicago Law Review*. https://www.jstor.org/stable/pdf/4495588.pdf?refreqid=excelsior%3A0d3326840fcc78d0eecc0ea9f2c1313a.

Senftleben, M. 2019. "Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3367219.

UNHRC. 2018. "Report of the Special Rapporteur Mr David Kaye on the Promotion and Protection of the Right to Freedom of Opinion and Expression." https://www.un.org/ga/search/view_doc.asp?symbol=A/73/348.

Urban, Jennifer M., Joe Karaganis, and Brianna L. Schofield. 2016. "Notice and Takedown in Everyday Practice." *Berkeley Law University of California* 1–147. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

Visser, D. 2019. "Trying to Understand Article 13." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354494.

Wagner, B. 2009. "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410.

Working Party. 2018. "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679." https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826.