Dr Felipe Romero-Moreno response to targeted consultation addressed to the participants to the stakeholder dialogue

on Article 17 of the Directive on Copyright in the Digital Single Market

bileta
British and Irish Law Education and Technology Association

Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market

Fields marked with * are mandatory.

INTRODUCTION

The Directive on Copyright in the Digital Single Market (Directive 2019/790/EC, the 'DSM Directive') requires the Commission to issue guidance on the application of Article 17, in particular regarding the cooperation between online content-sharing service providers and rightholders. The guidance should take into account the discussions held during the stakeholder dialogue meetings organised by the Commission pursuant to paragraph 10 of that article. The DSM Directive is addressed to the Member States who are required to transpose it by 7 June 2021. At this stage, the guidance will focus on assisting Member States in that task.

Following an open call for interest to participate in the stakeholder dialogue, the Commission organised six stakeholder dialogue meetings between October 2019 and February 2020 to gather the views of relevant stakeholders on the main topics related to the application of Article 17.

This consultation paper builds on the discussions at the stakeholder dialogue and presents the initial views of the Commission services with the view to finalising the Commission guidance.

We encourage the representative organisations to gather the views of their members and to provide, to the extent possible, a coordinated reply to the consultation. Where this is not possible, replies can be provided by individual members.

About yourself

* I'm giving my contribution as
  - ○ Organisation representing users, including fundamental rights organisations
  - ○ Organisation representing online content-sharing service providers
  - ○ Organisation representing rightholders
  - ○ Public authority
  - ◉ Other

* Please specify

Expert in Article 17 of the DSM Directive

E-mail (this won't be published)

f.romero-moreno@herts.ac.uk

* Are you registered in the Transparency Register of the EU?

- ○ Yes
- ◉ No

* Publication settings

The Commission will publish the responses to this public consultation. You can choose to opt out of the publication.

- ○ Your contribution will not be published
- ◉ Your contribution (and your type of respondent) will be published

☑ I agree with the privacy statement

Privacy statement

Privacy_statement.pdf

I. SCOPE OF SERVICES COVERED BY ARTICLE 17

Background

Article 17 applies to online content-sharing service providers as defined in Article 2(6) of the Directive. An online content-sharing service provider is defined as an information society service provider of which the main or one of the main purposes is to store and give the public access to a large amount of copyrightprotected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.

Article 2(6) also provides a non-exhaustive list of excluded providers of services, which are not online content-sharing service providers within the meaning of the Directive.

Special rules apply to new online content-sharing service providers, which meet the conditions in Article 17 (6).

Possible elements for the guidance

The guidance should indicate how to transpose the definition of 'online content-sharing service provider' into national law and explain the different elements of the definition itself, as well as of the list of service providers, which are expressly excluded.

The non-exhaustive nature of the exclusion for particular online service providers by use of the term 'such as' denotes that other service providers could also qualify as an excluded service provider on a case-bycase basis.

In order to provide legal certainty, Member States should explicitly set out in their implementing laws all elements of the definition of 'online content-sharing service provider' in Article 2(6), including the excluded service providers set out in Article 2(6). As regards these excluded service providers, the guidance should state that the Union legislature has expressly excluded from the scope of the definition the particular examples set out in Article 2(6).

For other services, which are not identified as examples but which may also be excluded, a case-by-case assessment would be necessary.

Recital 63 states that a case-by-case assessment would be required in order to determine whether an online service provider falls within the scope of the rules in Article 17. This does not affect the possible application of Article 3(1) and (2) of Directive 2001/29/EC to excluded service providers using copyrightprotected content, as recalled by recital 64.

Article 2(6) should be read in the light of recitals 62 and 63. It order to increase legal certainty as to the scope and as an aid to interpretation, Member States should be advised to also transpose elements of Recitals 62 and 63. Member States should apply the different elements of the definition, such as the concept of 'large amount of copyright protected content' in the light of these recitals, while they should refrain from further defining these elements going beyond the text of the directive, in order to avoid fragmentation.

Member States should bear in mind that the definition is drafted in a sufficiently neutral manner, which takes account of possible changes in modes of delivery, technology and usage and the fact that the DSM Directive will have to be applied in circumstances, which may change over time.

Question 1: Are there any additional elements related to the definition of an online content-sharing service provider, besides those outlined above, which you consider require some guidance? If yes, please indicate which ones and how you would suggest the guidance to address them. *2600 character(s) maximum*

II. AUTHORISATIONS (Art. 17 (1-2))

Background

Article 17(1) requires Member States to provide that online content-sharing service providers, as defined in Article 2(6), perform an act of communication to the public or an act of making available to the public for the purposes of this Directive when they give the public access to protected content uploaded by their users and therefore need to obtain an authorisation from relevant rightholders, for instance by concluding a licensing agreement. Under Article 17(2) the authorisation obtained by the online content-sharing service providers must also cover the acts carried out by users, under certain conditions.

Possible elements for the guidance

(i) Authorisation models

The guidance should explain how Member States should approach the requirement of 'authorisation' in Article 17(1). The term 'authorisation' is not defined and it should be interpreted in the light of the aim and objective of Article 17.

Article 17 is a lex specialis to Article 3 of Directive 2001/29/EC and of Article 14 of Directive 2000/31/EC. This is confirmed by Recital 64, which states clearly that Article 17 does not affect the concept of communication to the public or of making available to the public elsewhere under Union law, nor does it affect the possible application of Article 3(1) and (2) of Directive 2001/29/EC to other service providers using copyright-protected content. As such, Member States would not be able to rely in their transposition of Article 17 on their implementation of either of those directives in relation either to the notion of
'authorisation' or indeed for the notion of 'communication to the public'. Therefore, Member States should explicitly introduce into national law the notion of 'authorisation' for the lex specialis 'act of communication to the public' in Article 17(1).

Article 17(1) provides that an authorisation may for instance include a licensing agreement and this is also set out in Recital 64. Accordingly, an authorisation may take the form of a licensing agreement but may also take another form in national law. The guidance could give indications of different authorisation schemes that Member States could provide for, taking into account the specificities and practices of different sectors. Both individual and collective licensing solutions should be possible. Extended collective licences (ECL) could be considered in specific cases and for specific sectors, provided that they comply with the conditions of Article 12 of the DSM Directive.

The guidance would also recall that rightholders are not obliged to grant an authorisation to online contentsharing service providers, as explained in recital 61. Nevertheless, where rightholders do not grant an authorisation, online content-sharing service providers are not liable for copyright infringements if they comply with the conditions set out in Article 17(4) (see section III.1).

In order to foster the grant of authorisations in any chosen form at national level and to ensure the *effet utile* of Article 17(1), Member States could be recommended to maintain or establish voluntary mechanisms to facilitate agreements between rightholders and service providers. For example, voluntary mediation mechanisms could be considered in specific cases or sectors to support parties willing to reach an agreement but facing difficulties in the negotiations.

(ii) Authorisations covering users

Member States should implement explicitly in their legislation Article 17(2) under which an authorisation granted to online content-sharing service providers should also cover acts carried out by (i) users acting for non-commercial purposes or (ii) users whose activity does not generate significant revenues. It is important to bear in mind that these authorised uses are in addition to what else is authorised for content-sharing service providers.

Under this provision, authorisations granted to service providers are deemed to cover the acts, within the material scope of the authorisation granted, that are carried out by users falling in any one of these categories (non-commercial purpose or non-significant revenues). It is sufficient for a user to satisfy one of these conditions to be covered by the authorisation.

The guidance could illustrate this provision, which would for example cover users uploading a home video including music in the background or users uploading a tutorial generating limited revenues, which includes music or images when no exceptions apply. On the other hand, users acting on a commercial basis and deriving significant revenues from their uploads would be outside the scope of or not covered by that authorisation (unless the parties have explicitly agreed to cover also these users contractually). Member States should not set out quantitative thresholds when implementing the concept of 'significant revenues' which should be examined on a case-by-case basis. Member States should be recommended to assess the notion of 'significant revenue' by reference to all the

circumstances of the user's activity in question, including whether there is a licence agreement where the parties have agreed on specific thresholds (which should however not go below what is authorised under Article 17(2)).

Member States should interpret the notion of authorisation in Article 17(2) in light of recital 69 according to which service providers do not have to obtain a separate authorisation when rightholders have already authorised users to upload specific content. In these cases, the act of communication to the public has already been authorised within the scope of the authorisation granted to the user. The same recital also indicates that service providers should not presume that their users have in all cases obtained all the necessary authorisations for the content they upload.

In order to enhance transparency and legal certainty, the guidance could encourage the Member States to put in place an exchange of information on authorisations between rightholders, users and service providers.

Question 2: Are there any additional elements related to authorisations under Article 17(1) and 17 (2), which should be covered by the guidance? If yes, please explain which ones and how you would suggest the guidance to address them. *2600 character(s) maximum*

Question 3: Do you have any concrete suggestions on how to ensure a smooth exchange of information between rightholders, online content-sharing service providers and users on authorisations that have been granted?

2600 character(s) maximum

III. SPECIFIC LIABILITY REGIME UNDER ARTICLE 17

Article 17(4) establishes a specific liability regime for online content-sharing service providers that have not obtained an authorisation from the relevant rightholders under the applicable national rules implementing Article 17(1). Therefore, the *effet utile* of this provision will depend on the system of 'authorisation' put in place by the Member State under Article 17 (1) and (2). As outlined in recital 61, the goal of Article 17 is 'to foster the development of the licensing market between rightholders and online content-sharing service providers'. Article 17(4) only becomes applicable in those cases in which the primary goal of authorisation of acts of communication to the public performed by online content sharing service providers within the meaning of Article 17(1), for instance by concluding a licensing agreement, could not be achieved.

In the absence of an authorisation, Article 17(4) sets out three cumulative conditions, which service providers may invoke as a defence against liability.

The conditions in Article 17(4) are subject to the principle of proportionality, as specified in Article 17(5). In this respect, the guidance should give indications to Member States on the practical application of the proportionality criteria to the conditions set in Article 17(4), notably how the type, size and audience of the service, the availability of suitable and effective means and the related costs, as well as the type of content uploaded by the users could be considered in different cases.

1. BEST EFFORTS TO OBTAIN AN AUTHORISATION (ARTICLE 17(4)(a))

Background

The first condition in Article 17(4) letter (a) is that service providers should be liable for unauthorised acts of communication to the public, including acts of making available to the public, unless they demonstrate they have made best efforts to obtain an authorisation. The principle of proportionality, as set out in Article 17(5), should be taken into account when assessing whether a service has made its best efforts under Article 17 (4) letter (a). Pursuant to Article 17(8), the application of Article 17 should not lead to any general monitoring obligation.

Possible elements for the guidance:

The guidance could give non-exhaustive indications of actions carried out by service providers that could constitute best efforts to obtain an authorisation by the service providers. In particular, it should illustrate, which action on the part of service providers would constitute best efforts. This would include any action taken by service providers to seek out and/or engage with rightholders and the response, if any, to such solicitation and/or engagement by rightholders. Member States may wish to include such actions, which could, if relevant, vary from sector to sector, in their transposition law.

The authorisation models defined by Member States pursuant to Article 17(1) will have an impact on how easily service providers may be able to fulfil the requirement of 'best efforts' to obtain an authorisation. The threshold of 'best efforts' may be more easily satisfied where a Member State has taken measures to facilitate the grant of authorisations, for example with regard to licensing models, mediation mechanisms or exchange of information. Where a Member State has opted for a system, which leaves greater flexibility in the authorisation regime, service providers may need to adduce evidence that they have tried and been unable to get an authorisation. Keeping records of service providers' engagement with rightholders may help addressing this situation. The evidential standard to prove best efforts would depend therefore on the type of authorisation in national law. For example, participation in a voluntary mediation, where available, could be taken into account in order to satisfy best efforts.

The guidance should recall the importance of applying the best efforts obligation on a case-by-case basis and according to the proportionality principle and the criteria provided for in Article 17(5).

To illustrate the best effort obligation, the guidance should make clear that service providers have to engage proactively as a minimum with rightholders which can be easily identified and located, in order to seek an authorisation. This includes rightholders representing a broad catalogue of works or other subject matter, or their representatives with a mandate to act on their behalf such as collective management organisations (CMOs) acting in accordance with Directive 2014/26/EU.

At the same time, in accordance with the principle of proportionality, service providers should not be expected to proactively seek out all rightholders whose content may be uploaded on their services, in particular those who are not easily identifiable by any reasonable standard. The guidance should however explain that online content-sharing service providers should as a rule enter into negotiations with those rightholders that wish to offer an authorisation for their content, irrespective of whether their type of content (eg. music, audio-visual content, images, text, etc...) is prevalent or is less common on the website of the service provider. Nevertheless, pursuant to the principle of proportionality, in certain cases (notably in case of smaller service providers) a lower level of effort to obtain an authorisation may be expected for types of content which are less common on the website of a given service provider (e.g. for images or texts on a video-sharing platform).

In the light of Recital 61, licensing agreements should be fair and keep a reasonable balance between both parties. That recital also states that rightholders should receive appropriate remuneration for the use of their works or other

subject matter. As a consequence, service providers refusing to conclude a licence offered on fair terms and which maintains a reasonable balance between the parties should not be considered to have deployed their best efforts to obtain an authorisation. On the other hand, service providers should not be required to accept licensing offers that are not on fair terms and which do not keep a balance between the parties, including as regards the remuneration to be paid.

The guidance should refer to the relevant provisions of Directive 2014/26/EU applying to licences negotiated and concluded by CMOs, in particular Article 16 (conducts of negotiations and licencing terms) and Article 35 (resolution of disputes). As mentioned under Section II, Member States may also maintain or establish voluntary mechanisms aimed at facilitating the conclusion of licensing agreements between online content-sharing service providers and rightholders.

Question 4: In which cases would you consider that an online content-sharing service provider has made its best efforts to obtain an authorisation, in light of the principle of proportionality? Please give some concrete examples, taking into account the principle of proportionality. *2600 character(s) maximum*

Question 5: In your view, how should online content-sharing service providers, in particular smaller service providers, make their best efforts to obtain an authorisation for content, which is less common on their service?

2600 character(s) maximum

Question 6: Are there any additional elements related to Article 17(4)(a), which should be covered by the guidance besides those outlined above? If yes, please explain which ones and how you consider the guidance should address them.

2600 character(s) maximum

2. 'BEST EFFORTS' TO AVOID UNAUTHORISED CONTENT (Art. 17(4)(b))

Background

The second condition set out in Article 17(4) is that online content-sharing service providers should be liable for the use of unauthorised content unless they demonstrate that they have made their best efforts, in accordance with high industry standards of professional diligence, to ensure the unavailability of specific works and other subject matter for which the rightholders have provided them with the relevant and necessary information. The principle of proportionality, as set out in Article 17(5), and Article 17(7) should be taken into account. Pursuant to Article 17(8), the application of Article 17 should not lead to any general monitoring obligation.

Possible elements for the guidance:

Member States should bear in mind that these provisions are subject to the obligation on them in Article 17 (7) and (9) to ensure that legitimate uses remain unaffected by the cooperation of service providers with rightholders. The guidance should give indications to Member States on how this could be achieved, as explained in section IV.

The guidance should recommend that in their implementing laws Member States should not mandate the use of technology or impose any specific technological solutions on service providers in order to demonstrate best efforts. This would not only ensure a technologically neutral and future proof application of Article 17(4)(b) but also provide for a less intrusive approach. The service providers together with rightholders may cooperate on the best way to approach identification of the works in question, including by recourse to technology taking into account that the cooperation should not lead to any general monitoring obligation.

The guidance should underline that service providers have to act diligently when making their best efforts to implement any relevant solutions. As stated in Recital 66, to assess whether a given service provider has made its best efforts, account should be taken of whether the service provider has taken all the steps that would be taken by a diligent operator to achieve the result of preventing the availability of unauthorised works or other subject matter on its website taking into account best industry practices and the effectiveness of the steps taken in light of all relevant factors and developments. However, service providers should remain free to choose the technology or the solution that they consider the most appropriate to comply with the best efforts obligation in their specific situation, given that account should be taken of the principle of proportionality.

The stakeholder dialogue showed that content recognition technology is already used today to manage the use of copyright protected content, at least by the major online content-sharing service providers. Besides content recognition technology based on fingerprinting, other solutions, such as watermarking, solutions based on metadata and key word search or a combination of different technologies are currently deployed to detect unauthorised content.

Therefore, in most cases, it is expected that service providers will rely (or continue to rely) on technological tools in order to comply with their obligation under Article 17(4)(b) but it is not a prerequisite for the application of Article 17(4). The guidance should in this context recall that the deployment of any solution, including use of technology, such as content recognition technologies, has to respect Article 17(7) and 17 (9), which lays down safeguards for legitimate uses (see section IV below).

The guidance should also recall the importance of applying the 'best effort' obligation on a case-by-case basis and according to the proportionality principle and the criteria provided for in Article 17(5). In this respect, the guidance should give indications to Member States along the following lines:

- The type, size and audience of the service: larger service providers with a significant audience may be expected to deploy more advanced and costly solutions/technologies than 'smaller' service providers, with more limited audiences and resources. It could be more proportionate to expect smaller service providers to resort to simpler solutions (like metadata or key word search) as long as these solutions are effective. In some cases, notably for small service providers, relying on ex post action following rightholders' notifications (notice and take down) may be proportionate, as explained in recital 66.

- The availability of suitable and effective means and the related costs should also be considered, for example when service providers buy solutions from third parties/ technology providers, when these are developed in-house as well as the costs related to human review in the context of disputes (see Section IV). The cumulative cost of different solutions that may need to be implemented by a service provider should also be considered, as well as limitations of technologies depending on the type of content.

- The type of content uploaded by the users: when a service provider makes available different types of content, the level of efforts to be made may vary depending on whether the content is prevailing in their website or residual. It can be expected that service providers make more efforts regarding the former as compared to the latter.

In line with Article 17(4)(b), the guidance should underline that the best efforts to ensure the unavailability of specific unauthorised content are to be assessed on the basis of the *'relevant and necessary information'* rightholders must provide to online content-sharing service providers. Whether any information provided by rightholders is "relevant and necessary information" in any given situation should be assessed on a case-bycase basis. Recital 66 specifies that if no such information is provided by rightholders, service providers are not liable for unauthorised uploads of unidentified content.

The guidance would provide some examples of what may constitute relevant and necessary information in different cases. Such information will vary depending on the solutions deployed by service providers (for example metadata on the work such as title, author/producer, duration; fingerprints or the actual content file). The information provided by rightholders should be relevant and accurate to allow service providers to take action on that basis. Member States should be free to define sanctions for abuse of the cooperation mechanism laid down in Article 17, such as the provision of false information.

Flexibility could be left to rightholders and service providers to agree on mutually convenient cooperation arrangements in view of ensuring the unavailability of unauthorised content, within the boundaries of the safeguards for legitimate uses.

Question 7: In which cases would you consider that an online content-sharing service provider has or has not made its best efforts to ensure the unavailability of specific unauthorised content in accordance with high industry standards of professional diligence and in light of the principle of proportionality and the user safeguards enshrined in Article 17(7) and (9)? Please give some concrete examples.

2600 character(s) maximum

Consistent with the CJEU rulings in Sabam v Netlog and Sabam v Scarlet, it might not be reasonable to apply content-based fingerprinting to 'all' files carried through the network due to the usually processorexhaustive 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, content of high commercial value – might be preferable to guarantee adequate speed with limited processing resources. Respecting the ECtHR and CJEU 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.

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. 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.

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. 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 - seeEuropean Patent Office. 2014. “European Patent Specification.” https://www.audiblemagic.com/wp-content/uploads/2014/10/EP1490767B1-1.pdf at pages 8-9.

Question 8: Which information do you consider ‘necessary and relevant’ in order for online contentsharing service providers to comply with the obligation set out in Article 17(4)(b)?

2600 character(s) maximum

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 - see 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/ at page 4. To do so, as required under Article 17(4)(b), 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.

The issue here is 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, 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.

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. Therefore, unless copyright databases are centralised and targeted exclusively at music and video with highcommercial value content, arguably the implementation of upload filters will mean that fragmentation could be a real problem. On the other, OCSSPs would have to check uploaded content against different platforms. The result would be that the cost of implementing Article 17 would increase with every supplementary database against which UGC must be compared (Gann and Abecassis 2018, 4-11).

Question 9: Are there any other elements related to the best efforts to ensure the unavailability of unauthorised content, besides those outlined above, for which you think some guidance is needed? If yes, please explain which ones and how you consider the guidance should address them.

2600 character(s) maximum

In C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited [2019] EU:C:2019:458, 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' – see paragraph [46]. Moreover, 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 – see paragraph [53]. In this context, it would be advisable for the EC to clarify what type of information should be set out in the staydown injunction and the parameters for these injunctions to be compatible with international law. For instance, it is arguable that the scope of ratione personae, ratione materiae and ratione temporis of the surveillance and technical measures required to implement monitoring systems should be set out in the injunction that is, the number of users and services to be affected, the types of communications to be impacted and the time to be taken over the measures. Moreover, it should also be clarified the level of examination required to perform user monitoring, namely, Deep Packet Inspection (DPI), Shallow Packet Inspection (SPI) or both.

3. NOTICES SUBMITTED BY RIGHTHOLDERS TO REMOVE UNAUTHORISED CONTENT AND THE RELEVANT AND NECESSARY INFORMATION TO PREVENT FUTURE UPLOADS (ART. 17(4)(c))

Background

The third condition set out in Article 17(4) (c), which is also subject to the principle of proportionality laid down in paragraph 5 and the safeguards for legitimate uses in paragraph 7, is that online content-sharing service providers should be liable for the use of unauthorised content unless they demonstrate that they have 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 that they have made best efforts to prevent their future uploads in accordance with Article 17(4)(b). Pursuant to Article 17 (8), the application of Article 17 should not lead to any general monitoring obligation.

Possible elements for the guidance:

The guidance should give indications to Member States on how they should implement Article 17(4)(c) in their national laws. Member States should bear in mind that the two conditions set in letter (c) are subject to the principle of proportionality provided for in Article 17(5). The 'best efforts' that service providers should make to prevent future uploads of notified works should be approached in the same way as in relation to Article 17(4)(b). The guidance should recall the importance of assessing whether the best efforts have been made by service providers on a case-by-case basis.

Member States should also bear in mind that the application of Article 17 should not lead to any general monitoring obligation and that legitimate uses have to be safeguarded as provided for in paragraphs 7 and 9, and as further explained in section IV. This is particularly relevant for the application of the second part of letter (c), according to which service providers have to make their best efforts to prevent future uploads of notified works.

The guidance should also indicate that when implementing Article 17(4) letter (c), Member States need to clearly differentiate the type of information rightholders provide in a 'sufficiently substantiated notice' for the removal of content (the 'take-down' part of letter (c)) from the "relevant and necessary information" they provide for the purposes of preventing future uploads of notified works (the 'stay-down' part of letter (c), which refers back to letter b).

With regard to the elements to be included in a 'sufficiently substantiated notice' submitted by rightholders, the guidance should recommend Member States to follow in their implementation the Commission Recommendation on Measures to Effectively Tackle Illegal Content Online[1]. The information provided should be specific and detailed in nature in a way in which it verifies not only the work or protected subject matter and the specific rights held by the rightholder but where it is alleged to be on the website in question.
Points 6 to 8 of the Recommendation list elements that could be included in the notices. As the Recommendation is a horizontal non-binding instrument and therefore not copyright specific, existing national rules and current practices for copyright notices, which may contain more details, could also be applied.

Article 17(4) letter (c) second part (the 'stay down' obligation) refers back to letter (b) of the same paragraph. As a consequence, in order for the service providers to be able to deploy their best efforts to avoid future uploads under this provision, rightholders have to provide them with the same type of 'relevant and necessary' information which is relevant for the application of letter (b). This means for example that, if a service provider uses fingerprinting technologies to avoid future uploads of notified works, receiving as information only the title of a song and its location, as identified in a notice, would be insufficient. In this case, to allow service providers to avoid future uploads of notified works, rightholders would need to provide the services with fingerprints or content files. If rightholders have already provided the 'necessary and relevant' information under letter (b) of Article 17(4) with regard to a specific notified work, they should not be obliged to re-submit the same information for the purposes of 'stay-down', but this should be assessed on a case-by-case basis.

[1] See Commission Communication of 1 March 2018 available at: https://ec.europa.eu/digital-single-market /en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

Question 10:What information do you consider a sufficiently substantiated notice should contain in order to allow the online content-sharing service providers to act expeditiously to disable access /remove the notified content?

2600 character(s) maximum

Question 11: Are there any other elements related to the 'notice and take down' and 'notice and staydown' systems provided for in Article 17(4)(c) that should be covered by the guidance? If yes, please explain which ones and how you would suggest the guidance to address them.

2600 character(s) maximum

In Sabam v Netlog and Sabam v Scarlet[33]-[38] 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. This contrasts with C-18/18 Eva Glawischnig-Piesczek v Facebook where 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' – see [46].

Another issue for the EC to consider is how monitoring systems, which rely on upload filters could be implemented in a less data processor-intrusive way for online intermediaries and minimally impact users' rights. For instance, in

the context of Article 17 of the CDSM for general monitoring obligations to become lawful 'duties of care' and 'specific' enough to comply with Recitals 47 and 48 E-Commerce Directive, it would be possible 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. Moreover, rightholders could 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; then, checking the frequency and number of unlawful uploads that is, asking a database for suspected repeat infringement IP addresses; next, sending a message alerting of potential commercial-scale infringement or redirecting to a commercial website; and lastly, giving the opportunity to alleged commercialscale uploaders to challenge the blocking before actually implementing it.

4. SPECIFIC LIABILITY REGIME FOR START-UPS (ARTICLE 17.6)

Background

Article 17(6) provides for a specific liability regime for 'new' companies, with lighter conditions. This is in practice a two-tier regime applicable to services, which have been active in the EU for less than 3 years and have an annual turnover of less than 10 million euros with different rules applying to them depending on the audience they attract. In practice:
(i) If those 'new' services have less than 5 million unique visitors they are required to make their best efforts to obtain an authorisation (Art.17 (4) (a)) and they have to comply with the 'notice and take down' obligation under Art. 17(4) (c), first part.

(ii) If those 'new' services have more than 5 million unique visitors they are subject to the same obligations of best efforts to obtain an authorisation and 'notice and take down' as services with a smaller audience but in addition, they also need to comply with the obligation to avoid future uploads of notified works under Article 17 (4) (c) second part ('stay down' obligation).

For both categories of services, the condition of best efforts to ensure the unavailability of unauthorised content, provided for in Article 17 (4)(b), is not applicable.

Possible elements for the guidance:

The guidance should provide indications to the Member States for the implementation of the specific liability regime set out in Article 17(6). It could focus on certain elements of the liability regime, which may raise practical questions, such as how to calculate the annual turnover of the services and the number of monthly unique visitors. It would remind for example that the annual turnover needs to be calculated in accordance with the Commission Recommendation 2003/361/EC for SMEs. It would also explain that the number of monthly unique visitors refers to visitors across the Union, as explained in recital 66, and not per Member State.

The guidance should also clarify that the principle of proportionality provided for in Article 17(5) and the safeguards for legitimate uses under Article 17(7) apply to the liability regime for 'new' services. In this context, the guidance could provide some examples of what best efforts could be expected from the 'new' services covered by Article 17(6) for obtaining authorisations and where applicable, for preventing future uploads of notified works, in the light of the principle of proportionality.

Question 12: What specific elements of the specific liability regime for "new" services, provided for in Article 17(6), should in your opinion be addressed in the guidance and how? *2600 character(s) maximum*

IV. SAFEGUARDS FOR LEGITIMATE USES OF CONTENT (Art. 17(7)) and REDRESS MECHANISM FOR USERS (Art. 17(9))

Background

Article 17(7) and 17(9) lay down rules aiming to ensure that any action undertaken together by service providers and rightholders does not lead to the unavailability of content which does not infringe copyright. This is of particular importance (but not only) for the application of Article 17(4) letter (b) and second half of letter (c), whereby online content-sharing service providers need to make their best efforts to ensure the unavailability of unauthorised content and to prevent future uploads of notified works. Article 17(7) also provides that the Member States must ensure that users in each Member State are able to rely on the existing exceptions or limitations for quotation, criticism, review and use for the purpose of caricature, parody or pastiche when they upload and make available their content on online content-sharing service providers' websites. Under Article 5 of Directive 2001/29/EC these exceptions were optional and therefore not all Member States have implemented them. Article 17 (7) makes these exceptions mandatory for all Member States for the uses of copyright protected content covered by this provision.

Article 17(9) requires online content-sharing service providers to put in place a redress mechanism allowing users to challenge the blocking or removal of their content. Disputes can occur when content-sharing service providers disable or remove access to user uploaded content, whereas users consider their uploads legitimate, for example uses of third party content under an exception or limitation to copyright.

Article 17(9) further requires that the Directive shall in no way affect legitimate uses, and shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679. It also requires online content-sharing service providers to inform their users in their terms and conditions that they can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law.

Possible elements for the guidance:

The guidance should explain what Member States have to do to implement Article 17(7) and the relationship between that provision and Article 17(4). Article 17(7) is addressed to safeguarding any content uploaded by users that does not infringe copyright or related rights including by virtue of the application of any exception or limitation. Such non-infringing use is often referred to as 'legitimate use'. In addition, Article 17(7) second paragraph introduces certain mandatory exceptions for users that upload content online.

Member States should be recommended to explicitly transpose in their law the text of Article 17(7) first paragraph whereby the cooperation between online content-sharing service providers and rightholders, in particular under Article 17(4), must not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation.

Member States are required to transpose in their national laws the mandatory exceptions in Article 17(7) second paragraph covering the case of content uploaded by users on online content-sharing services for:

(a) quotation, criticism, review

(b) use for the purpose of caricature, parody or pastiche

Whilst the exceptions or limitations in Directive 2001/29/EC are optional in nature and addressed to any user, Article 17(7) applies to all users in all Member States who must be able to rely on these exceptions or limitations when they upload content on online content-sharing service providers' websites. Recital 70 explains that allowing users to upload and make available content generated by them for the purposes of the exceptions or limitations in Article 17(7) is particularly important for 'striking a balance between the fundamental rights laid down in the Charter of Fundamental Rights of the European Union ('the Charter'), in particular the freedom of expression and the freedom of the arts, and the right to property, including intellectual property'.

(i) Legitimate uses under Article 17(7)

Examples of legitimate uses may include (1) uses under exceptions and limitations, (2) uses by those who hold or have cleared the rights in the content they upload or covered by the authorisation under Article 17 (2); (3) uses of content not covered by copyright or related rights, notably works in the public domain or for example content where the threshold of originality is not met.

The guidance could recall that uses under exceptions and limitations cover the upload and making available of content under the mandatory exceptions in Article 17(7) but also under other – optional - exceptions that Member States may have implemented under Article 5 of Directive 2001/29/EC. Some of those are particularly relevant for uses on online content-sharing services and Member States, which have not done so, could be recommended to implement them for uses covered by Article 17 (for ex. incidental use)[1].

Member States that may have already implemented the exceptions made mandatory by Article 17(7) under Directive 2001/29/EC should review their legislation to make sure it complies with Article 17(7) and if needed, adapt it accordingly. Member States whose laws do not provide for these exceptions will have to transpose them as a minimum for the uses covered by Article 17.

The guidance should give indications to the Member States on the interpretation of the mandatory exceptions, in line with the case law of the Court of Justice of the European Union.

(ii) Practical application of Article 17(4) in compliance with Article 17(7)

The guidance should also give indications to the Member States as to how they can direct online contentsharing service providers and rightholders to apply in practice Article 17(4) in compliance with Article 17(7). The objective should be to ensure that legitimate content is not blocked when technologies are applied by online content-sharing service providers under Article 17(4) letter (b) and the second part of letter (c).

The guidance should explain that the balancing sought by the Directive requires, besides the effective complaint and redress mechanism discussed in the subsequent section, that the cooperation between service providers and rightholders does not result in blocking legitimate uses. Therefore, the guidance would take as a premise that it is not enough for the transposition and application of Article 17 (7) to only restore legitimate content ex post, once it has been blocked. When service providers apply automated content recognition technologies under Article 17(4), on the basis of the relevant and necessary information provided by the rightholders, legitimate uses should also be considered at the upload of content.

It should be born in mind that in the current state of the art, content recognition technology cannot assess whether the uploaded content is infringing or covered by a legitimate use. However, technology may assist service providers to distinguish uploads likely to be infringing for the purposes of Article 17(4) from uploads likely to be legitimate, based on the application of technical parameters as explained below. In order to ensure compliance with Article 17(7) in practice, automated blocking of content identified by the rightholders should be limited to likely infringing uploads, whereas content, which is likely to be legitimate, should not be subjected to automated blocking and should be available.

This distinction between likely infringing and likely legitimate uploads would not introduce any new legal concepts, nor would it imply a final legal assessment as to whether an upload is legitimate or not, but it would be a reasonable and practical way for service providers to apply Article 17(4) in line with Article 17(7) when they use content recognition technology. This mechanism should also not prevent the possible use of technology for reporting and remunerating the use of authorised content under contractual terms agreed by rightholders and service providers.

Under this approach, when uploads match with the relevant and necessary information provided to them by the rightholders, service providers should assess their legitimacy in compliance with Article 17(7) and proceed, where applicable, to block likely infringing uploads. In such a case users should still be able to contest the blocking under the redress mechanism provided for in Article 17(9), which requires human review for the contested content before a decision is taken whether it should stay down or be restored.

In cases when it is not possible for online content-sharing service providers to determine on a reasonable basis whether an upload is likely to be infringing and the service providers use content recognition technology, the service providers should notify the user that (part of) the upload matches with the information (e.g. fingerprint) provided by the rightholders. If the user contests the infringing nature of its upload, service providers should submit the upload to human review for a rapid decision as to whether the content should be blocked or be available. Such content should remain online during the human review. If rightholders disagree with the decision of service providers to keep the content up, they would be able to submit a notice in compliance with Article 17(4) letter (c) to ask for the removal of the content that they consider infringing. If, on the other hand, upon being notified by the service provider, the user does not contest the infringing nature of the upload, the content could be blocked without further review, without prejudice to users' ability to rely on other available redress, including judicial review.

The human review process should be swift and allow both rightholders and users to provide their views. If, as a result of the human review, the service provider decides to disable or remove the uploaded content, it should inform the user of the outcome of the review; and the user should be able to have recourse to the out-of-court dispute resolution mechanism, provided for in Article 17(9).

The distinction between likely infringing and likely legitimate uploads could be carried out by service providers in cooperation with rightholders based on a number of technical characteristics of the upload, as appropriate. Relevant technical parameters could be, among others, the level of match with the reference file provided by rightholders for the purposes of Article 17(4), the length/size of third party content used in the upload and whether it is surrounded by user’s own content. For example, in application of such technical parameters, the upload of a video of 30 minutes, where 29 minutes are an exact match to a reference file provided by a rightholder, could likely be considered an infringing one, unless it is in the public domain or the use has been authorised. On the other hand, a user generated video composed by very short extracts, such as one or two minutes of different scenes from third party films, accompanied by additional content such as comments added by the user for the purpose of reviewing these scenes could be more likely to be legitimate because potentially covered by an exception such as the quotation exception. Similarly still images uploaded by users which match only partially the fingerprints of a professional picture could be

legitimate uploads under the parody exception, as they could be 'memes', i.e. new images created by users by adding elements to an original picture to create a humoristic or parodic effect.

The application of technical parameters should not be arbitrary and should be without prejudice to any legal decision on the nature of the content uploaded, i.e. whether it is an infringement of copyright or a related right or not.

Member States should remain free to introduce specific measures to discourage the abuse of this mechanism by users or rightholders.

Finally, in order to minimise the risk that authorised content uploaded with the authorisation of rightholders is blocked, Member States may consider recommending service providers to use the practice of 'whitelisting', which allows rightholders to indicate to the service providers users and uses that they have authorised. For example, in case of co-productions or partnerships, broadcasters can indicate to service providers which other broadcasters or partners are authorised to upload their content. Such uses would not require the application by service providers of content recognition technologies for blocking purposes.

(iii) Complaint and redress mechanism under Article 17(9)

Article 17(9) requires Member States to provide for a complaint and redress mechanism that online contentsharing service providers have to make available to users in the event of dispute over the blocking or removal of their content; it also requires Member States to ensure that out-of-court redress mechanisms are available for the settlement of these disputes. When approaching Article 17(9) Member States should bear in mind that the obligation on service providers to put in place a complaint and redress mechanism should be implemented in line with the Union law rules on freedom to provide services, including the 'country of origin' principle provided for in Article 3 of Directive 2000/31/EC on e-commerce, when applicable.

The guidance should give indications to the Member States on how they could instruct service providers to apply the complaint and redress mechanism in practice. It could suggest that when content is blocked as a result of the application of the mechanism described above for the practical application of Article 17(4) in compliance with Article 17(7), the contested content, which is likely infringing should stay down pending the human review required under the redress mechanism. This would correspond to the approach that only uploads likely to be infringing could be automatically blocked under Article 17(4) in compliance with Article 17(7) and Article 17(9). Content that service providers remove ex post under the notice and take down procedure under Article 17(4) letter (c) should only stay down pending the redress, provided that the notice submitted by rightholders is a 'sufficiently substantiated' notice.

In line with the requirement of Article 17(9) that the complaints by users be processed without undue delay, the guidance should suggest that as a rule service providers and rightholders must react to complaints from users within a reasonably short timeframe to ensure that the mechanism is expeditious. If rightholders do not react in a reasonable timeframe, content which has been blocked or taken down should become available or be restored. The guidance should also recall rightholders' obligation to duly justify their requests to have content uploaded by users blocked or removed and encourage rightholders to provide this justification in clear and simple terms to make it understandable to an average internet user.

If the final decision by service providers is to keep the content unavailable, users must be able to contest this decision through the impartial out-of-court dispute settlement mechanism, which Member States have to make available. The guidance should indicate that the out-of- court dispute settlement mechanism can be an existing one but with relevant expertise to handle copyright disputes. It should also be easy to use and with no cost for users.

The guidance should also indicate to the Member States that they need to implement in their law the obligation on online content-sharing service providers to inform their users in their terms and conditions that users can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law.

The guidance could also recommend how service providers can increase users' awareness of what may constitute legitimate uses, as required by Article 17(9). For example, Member States could encourage the service providers to put in place standard forms for users to contest the blocking or removal of their content. This could also be accompanied by information aiming to foster users' awareness of copyright concepts and to encourage a responsible behaviour when uploading content online.

Finally, the guidance should underline that any processing of personal data and identification of users that may be required in the context of the application of Article 17 needs to be done in compliance Directive 2002/51/EC on e-privacy and Regulation 2016/679 on general data protection. Member States should monitor the correct application of these rules.

[1] Article 5.3 (h) of Directive 2001/29/EC

Question 13: Do you have additional suggestions to implement Article 17(7) to ensure a fair balance between different fundamental rights notably between copyright and freedom of expression? Would you agree with the approach presented above or do you consider other solutions could be used?

2600 character(s) maximum

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), arguably rightholders should always be encouraged to favour monetisation over blocking. However, perhaps rightholders might fail to reach an agreement concerning this matter. Accordingly, consistent with ECtHR and CJEU 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 processorexhaustive ones, but only if previous stages do not return a match. 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. 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. 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. 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 should be registered in a database. Moreover, 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; then, checking the frequency and number of unlawful uploads that is, asking a database for suspected repeat infringement IP addresses; next, sending a message alerting of potential commercial-scale infringement or redirecting to a commercial website; and lastly, giving the opportunity to alleged commercial-scale uploaders to challenge the blocking before blocking.

Question 14: Do you have additional suggestions on how the guidance should address the implementation of the complaint and redress mechanism and of the out-of-court dispute settlement under Article 17(9)?

2600 character(s) maximum

According to Article 17(9), Member States must ensure that service providers adopt complaints and redress mechanisms for users in case of disputes. Controversially, however, the Directive strikes the human rights balance clearly in favour of the major rightholders, as it neither demands that users affected by takedowns be notified of requests, nor does it afford users counter-notice and put-back procedures or monetary remedies compared to the US Digital Millennium Copyright Act - see Urban, Jennifer M., Joe Karaganis, and Brianna L. Schofield. 2016. "Notice and Takedown in Everyday Practice." BerkeleyLaw University of California at pages 16, 22. It is true that some EU countries have adopted counter-notification systems. However, one might argue that to ensure harmonization across all Member States, the Directive should make it an explicit legal duty that service providers are not only required to notify users of the removal of their content but also give them the opportunity to send counter-notices and rely on recovery remedies. Notably, in Tele2/Watson the CJEU observed that where human rights were infringed, notification was a fundamental safeguard necessary to permit individuals to exercise their right to a legal remedy - see [141]. Indeed, the Grand Chamber in Barbulescu v Romania agreed that in the absence of a prior warning to the claimant advising him that his internet usage was being monitored, he still had a reasonable expectation of privacy - see [133]. Similarly, another point that should be mentioned is that to ensure due process, under the DMCA users are also able to send counter-notices to the service provider requesting that their uploaded content be reinstated. Lastly, to avoid the abuse of these procedures, the DMCA additionally gives parties who make a knowing material misrepresentation in notifications and counter-notifications the right to recover costs and damages (Urban, Karaganis, and Schofield 2016, 16). This is despite the fact that the wording and penalty is different for these notifications and counter-notifications, thereby resulting in abusive notices as well as users being discouraged from submitting counter-notices (Bridy and Keller 2017, 9–10).

Question 15: Are there other elements than those outlined above that should be addressed for the concrete implementation of Article 17(7) and (9)? If yes, please explain which ones and how the guidance should address them.

2600 character(s) maximum

The ECtHR's case-law has reiterated that the simple impression of imbalance in the defendant's rights suffices to infringe the right to a fair trial under Article 6(1) - see Borgers v Belgium App no 12005/86 (1991) 15 EHRR 92 [29]. The EC Impact Assessment states that when rightholders provide the contents or fingerprints needed for notice and staydown to function, the effect is likely to be limited or overridden by the positive effects of such a solution - at page 151. However, it could be argued that rather than just being left to rightholders to decide, Article 17 should make it a mandatory legal requirement that the determination as to whether a specific use of content is permitted is explicitly set out Member State law. Importantly, Urban, Karaganis, and Schofield state the statistic that each week Google receives millions of takedown requests, of which over 15% fail to sufficiently identify the allegedly infringed file or the supposed infringing content. It stresses that this is particularly concerning as detecting the file in question is essential to assessing claims as well as removing material (Urban, Karaganis, and Schofield 2016, 12). Thus, perhaps unsurprisingly, in Promusicae v Telefonica, the AG advised that requiring the participation of State authorities was crucial because unlike rightholders – and indeed unlike the DSM Directive – these authorities took into account circumstances which exempted users suspected of infringement - see [AG 114]. It can be noted that this is consistent with Urban, Karaganis, and Schofield (2016) report, which echoes that since the decision to takedown material might be context-dependent, rightholders often take down particular uses of content indiscriminately. It explains that what sets the boundaries between 'tolerated' and 'unacceptable' use curiously differs from rightholder to rightholder. Moreover, it elaborates that to assess what constitutes 'tolerated' use, and relying on YouTube's Content ID, rightholders block clearly illegal uses, monetize borderline cases or enable transformative uses without monetization (Urban, Karaganis, and Schofield 2016, 57–59). To put it differently, under Article 17 cases with similar facts are unlikely to achieve similar results because what amounts to 'tolerated'

and ‘unacceptable’ use can vary greatly between rightholders. Accordingly, it should be a mandatory legal requirement that the determination as to whether a specific use of content is ‘tolerated’ and ‘unacceptable’ is explicitly set out Member State law.

V. INFORMATION TO RIGHTHOLDERS (Art. 17(8))

Background

Under Article 17(8), online content-sharing service providers need to provide rightholders, at their request, with information on the functioning of the tools used for ensuring the unavailability of content. Where they conclude licensing agreements with rightholders, the service providers also need to provide them with information on the use of their content, without however having to provide rightholders with detailed and individualised information for each work or other subject matter identified (recital 68).

Possible elements for the guidance

The guidance should recall the different elements set out in Article 17(8) and explain in particular how Member States should direct the parties to apply this provision in practice. It should give indications as to the information that service providers should provide to rightholders, if requested, to comply with it. For example, information on content recognition tools deployed by service providers to avoid unauthorised content could include descriptions on the efficiency of these tools, the general parameters used for their deployment, as well as any changes made overtime to the operation of these tools. As regards information on the use of content covered by the agreements concluded between service providers and rightholders, the guidance should recall that service providers are not required to provide detailed and individualised information on each work, and encourage the development of standardised reporting through voluntary cooperation between stakeholders. Some more specific requirements on reporting exist already under Article 17 of Directive 2014/26/EU and govern the relationship between users and CMOs.

In line with the Commission Recommendation on illegal content online, in order to ensure a high level of transparency to users, the guidance could recommend that Member States encourage online contentsharing service providers to publicly report on the functioning of their practices with regard to Article 17(4).

Question 16: What are the most important elements that the guidance should cover in relation to the information that online content-sharing service providers should provide to rightholders on the functioning of their tools to ensure the unavailability of unauthorised content and on the use of rightholders’ content under Article 17(8)? Please provide examples of particular information that you would consider as covered by this obligation.

2600 character(s) maximum

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). In this context, it would be advisable for the EC to clarify what type of information should be set out in the staydown injunction and the parameters for these injunctions to be compatible with international law. For instance, it is arguable that the scope

of ratione personae, ratione materiae and ratione temporis of the surveillance and technical measures required to implement monitoring systems should be set out in the injunction that is, the number of users and services to be affected, the types of communications to be impacted and the time to be taken over the measures. Moreover, it should also be clarified the level of examination required to perform user monitoring, namely, Deep Packet Inspection (DPI), Shallow Packet Inspection (SPI) or both.

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).

Question 17: Are there any other elements beyond the ones listed above which should be covered by the guidance? If yes, please explain which ones and how you would suggest the guidance to address them.

2600 character(s) maximum

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:

The first procedural safeguard should be for the different types of works to be protected to be specifically set out, thereby being made accessible to the public.

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.

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.

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.

The fifth procedural safeguard should be for upload filters to only target Deep Packet Inspection 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 commercialscale uploaders.

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.

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.

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.

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

VI. OTHER TOPICS

Question 18: Do you think the guidance should address any other topic related to Article 17? If yes, please indicate which topics you consider should be included in the guidance and how you consider the guidance should address them.

2600 character(s) maximum

The EC should additionally consider to what extent Article 17 of the EU Directive on Copyright in the Digital Single Market 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. For guidance, please see Romero-Moreno, Felipe (17 March 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 https://www.tandfonline.com/doi/full/10.1080/13600869.2020.1733760

FINAL REMARKS

Should you wish to upload any other documentation to support your views, please do so.

Please upload your file

The maximum file size is 1 MB

Contact

EC-COPYRIGHT-DIALOGUES@ec.europa.eu