The Death of 'No Monitoring Obligations'

A Story of Untameable Monsters

by **Giancarlo F. Frosio***

Abstract: In imposing a strict liability regime for alleged copyright infringement occurring on YouTube, Justice Salomão of the Brazilian Superior Tribunal de Justiça stated that "if Google created an 'untameable monster,' it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites." In order to tame the monster, the Brazilian Superior Court had to impose monitoring obligations on Youtube; this was not an isolated case. Proactive monitoring and filtering found their way into the legal system as a privileged enforcement strategy through legislation, judicial decisions, and private ordering. In multiple jurisdictions, recent case law has imposed proactive monitoring obligations on intermediaries across the entire spectrum of intermediary liability subject matters. Legislative proposals have followed suit. As part of its Digital Single Market Strategy, the European Commission, would like to introduce filtering obligations for intermediaries in both copyright and AVMS legislations. Meanwhile, online platforms have already set up miscellaneous filtering schemes on a voluntary basis. In this paper, I suggest that we are witnessing the death of "no monitoring obligations," a well-marked trend in intermediary liability policy that can be contextualized within the emergence of a broader move towards private enforcement online and intermediaries' self-intervention. In addition, filtering and monitoring will be dealt almost exclusively through automatic infringement assessment systems. Due process and fundamental guarantees get mauled by algorithmic enforcement, which might finally slay "no monitoring obligations" and fundamental rights online, together with the untameable monster.

Keywords: Proactive monitoring obligations; filtering obligations; intermediaries; fundamental rights online

Recommended citation: Giancarlo F. Frosio, The Death of 'No Monitoring Obligations': A Story of Untameable Monsters, 8 (2017) JIPITEC 199 para 1.

A. Introduction

1 In the next few pages, I will be telling you a story that is in between a dark fairy tale and mystery fiction. This story is filled with monsters—untamable ones—and its protagonist has been murdered or at least might be in danger of sudden death. However, let us start from the beginning as any good story is supposed to start.

2 Once upon a time there was "no monitoring obligation." Traditionally, online service providers have enjoyed an exemption to any general obligation to monitor the information, which they transmit or store or actively seek facts or circumstances indicating illegal activity.[1] Together with safe harbor provisions that impose liability on hosting providers according to knowledge-and-take-down,[2] the "no

* Senior Researcher and Lecturer, Center for International Intellectual Property Studies (CEIPI), Universitè de Strasbourg; Non-Resident Fellow, Stanford Law School, Center for Internet and Society. The author can be reached at gcfrosio@ceipi.edu.

1 See eg Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ (L 178) 1-16 [hereinafter eCommerce Directive] Art 15; The Digital Millennium Copyright Act of 1998, 17 USC § 512(m) (United States) [hereinafter DMCA].

2 See eg eCommerce Directive (n 1) Art 12-15; DMCA (n 1) § 512(c)(1)(A-C).

monitoring obligations" rule set up a negligence-based intermediary liability system. Online hosting providers may become liable only if they do not take down allegedly infringing materials promptly enough upon knowledge of their existence, usually given by a notice from interested third-parties.[3] Although imperfect because of considerable chilling effects,[4] a negligence-based intermediary liability system has inherent built-in protections for fundamental rights. The European Court of Justice has confirmed multiple times—at least with regard to copyright infringement—that there is no room for proactive monitoring and filtering mechanisms under EU law.[5] Again, the Joint Declaration of the Three Special Rapporteurs on Freedom of Expression calls against the imposition of duties to monitor the legality of the activity taking place within the intermediaries' services.[6]

3 However, rumor has it that the principle of "no monitoring obligations"—and the negligence-based system it propels—might be in great danger, if it has not been killed off already. A fundamental tenet of online intermediaries' governance has been increasingly challenged.[7] Who killed—or is trying to kill—"no monitoring obligations"? And why? The predicament in which the principle of no proactive monitoring finds itself is the result of miscellaneous concomitant factors and spans all subject matters relevant to intermediary liability online. In search of the culprit, this paper will investigate recent case law, law reform, and private ordering.[8]

B. Untameable Monsters, Internet Threats and Value Gaps

4 As mentioned, this is a story of untameable monsters. These monsters have recently been seen in Brazil, apparently in the proximities of the Brazilian *Superior Tribunal de Justiça* (STJ). In imposing a strict liability regime for alleged copyright infringement occurring on YouTube, Justice Luis Felipe Salomão of the Brazilian STJ stated that "if Google created an 'untameable monster,' it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites."[9] As per Justice Salomão's metaphor, the dangers for "no monitoring obligations" might follow as reaction to a fear for technological innovation that has posed unprecedented challenges to semiotic governance.

5 By evoking the untamable monster, Justice Salomão echoes a recurrent narrative in recent intermediary liability—especially copyright—policy. This narrative has focused on the "threat" posed by digitalisation and internet distribution.[10] It has led to overreaching expansion of online enforcement. The Court in *Dafra* stressed the importance of imposing liability on intermediaries, stating that "violations of privacy of individuals and companies, summary trials and

3 Please consider that there is no direct relation between liability and exemptions, which function as an extra layer of protection intended to harmonize at the EU level conditions to limit intermediary liability.

4 See e.g. Wendy Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (2010) 24 Harv J L & Tech 171, 175–76; Center For Democracy & Technology, Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech 1-19 (September 2010). There is abundant empirical evidence of "over-removal" by internet hosting providers. See eg Althaf Marsoof, 'Notice and Takedown: A Copyright Perspective' (2015) 5(2) Queen Mary J of Intell Prop 183, 183-205; Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (2014) 18 Va J L & Tech 369; Jennifer Urban and Laura Quilter, 'Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara Comp and High Tech L J 621; Lumen <www.lumendatabase.org> (formerly Chilling Effects—archiving takedown notices to promote transparency and facilitate research about the takedown ecology). However, recent U.S. caselaw gave some breathing space to UGC creators from bogus takedown notices in cases of blatant misrepresentation of fair use defences by copyright holders. See Stephanie Lenz v. Universal Music Corp, 801 F.3d 1126, 1131 (9th Cir 2015) (holding that "the statute requires copyright holders to consider fair use before sending takedown notifications").

5 See Case C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECLI:EU:C:2011:771 (re-stating the principles in favour of access providers); C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* [2012] ECLI:EU:C:2012:85 (confirming the principle in favour of hosting providers).

6 See Joint Declaration of the Three Special Rapporteurs for Freedom of Expression (2011) 2.b. <http://www.osce.org/fom/78309?download =true>.

7 See Giancarlo Frosio, 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe' (2017) 12 Oxford JIPLP (published online on 12 May) <https://doi.org/10.1093/jiplp/jpx061> (discussing a move from a negligence-based to a strict liability approach in recent proposals).

8 Please consider that this paper has chosen to give special emphasis to the review of case law on point. Private ordering and legislative proposals are described in lesser detail, both for reasons of space and because they have been the focus of other recent pieces from this author. See Frosio (n 7) (discussing filtering monitoring reform proposals); Giancarlo Frosio, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (2017a) 112 Northwestern U L Rev 19 (2017) (discussing reform proposals); Giancarlo Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2017b) <https://papers.ssrn.com/ abstract=2976023> (discussing private ordering).

9 Google Brazil v Dafra, Special Appeal No. 1306157/SP (Superior Court of Justice, Fourth Panel, 24 March 2014) <https://cyberlaw.stanford.edu/page/wilmap-brazil>.

10 See James Boyle, The Public Domain: Enclosing the Commons of the Mind (Yale University Press 2008) 54-82.

public lynching of innocents are routinely reported, all practiced in the worldwide web with substantially increased damage because of the widespread nature of this medium of expression."[11] A paradigmatic example of the "internet threat" discourse is Justice Newman's statement in *Universal v Corley*. Responding to the requests of the defendants not to use the Digital Millennium Copyright Act (DMCA) as an instrument of censorship, Justice Newman from the United States Court of Appeal of the Second Circuit replied: "[h]ere, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright."[12] In another landmark case, which recently appeared before the European Court of Human Rights (ECHR), the "Internet threat" discourse resurfaced again to impose proactive monitoring obligation on online news portals. This time discussing hate speech, rather than copyright infringement, the ECHR noted that in the Internet, "[d]efamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online."[13]

6 More recently, untameable monsters and Internet threats—perhaps of an imaginary type—have been evoked to justify the upcoming European copyright reform in the Digital Single Market and the introduction of filtering obligations for online intermediaries. The proposal for a Directive on Copyright in the Digital Single Market aims—*inter alia*—to close the so-called 'value gap' between Internet platforms and copyright holders.[14] Calling for a fairer allocation of value generated by the online distribution of copyright-protected content by online platforms,[15] the Communication on Online Platforms and the Digital Single Market noted that rebalancing is needed because "new forms of online content distribution have emerged [...] that may make copyright protected content uploaded by end-users widely available."[16] The idea of a 'value gap' echoes a discourse almost exclusively fabricated by the music and entertainment industry,[17] which appears to be scarcely concerned with empirical evidence. The European Copyright Society stressed this point by noting: 'we are disappointed to see that the proposals are not grounded in any solid scientific (in particular, economic) evidence."[18] Actually, the Draft Directive's Impact Assessment itself admits lack of empirical support quite plainly by noting that "the limited availability of data in this area [. . .] did not allow to elaborate a quantitative analysis of the impacts of the different policy options."[19] Moreover, a Report commissioned by the European Commission—and delivered in May 2015 but released only recently following an access to document request from a Pirate Party's MEP[20]—showed that there is actually no "robust statistical evidence of displacement of sales by online copyright infringements."[21] In sum, reform and enforcement expansion is based on unfounded assumptions. In contrast, the literature has shown to a certain degree of consistency that there is in fact an added value to promote, rather than a value gap to close.[22] Overlooking this empirical evidence—or at least moving forward without an impact statement that would consider all evidence and possible narratives—does characterize the reform as a reactionary measure to volatile fears

11 Dafra (n 9) § 5.4.

12 Universal v Corley, 273 F.3d 429, 60 U.S.P.Q.2d 1953, 1968 (2nd Cir. 2001).

13 *Delfi AS v. Estonia* N 64569/09 (ECHR, 16 June 2015) § 110.

14 Commission, 'Proposal for a Council Directive on Copyright in the Digital Single Market' COM (2016) 593 final, art 13.

15 Communication from the Commission to the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe, COM(2016) 288 Final (May 25, 2016) 9.

16 *Id.*

17 See Martin Husovec, 'EC Proposes Stay-down & Expanded Obligation to Licence UGC Services' (*Hut'ko's Technology Law Blog*, 1 September 2016) <http://www.husovec.eu/2016/09/ec-proposes-stay-down-expanded.html>.

18 European Copyright Society, General Opinion on the EU Copyright Reform Package (24 January 2017) 5.

19 Commission, 'Staff Working Document, Impact Assessment on the Modernisation of EU Copyright Rules' SWD (2016) 301 final, PART 1/3, p 136. In general, there is no clear evidence on the effects of copyright infringement in the digital environment, the scale of it, the nature of it, or the effectiveness of more aggressive enforcement strategies. See Ian Hargreaves, 'Digital Opportunity. A Review of Intellectual Property and Growth' (May 2011) 10. See also Joe Karaganis, 'Rethinking Piracy', in Joe Karaganis (ed), *Media Piracy in Emerging Economies* (Social Science Research Center 2011) 4-11 (making the same point).

20 See Julia Reda, What the Commission Found Out About Copyright Infringement but 'Forgot' to Tell Us, (JuliaReda.eu, 20 September 2017) <https://juliareda.eu/2017/09/secret-copyright-infringement-study>.

21 Martin van der Ende, Joost Poort, Robert Haffner, Patrick de Bas, Anastasia Yagafarova, Sophie Rohlfs, Harry van Til, *Estimating Displacement Rates of Copyrighted Content in the EU: Final Report*, European Commission, May 2015, 7.

22 See, for an extended review of the literature proving this point, Giancarlo Frosio, 'Digital Piracy Debunked: A Short Note on Digital Threats and Intermediary Liability' (2016) 5(1) Internet Policy Review 1-22 <http://policyreview.info/articles/analysis/digital-piracy-debunked-short-note-digital-threats-and-intermediary-liability>. See also eg Michael Masnick and Michael Ho, The Sky is Rising: A Detailed Look at the State of the Entertainment Industry (Floor 64, January 2012), <http://www.techdirt.com/skyisrising>; Joel Waldfogel, 'Is the Sky Falling? The Quality of New Recorded Music Since Napster' (VOX, 14 November 2011) <http://www.voxeu.org/index.php?q=node/ 7274>.

based on a moral approach rather than a welfare cost/benefit analysis.[23]

C. Private Ordering

7 Filtering and proactive monitoring have been increasingly sought—and deployed—as enforcement strategies online. Proactive monitoring comes first—and largely—as a private ordering approach following rightholders and government pressures to purge the Internet from allegedly infringing content or illegal speech. In the midst of major lawsuits launched against them,[24] YouTube and Vimeo felt compelled to implement filtering mechanisms on their platforms on a voluntary basis. Google lunched Contend ID in 2008.[25] Vimeo adopted Copyright Match in 2014.[26] Both technologies rely on digital fingerprinting to match an uploaded file against a database of protected works provided by rightholders.[27] Google's Content ID—but Copyright Match works similarly—applies four possible policies, including (1) muting matched audio in an uploaded video, (2) completely blocking a matched video, (3) monetizing a matched video for the copyright owner by running advertisement against it, and (4) tracking a match video's viewership statistics.[28] Tailoring of Contend ID policies is also possible and rightholders can block content in some instances and monetize in others, depending on the amount of copyrighted content included in the allegedly infringing uploaded file. The system also allows end-users to dispute copyright owners' claims on content.[29]

8 The promotion of private ordering is a strategy increasingly adopted by governments as—in Europe for example—it would allow to circumvent the EU Charter on restrictions to fundamental rights and avoid the threat of legal challenges.[30] The *Communication on Online Platforms and the Digital Single Market* puts forward the idea that "the responsibility of online platforms is a key and cross-cutting issue."[31] Again, few months later, in its most recent Communication, the Commission made this goal even clearer by openly pursuing 'enhanced responsibility of online platforms' on a voluntary basis.[32] In other words, the Commission would like to impose an obligation on online platforms to behave responsibly by addressing specific problems.[33] Online platforms would be invested by a duty to 'ensure a safe online environment' against illegal activities.[34] Hosting providers—especially platforms—would be called to actively and swiftly remove illegal materials, instead of reacting to complaints. They would be called to adopt effective voluntary '*proactive* measures to detect and remove illegal content online'[35] and are encouraged to do so by using automatic detection and filtering technologies.[36] As the Commission puts it, the goal is "to engage with platforms in setting up and applying voluntary cooperation mechanisms" [37], in particular by setting up a privileged channel with 'trusted flaggers', competent authorities and specialized private entities with specific expertise in identifying illegal content'.[38]

9 The adoption of voluntary filtering measures does expand beyond intellectual property enforcement to reach speech-related crimes. "Online platforms must be encouraged to take more effective voluntary action to curtail exposure to illegal or harmful content" such as incitement to terrorism, child sexual abuse and hate speech.[39] As an umbrella framework, the Commission recently agreed with all major online hosting providers—including Facebook, Twitter, YouTube and Microsoft—on a code of conduct that includes a series of commitments to combat the spread of illegal hate speech online in Europe.[40] Also, in partial response

23 See Frosio (n 8) 3-12.

24 See Viacom Int'l v. YouTube Inc 676 F3d 19 (2nd Cir 2012) (upholding YouTube's liability in the long lasting legal battle with Viacom by holding that Google and YouTube had actual knowledge or awareness of specific infringing activity on its website); Capitol Records LLC v. Vimeo 972 F Supp 2d 500 (SDNY 2013) (denying in part Vimeo's motion for summary judgment).

25 See YouTube, How Content ID Works <https://support.google.com/youtube/answer/2797370?hl=en>.

26 See Chris Welch, 'Vimeo Rolls Out Copyright Match to Find and Remove Illegal Videos' (*The Verge*, 21 May 2014) <https://www.theverge.com/2014/5/21/5738584/vimeo-copyright-match-finds-and-removes-illegal-videos>.

27 See YouTube (n 25).

28 ibid.

29 YouTube, Dispute a Content ID Claim <https://support.google.com/youtube/answer/2797454?hl=en>.

30 See, for an overview of private ordering strategies. Frosio (n 23).

31 Communication (n 15) 9.

32 See Communication from the Commission to the European Parliament, the Council, and the Economic and Social Committee, and the Committee of the Regions, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms, COM(2017)555final (September 28, 2017).

33 See Communication (n 15) 8.

34 Communication (32) § 3.

35 ibid § 3.3.1 (noting that adopting such voluntary proactive measures does not lead the online platform to automatically lose the hosting liability exemption provided by the eCommerce Directive

36 ibid § 3.3.2.

37 Communication (n 15) 8.

38 See Communication (32) § 3.2.1.

39 Communication (n 15) 9. See also Communication (32) § 1-2.

40 See Commission, European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech, Press Release (31 May 2016) <http://europa.eu/rapid/press-release_IP-16-1937_en.htm>.

to this increased pressure from the EU regarding the role of intermediaries in the fight against online terrorism, major tech companies announced that they will begin sharing hashes of apparent terrorist propaganda.[41] For some time, YouTube and Facebook have been using ContentID and other matching tools to filter "extremist content."[42] In this context, tech companies plan to create a shared database of unique digital fingerprints—knows as hashes—that can identify images and videos promoting terrorism.[43] This could include recruitment videos or violent terrorist imagery or memes. When one company identifies and removes such a piece of content, the others will be able to use the hash to identify and remove the same piece of content from their own network. The fingerprints will help identify image and video content that are "most likely to violate all of our respective companies' content policies".[44] Despite the collaboration, the task of defining removal policies will remain within the remit of each platform.[45]

D. Case Law

10 As mentioned, voluntary monitoring and filtering schemes emerged as a response to major lawsuits threatening online intermediaries. In fact, private ordering confirms a trend in recent intermediary liability policy that surfaced consistently in judicial decisions.[46] In multiple jurisdictions, case law has imposed proactive monitor obligations on online intermediaries for copyright infringement. However, proactive monitoring obligations have been spanning the entire spectrum of intermediary liability subject matters: intellectual property, privacy, defamation, and hate/dangerous speech.

11 Proactive monitoring obligations have been applied by courts on the basis of miscellaneous doctrines attempting to impose strict liability rather than negligence-based standards to intermediaries.[47] In Europe, for example, the eCommerce Directive also contains a provision that dilutes the notice-and-take-down principle by extending in specific circumstances liability beyond the liability upon knowledge. According to Art. 14(3) further obligations can be imposed by court or authority orders "requiring the service provider to terminate and prevent an infringement."[48] In this respect, the eCommerce Directive prohibits *general* monitoring obligations, although it does allow national law to provide for monitoring obligations "in a specific case."[49] The eCommerce Directive also acknowledges that Member States can impose duties of care on hosting providers "in order to detect and prevent certain types of illegal activities."[50] However, their scope should not extend to general monitoring obligations, if any meaning should be given to the previous statement in Recital 47 that only specific monitoring obligations are allowed. Moreover, the Directive states that duties of care should "*reasonably* be expected from the service providers," and no general monitoring obligation can fulfill such an expectation as they are explicitly barred by the Directive itself.[51] In order to distinguish general from specific monitoring obligations, it should be considered that (1) as an exception, specific monitoring obligations must be interpreted narrowly, (2) both the scope of the possible infringements and the amount of infringements that can be reasonably expected to be identified, must be sufficiently narrow, and (3) it must be obvious which materials constitute an infringement.[52] As Van Eecke noted

> *[i]f [clear criteria] are not defined, or only vague criteria are defined by the court (e.g. "remove all illegal videos"), or if criteria are defined that would oblige the hosting provider to necessarily investigate each and every video on its systems (e.g. "remove all racist videos"), or if the service provider were required also to remove all variations in the future (e.g.*

41 See 'Google in Europe, Partnering to Help Curb the Spread of Terrorist Content Online' (*Google Blog*, 5 December 2016) <https://blog.google/topics/google-europe/partnering-help-curb-spread-terrorist-content-online>.

42 See Joseph Menn and Dustin Volz, 'Exclusive: Google, Facebook Quietly Move Toward Automatic Blocking of Extremist Videos' (*Reuters*, 25 June 2016) <http://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M> (apparently, the "automatic" removal of extremist content is only about automatically identifying duplicate copies of video that were already removed through human review).

43 Olivia Solon, 'Facebook, Twitter, Google and Microsoft Team up to Tackle Extremist Content (*The Guardian,* 6 December 2016) <https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content>.

44 See 'Partnering to Help Curb Spread of Online Terrorist Content' (*Facebook Newsroom*, 5 December 2016) <https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content>.

45 ibid.

46 *See*, for full reference, summaries in English and links to most decision cited in the next few pages, The World Intermediary Liability Map (WILMap), <http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap> (a project designed and developed by Giancarlo Frosio and hosted at Stanford CIS).

47 See Broder Kleinschmidt, 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content' (2010) 18(4) IJLIT 332, 346-347.

48 See eCommerce Directive (n 2) Art. 14(3).

49 ibid Recital 47.

50 ibid Recital 48.

51 ibid (emphasis added).

52 See Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48(5) Common Market L Rev 1455, 1486-1487.

"remove this video, but also all other videos that belong to the same repertory"), a general monitoring obligation would be imposed.[53]

12 Although space limitation necessary constricts the scope of this review, this section will select several cases in multiple jurisdictions where monitoring obligations have been imposed. As said, this case law deals with the entire variety of potential infringements that may trigger online intermediary liability, proving that—also at the judicial level—the emergence of proactive monitoring obligations is a global intermediary liability policy trend. However, notable exceptions to this emerging trend—such as the landmark Belen case in Argentina—will also be considered.

I. Copyright: From Dafra to Baidu

13 Multiple judicial decisions have imposed proactive monitoring obligations for copyright infringement on hosting providers. Let us start by going back to the beginning of our story then. As mentioned earlier, the Brazilian STJ imposed proactive monitoring obligations on YouTube.[54] The Brazilian STJ found Google liable for copyright infringement for YouTube-hosted videos parodying a well-known commercial.[55] As such, Dafra stands as a perfect case study regarding the effects of filtering on freedom of expression online. Dafra is a motorcycle manufacturer, which broadcasted a commercial titled "Meetings," as part of a national advertising campaign known as "Dafra – You on Top."[56] Shortly after launching the advertising campaign, a YouTube user published a "fan-dub" of the original Dafra video.[57] In the user-generated parody version of Dafra's commercial, the actor's original voice was replaced by a very similar one making statements tarnishing Dafra's goodwill.[58] Google took down the initial video per Dafra's request, but several other versions of the video were posted constantly by other users under different titles.[59] Therefore, Dafra sued Google for copyright infringement, claiming that Google had not adopted the necessary measures to avoid further viewing of videos with the same content, regardless of the title that users may have given to those videos.[60] The plaintiff had asked Google not only to remove the video but also to use search blocking mechanisms to prevent posting any unauthorized material related to the "Dafra – You on Top" campaign on YouTube.[61]

14 The STJ upheld the plaintiff's claims for copyright infringement and ordered Google to remove all the adulterated advertisements within 24 hours, under a penalty of R$ 500 per day for noncompliance.[62] According to the decision, Google must remove not only the infringing video, which is the object of the lawsuit, but also any similar and related unauthorized videos, even if they are uploaded by other users and bear a different title.[63] However, the Court recognized "certain limitations of proactive control."[64] The judgment does not address future videos and Google's obligation only reaches unauthorized videos with "Dafra – You on Top" in the title.[65] In fact, Google claimed a "technical impossibility" defense, arguing that it was impossible to take down all videos because there are currently no blocking filters able to identify all infringing materials.[66] Justice Salomão—the rapporteur of the case—quashed Google's "technical impossibility defense" because lack of technical solutions for fixing a defective new product does not exempt the manufacturer from liability, or from the obligation of providing a solution.[67] If Google created an 'untamable monster,'—Justice Salomão continued—"it should be the only one charged with any disastrous consequences generated by the lack of control of the users of its websites."[68]

15 *Dafra* is not an isolated case. Recently, several European national decisions implemented proactive monitoring obligations for hosting providers in apparent conflict with a well settled jurisprudence of the CJEU. In *Allostreaming*—a landmark case in France—the Paris Court of Appeal confirmed in part a previous decision of the *Tribunal de Grande Instance*.[69] The Court imposed on access providers

53 ibid 1487.

54 See Dafra (n 9). See also Giancarlo Frosio, 'Brazilian Supreme Court Found Google Liable for Videos Parodying Dafra's Commercials' (*CIS Blog*, 31 January 2014) <https://cyberlaw.stanford.edu/blog/2014/01/brazilian-supreme-court-found-google-liable-videos-parodying-dafra%E2%80%99s-commercials>.

55 See Dafra (n 9) § 1.

56 ibid.

57 ibid.

58 ibid. See also YouTube, This video is unavailable <https://www.youtube.com/watch?v=luu_73y_hCk>.

59 See Dafra (n 9) § 1.

60 ibid.

61 ibid.

62 ibid § 8.

63 ibid § 5.2.

64 ibid.

65 ibid.

66 ibid § 4.

67 ibid § 5.4

68 ibid.

69 See APC et al v. Google, Microsoft, Yahoo!, Bouygues et Al (Cour d'Appel Paris, 16 March 2016) (France) [hereinafter Allostreaming 2016] confirming APC et al v. Google, Microsoft, Yahoo!, Bouygues et Al (TGI Paris, 28 November 2013) (France). See also Laura Marino, 'Responsabilités civile et pénale des fournisseurs d'accès et d'hébergement' (2016) 670 JCl. Communication 71, 71-79. But see TF1 v.

an obligation to block the illegal movie streaming website Allostreaming and affiliated enterprises. In addition, search engines, including Google, Yahoo! and Bing, are obliged to proactively expunge their search results from any link to the same websites.[70] Notably, the appellate decision reversed the first instance on the issue of costs allocation. According to the Court of Appeal, all costs related to blocking and delisting sixteen Allostreaming websites should be sustained by the search engines, rather than being equally shared as previously decided.[71] As to be considered later, the stand taken by the Paris Court of Appeal has obvious implications in regard to the inadequate balance with freedom to conduct business that monitoring obligations might bring about as discussed multiple times by the CJEU. In laying down its arguments for proactive monitoring and cost allocation, *Allostreaming* also evokes the specter of the untamable monster. The Court remarked that rightholders are "confronted with a massive attack" and are "heavily threatened by the massive piracy of their works."[72] Hence, the Court continues, it is "legitimate and in accordance with the principle of proportionality that [ISPs and search engines] contribute to blocking and delisting measures" because they "initiate the activity of making available access to these websites" and "derive economic benefit from this access (especially by advertising displayed on their pages)."[73] Regardless the logic of the argument, proactive monitoring and imposition of liability to innocent third parties is apparently still upheld by endorsing an Internet threat discourse.

16 Under the Telemedia Act, German courts found that host providers are ineligible for the liability privilege if their business model is mainly based on copyright infringement. In two disputes involving the Swiss-based file-hosting service, RapidShare, the Bundesgerichtshof (German Supreme Court) imposed monitoring obligations on RapidShare.[74] According to the Court, although RapidShare's business model is not primarily designed for violating rights, it nevertheless provides incentives to third parties to illegally share copyrighted content.[75] Therefore, as the Bundesgerichtshof also announced in Atari Europe v. RapidShare,[76] RapidShare—and similar file-hosting services—should abide to more stringent monitoring duties.[77] According to the Court, a hosting provider is not only required to delete files containing copyrighted material as soon as it is notified of a violation by the right holder, but must also take steps to prevent similar infringements by other users in the future.[78] File-hosting services are required to actively monitor incoming links to discover copyrighted files as soon as there is a specific reason to do so and to then ensure that these files become inaccessible to the public.[79] As indicated by the Court, the service provider should use all possible resources - including search engines, Facebook, Twitter, or web crawlers - to identify links made accessible to the public by user generated repositories of links.[80]

17 In Italy, a mixed case law emerged. Some courts imposed proactive monitoring obligations on intermediaries, whereas other courts took the opposite stance and confirmed that there is no monitoring obligation for intermediaries under European law.[81] There is a long-lasting legal battle between Delta TV and YouTube being fought before

DailyMotion (Cour d'Appel Paris, 2 December 2014) (stating that DailyMotion enjoys limitation of liability as a hosting provider and is not required to proactively monitor users' infringing activities). See also Giancarlo Frosio, 'France DailyMotion pays Damages for Late Removal of Infringing Materials' (*CIS Blog*, 8 December 2014) <https://cyberlaw.stanford.edu/blog/2014/12/france-dailymotion-pays-damages-late-removal-infringing-materials>.

70 See Allostreaming 2016 (n 69) 7.

71 ibid 42.

72 ibid.

73 ibid

74 See GEMA v RapidShare I ZR 79/12 (Bundesgerichtshof, August 15, 2013) (Germany) (where the German copyright collective society, GEMA, sued RapidShare in Germany, alleging that over 4,800 copyrighted music files were shared via RapidShare without consent from GEMA or the right holder). An English translation is here: <https://stichtingbrein.nl/public/2013-08-15%20BGH_RapidShare_EN.pdf>.

75 ibid.

76 See Atari Europe v. RapidShare I ZR 18/11 (Bundesgerichtshof, July 12, 2012) (Germany) (in this case, RapidShare neglected to check whether certain files violating Atari's copyright over the computer game "Alone in the dark" were stored on its servers by other users).

77 See GEMA v. RapidShare (n 74); Atari Europe v. RapidShare (n 76).

78 ibid.

79 See GEMA v. RapidShare (n 74) § 60.

80 ibid.

81 For case law confirming the safe harbour and no-monitoring obligations, see Reti Televisive Italiane S.p.A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) et al, N RG 3821/2011 (Milan Court of Appeal, 7 January 2015) (reversing a previous decision regarding the publication of fragments of television programs through the now-terminated Yahoo! Video service and clarified that RTI had the obligation to indicate in a "detailed, precise and specific manner" the videos that Yahoo! had to remove and the court of first instance could not "impose to a hosting provider general orders or, even worse, general monitoring obligations, which are forbidden by Directive 2000/31/EC"); Mediaset Premium S.p.a. v. Telecom Italia S.p.a. et al (Milan Tribunal, 27 July 2016) (discussing a blocking injunction against Calcion. at and clarifying that mere conduit internet providers do not have an obligation to monitor their networks and automatically remove content). See also Reti Televisive Italiane S.p.A. (RTI) v. TMFT Enterprises LLC- Break Media, (Rome Tribunal, 27 April 2016) (confirming no monitoring obligations but stating that rightholders do not need to list the URLs where the videos are made available).

the Tribunal of Turin. Delta TV sued Google and YouTube for copyright infringement of certain South American soap operas that users had uploaded to YouTube. In this case, Google complied with its notice-and-take-down policy, and the videos were removed as soon as the specific URLs were provided by Delta TV. In one interim decision, the Court agreed with Delta TV's claims and ordered Google and YouTube to remove the infringing videos and to prevent further uploads of the same content through the use of its Content ID software using as a reference the URLs provided by Delta TV.[82] The Court stressed that these proactive monitoring obligations derive from the fact that YouTube is a "new generation" hosting service, a role that brought on it a greater responsibility to protect third parties' rights.[83] More recently, the Tribunal of Turin delivered a final decision on the matter, confirming the previous decision and an obligation for YouTube to partially monitor its network by preventing the re-uploading of content previously removed.[84] The Court noted that "there subsists on YouTube an actual legal obligation to prevent further uploads of videos already flagged as infringing of third-party copyrights."[85] This would be—according to the Court—an *ex post* specific obligation or duty of care in line with Recital 40 of the eCommerce Directive. It is worth noting that multiple Italian cases applied a reasoning similar to that of the Brazilian STJ in *Dafra*, by stating that any hosting providers, whether active or passive, have an obligation to prevent the repetition of further infringements once they have actual knowledge of the infringement, according to the principle *cuius commoda, eius et incommoda* ("a party enjoying the benefits [of an activity] should bear also the inconveniences").[86] This civil law principle refers to a form of extra-contractual (or tort) liability for which whoever benefits from a certain activity should be liable for any damages that such activity may cause.

18 In China, the Beijing Higher People's Court developed an interesting standard for proactive monitoring. In the *Baidu* case, the Court set up a duty to monitor for hosting providers based on popularity of infringed works and high-volume views/downloads.[87] The plaintiff Zhong Qin Wen found his copyrighted works—in particular the short book *English Learning Diary of Koala Xiaowu – to Those Fighting for Their Dreams* (《考拉小巫的英语学习日记——写给为梦想而奋斗的人》)—made available on the platform BaiduWenku and sued Baidu for copyright infringement.[88] According to the High Court of Beijing, by using current technologies, it was reasonable for Baidu to exercise a duty to monitor and examine the legal status of an uploaded work once it has been viewed or downloaded more than a certain number of times.[89] According to the Court, Baidu needs to inspect the potential copyright status of the work by contacting the uploader, checking whether the work is originally created by the uploader or legally authorized by the copyright owners.[90] Apparently, this case sets a duty for Internet hosting providers to protect popular works that attract many views and downloads. However, both Beijing First Immediate People's Court and Beijing Higher People's Court failed to set a clear indication of how many views or downloads are enough to trigger the duty, thus making uncertain intermediaries' proactive monitoring obligations.[91]

Belen Rodriguez and Beyond: Exceptions to an Emerging Global Trend

19 Notable exceptions to this trend in enforcing proacting monitoring obligations highlight, however, some fragmentation in the international response to intermediary liability. A recent landmark case decided by the Argentinian Supreme Court rejected any filtering obligation to prevent infringing links from appearing in search engines' results in the future.[92] The case was brought forward by a well-

82 *See* Delta TV v Youtube, N RG 15218/2014 (Tribunal of Turin, 23 June 2014) (revising en banc a previous decision rejecting Delta TV's request on the basis that (i) there is no obligation on the part of Google and YouTube, as hosting providers, to assess the actual ownership of the copyrights in videos uploaded by individual users). See also Eleonora Rosati, 'Italian court says that YouTube's Content ID should be used to block allegedly infringing contents' (*IPKat*, 21 July 2014) <http://ipkitten.blogspot.fr/2014/07/italian-court-says-that-youtubes.html>.

83 ibid 12.

84 See Delta TV v Google and YouTube, N RG 38113/2013 (Turin Tribunal, 7 April 2017).

85 Eleonora Rosati, 'Italian court finds Google and YouTube liable for failing to remove unlicensed content (but confirms eligibility for safe harbour protection)' (*IPKat*, 30 April 2017) <http://ipkitten.blogspot.fr/2017/04/italian-court-finds-google-and-youtube.html>.

86 See eg David Drummond et al, N 1972/2010 (Milan Tribunal, Criminal Section, 16 April 2013) <http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf> (discussing the notorious Vividown case and convicting Google executives for violating data protection law, in connection with the online posting of a video showing a disabled person being bullied and insulted). See also Giovanni Sartor and Mario Viola de Azevedo Cunha, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (2010) 18(4) Int J law Info Tech 356, 373-374.

87 See Zhong Qin Wen v Baidu, 2014 Gao Min Zhong Zi, No. 2045 (Beijing Higher People's Court 2014) <https://cyberlaw.stanford.edu/page/wilmap-china>.

88 ibid.

89 ibid.

90 ibid.

91 ibid.

92 Rodriguez M. Belen c/Google y Otro s/ daños y perjuicios, R.522.XLIX. (Supreme Court, October 29, 2014) (Argentina). See also Pablo Palazzi and Marco Jurado, 'Search Engine Liability for Third Party Infringement' (2015) 10(4) JIPLP

known public figure—Belen Rodriguez—for violation of her copyright, reputation and privacy.[93] This case is one among numerous civil lawsuits brought against the search engines Google and Yahoo! by different 'celebrities' and well-known public figures for violation of their reputation and privacy.[94] The case discussed the question whether search engines are liable for linking in search results to third-party content that violates fundamental rights or infringes copyright. Initially, some lower courts found search engines strictly liable under Article 1113 of the Civil Code, which imposes liability, regardless of knowledge or intention, to those performing risky acts, such as indexing third party content creating wider audiences for illegitimate content, or serving as the "guardians" of the element that generates the damage, such as the search engine's software.[95] Finally, the Argentinian Supreme Court: (1) repudiated a strict liability standard and adopted a test based on actual knowledge and negligence; (2) requested judicial review for issuing a notice to take down content—except in a few cases of "gross and manifest harm"; and (3) rejected any filtering obligation to prevent infringing links from appearing in the future.[96] In the rather extreme view taken by the Argentinian Supreme Court, as a default rule, actual knowledge—and possibly negligence—would only arise after a judicial review has upheld the issuance of the notice. In any event, this conclusion—and the transaction costs that brings about—is mitigated by a category of cases exempted from judicial review that might finally be quite substantial. Apparently, the Argentinian Supreme Court believes that, if harm is not manifest, a balancing of rights might be necessary, which can be done only by a court of law, rather than a private party.

20 Indeed, multiple national decisions in Europe have denied the applications of monitoring obligations in application of the eCommerce Directive legal framework. Mixed approaches apparent in the Italian courts have been mentioned earlier. A good example of the court's rationale in these cases can be found in one of the Telecinco cases in Spain. The Madrid Court of Appeal dismissed the request of Telecinco—a Spanish broadcaster owned by the Italian Mediaset—to issue an injunction towards potential future infringements on YouTube. The Spanish Court laid out a set of arguments showing how European law and jurisprudence would pre-empt proactive monitoring at the national level. Although the CJEU interpreted Article 11 of the Enforcement Directive as meaning that an ISP may be ordered "to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind,"[97] the Madrid Court said, it also made clear that this rule "may not affect the provisions of Directive 2000/31 and, more specifically, Articles 12 to 15 thereof ... which prohibits national authorities from adopting measures which would require a hosting service provider to carry out general monitoring of the information that it stores."[98]A possible injunction against future infringements—the Court of Appeal concluded—would result either in an order to monitor UGCs proactively, contrary to the E-Commerce Directive, or in an obligation to implement a filtering system that, according to the CJEU, would seriously endanger ISPs' freedoms to conduct business and users' fundamental rights, including data protection and freedom of information.[99]

II. Trademark: The Internet Auction Cases

21 Proactive monitoring does not only emerge in copyright enforcement. Trademark enforcement has seen courts imposing upon intermediaries similar obligations.[100] In a series of landmark decisions, the German Federal Court of Justice—*Bundesgerichtshof*—imposed supplementary duties on host providers in addition to notice-and-takedown obligations.[101] A

244; Marco Rizzo Jurado, 'Search engine liability arising from third parties infringing content: a path to strict liability?' (2014) 9(9) JIPLP 718, 718-720.

93 See Belen (n 92).

94 See eg S. M., M. S. c/ Yahoo de Argentina SRL y Otro s/ daños y perjuicios, N 89.007/2006; AR/JUR/XXXXX/2013 (Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, 6 November 2013); Da Cunha, Virginia c. Yahoo de Argentina S.R.L. and Google, N 99.620/2006, AR/JUR/40066/2010 (Cámara Nacional de Apelaciones en lo Civil de la Capital Federal, 10 August 2010).

95 See eg Yahoo (n 94).

96 See Belen (n 92).

97 C-324/09 *L'Oréal SA and Others v. eBay International AG and Others* (2012) § 144.

98 See C-360/10 (n 5) § 32-33; C-324/09 (n 97) § 139.

99 ibid § 48.

100 See, for a general overview of intermediary liability for online trademark infringement, Graeme B. Dinwoodie, 'Secondary Liability for Online Trademark Infringement: The International Landscape' (2014) 37 Colum J L & Arts 463; Barton Beebe, 'Tiffany and Rosetta Stone - Intermediary Liability in U.S. Trademark Law' (2012) 41 CIPA Journal 192.

101 See Rolex v Ebay/ Ricardo (a.k.a. *Internetversteigerung* I) I ZR 304/01 (BGH 11 March 2004) § 31; Rolex v. eBay (a.k.a. *Internetversteigerung* II), I ZR 35/04 (BGH, 19 April 2007) (Germany); Rolex v. Ricardo (a.k.a. *Internetversteigerung* III), Case I ZR 73/05, (BGH, 30 April 2008) (Germany). See also L'Oreal v Ebay [2009] EWHC 1094 (Ch), 455-465 <http://www.bailii.org/ew/cases/EWHC/Ch/2009/1094.html> (for an English summary of the German Federal Court's decisions regarding internet auctions); Van Eecke (n 52) 1476-1478; Anne Cheung and Kevin Pun, 'Comparative study on the liability for trade mark infringement of online auction providers' (2009) 31(11) EIPR 559, 559-567.

seller on eBay sold replica Rolex watches and posted them on eBay by using the Rolex brand. Together with trademark infringement against the primary infringer, Rolex claimed that eBay, was also liable for supplying the platform for the seller to infringe her rights.[102] In particular, Rolex sought that eBay should not only take the infringing content down, but also prevent future infringements that are similar or identical to a present infringement.[103] In the so-called Internet Auction cases I-III, the German *Bundesgerichtshof* repeatedly decided that notified trademark infringements oblige internet auction platforms such as eBay to investigate future offerings—manually or through software filters—in order to avoid further trademark infringement, if the necessary measures are possible and economically reasonable.[104]

22 The *Bundesgerichtshof* based its decision on the German doctrine of *Störerhaftung*—a property law doctrine applied by analogy to intellectual property. Actually, the same doctrine has also been applied by German courts in the *RapidShare* cases mentioned earlier and other copyright cases. According to Sec. 1004 of the German Civil Code the proprietor enjoys a right to (permanent) injunctive relief against anybody who has caused an interference with the property—so called *Störer* (interferer in English).[105] However, nobody should be held liable as a *Störer* if the duty would burden him unreasonably. The German Courts struggled with the notion of what was "technically possible" and "reasonable." The third *Internetversteigerung* case found precautions against clearly noticeable infringements reasonable, such as blatant counterfeit items.[106] In contrast, it would be unreasonable to implement a filtering obligation that questions the business model of the intermediary.[107]

23 In a later decision, the *Bundesgerichtshof* tuned down its view of reasonable precautionary means. It noted that manually checking and visually comparing each product offered in an online auction against infringement—which was not clear or obvious—would be unreasonable.[108] In particular, the Court noted that obligations are unreasonable if due to the substantial amount of products offered, the platform's business model would be endangered.[109] Offering filtering tools to trade mark holders—as eBay does—in order to perform such manual checks themselves would be apparently sufficient.[110]

III. Privacy: The Max Mosley Saga

24 The long-standing saga of Max Mosley's sexual images has offered European courts a new opportunity to strike a balance between freedom of expression and the right to privacy in light of the ubiquitous distribution power of Internet search engines. Courts in France, Germany, and the UK, imposed proactive monitoring obligations to search engines, which were ordered to expunge the Internet from pictures infringing the privacy rights of Max Mosley—former head of the *Fédération Internationale de l'Automobile*. In 2008, the *News of the World* newspaper published photos of Max Mosley engaged in sexual roleplaying with prostitutes dressed as German prison guards. The *News of the World's* headline accompanying the photos referred to a "Sick Nazi Orgy."[111] Mosley successfully sued the newspaper in the United Kingdom and later in France for breach of privacy.[112] At the same time, Mosley unsuccessfully tried to obtain a judgment from the European Court of Human Rights holding that member states should legislate under Article 8 of the European Convention of Human Rights to prevent newspapers from publishing stories regarding individuals' private lives without first warning the concerned party.[113]

25 However, the Internet is more difficult to control than traditional newspapers. Mosley's images went viral and people linked to them endlessly in cyberspace. Since then, Mosley has started a personal battle with the Internet, specifically with search engines. Mosley sued Google in several European countries, demanding that the company filter out of search results any online photos of his sexual escapade, alleging that the online publication of these images infringes Mosley's right to privacy. The Tribunal de Grande Instance in Paris recently granted Mosley's petition and ordered Google to remove from its image search, results over a period of five years that display any of the nine images Mosley identified.[114] The order required Google to implement a filter that should automatically

102 See eg *Internetversteigerung* I (n 101) § 1-5.

103 ibid.

104 ibid § 46.

105 See German Civil Code § 1004.

106 *Internetversteigerung* III (n 101).

107 ibid.

108 See (a.k.a. *Kinderhochstühle im Internet*) I ZR 139/08 (BGH, 22 July 2010) (Germany).

109 ibid.

110 ibid.

111 See, for factual background, Giancarlo Frosio, 'French Court Forces Google to Proactively Block Photographs of Sexual Escapade from Image Search' (*CIS Blog*, 21 November 2013) <https://cyberlaw.stanford.edu/blog/2013/11/french-court-forces-google-proactively-block-photographs-sexual-escapade-image-search>.

112 See *Max Mosley v. News Group Newspaper Ltd* [2008] EWHC 1777 (QB) (United Kingdom).

113 See *Mosley v. The United Kingdom* [2011] ECHR 774 (United Kingdom).

114 See *Google v. Mosley* (TGI Paris, 6 November 2013) (France).

detect pages containing the infringing photos and proactively block new versions of posted images from search results continuously.[115] As per the cost of filtering, the court noted that blocking the search results may be simple and inexpensive, and present technology, such as PhotoDNA, makes it possible to filter not only exact copies of identified images but also modified copies.[116]

26 Mosley brought a similar claim against Google in the United Kingdom under Art. 10 of the Data Protection Act 1998—the right to prevent processing likely to cause damage or distress—to oblige the search engine to disable access to pictures infringing on his privacy.[117] Google sought to strike out the claim, on the basis that the order applied for would be incompatible with Articles 13 and 15 of the eCommerce Directive.[118] However, the Court noted, first, that either with regard to the processing of personal data, the protection of individuals is governed solely by the data protection legislation[119] or, at least the two Directives must be read in harmony, giving both, if possible, full effect.[120] Whichever way, the "person whose sensitive personal data has been wrongly processed by an internet service provider [has a legal remedy to] ask the court to order it to take steps to cease to process that data."[121] The court, after noting that "is common ground that existing technology permits Google, without disproportionate effort or expense, to block access to individual images," allowed the claim to go to trial because "evidence may well satisfy a trial judge that [blocking] can be done without impermissible monitoring."[122]

27 In Germany, The District Court of Hamburg followed in the footsteps of the French and UK decisions.[123] Google was found liable as an "interferer" (*Störer)* "because it has not taken the possible and reasonable steps in accordance with the indications of the plaintiff to prevent further breaches of rights [...] and contributes willingly and causally to the violation of the protected rights."[124] According to the Court, notice-and-take-down is "insufficient for the present serious infringement."[125] Apparently, the Court deploys again the "untamable monster" argument as "[g]iven the gravity of the infringement and his efforts so far, [Mosley] is not required to take action against all the major media companies—possibly in the world—distributing these images on their own sites."[126] The Court goes on by saying that the notice of each individual infringement is only an inadequate tool "because the duty to monitor and control would provisionally remain with the plaintiff."[127] Apparently, the Court seems to forget that this is actually the goal that the eCommerce negligence-based liability arrangement would like to achieve. On Google's technical capacity to monitor, the Court believed that if software programmes like PhotoDNA, iWatch and Content-ID and image recognition software that works with so-called robust hash values, are not able to meet the requests of the plaintiff, Google should take measures to be able to prevent future harm occurring to Mosley by developing appropriate software or updating existing software that would "delete and detect or block the infringing content."[128]

IV. Defamation and Hate Speech: Delfi and its Progeny

28 In multiple decisions, the European Court of Human Rights (ECHR) had to consider whether an Internet news portal should be liable for user-generated comments and obliged to monitor and filter proactively its networks to avoid liability. In a landmark case, the Grand Chamber of ECHR confirmed the judgment previously delivered by the Fifth Section and held that finding Delfi—one of the largest news portals on the Internet in Estonia—liable for anonymous comments posted by third parties had not been in breach of its freedom to impart information.[129] In particular:

> *the case concerned the duties and responsibilities of Internet news portals which provided on a commercial basis a platform for user-generated comments on previously published content and some users – whether identified or anonymous – engaged in clearly unlawful hate speech which infringed*

115 ibid.

116 ibid.

117 See Mosley v Google [2015] EWHC 59 (QB) (United Kingdom).

118 ibid § 27-37.

119 See eCommerce Directive (n 1) Recital 14.

120 See Mosley (n 117) § 45.

121 ibid § 46.

122 ibid § 54.

123 See *Max Mosley v Google Inc.* 324 O 264/11 (Hamburg District Court, 24 January 2014) (Germany). See also Dominic Crossley, 'Hamburg District Court: Max Mosley v Google Inc, Google go down (again, this time) in Hamburg' (*Inforrm's Blog*, 5 May 2014) <https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google-inc-google-go-down-again-this-time-in-hamburg-dominic-crossley>.

124 *Mosley* (n 123) § 176 and 179.

125 ibid § 189.

126 ibid § 190.

127 ibid § 189.

128 ibid § 190 and 195.

129 See *Delfi AS* (n 13). See also eg Lisl Brunner, 'The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia' (2016) 16(1) Human Rights L Rev 163, 163-174.

the personality rights of others.[130]

29 Delfi published an article that mentioned in its title that SLK, a company providing public ferry transportation between the mainland and some islands, "Destroyed Planned Ice Roads," which are public roads over the frozen sea.[131] Although the article was not itself defamatory, it attracted 185 comments including personal threats and offensive language directed against a member of the advisory board of SLK.[132] The target SLK board member was Jewish and several comments had a marked, and in some instances especially ignominious, anti-Semitic flare.[133] Delfi had in place a notice-and-take-down policy.[134] Upon SLK's request for removal of the comments, Delfi promptly removed the comments under its notice-and-take-down obligations.[135] However, Delfi refused SLK's additional claim for non-pecuniary damages.[136]

30 After a long-lasting legal battle in Estonian courts, the Estonian Supreme Court upheld previous judgments and reiterated that Delfi is a provider of content services,[137] rather than an information service provider, falling under the e-Commerce Directive. Delfi finally sought redress from the ECHR. The ECHR was asked to strike a balance between freedom of expression under Article 10 of the Convention and the preservation of personality rights of third persons under Article 8 of the same Convention.[138] The ECHR tackled this conundrum by delineating a narrowly construed scenario in which liability supposedly does not interfere with freedom of expression.[139] In a situation of higher-than-average risk of defamation or hate speech,[140] if comments from non-registered users are allowed,[141] a professionally managed and commercially based Internet news portal should exercise the full extent of control at its disposal—and must go beyond automatic keyword-based filtering or ex-post notice-and-take-down procedures—to avoid liability.[142] In later cases, the European Court of Human Rights has revisited—or best clarified—the issue of liability for Internet intermediaries. In *MTE*, the ECHR concluded that "the notice-and-take-down system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved."[143] Therefore, if the specifics of *Delfi* do not apply and the comments to be removed are "offensive and vulgar" rather than hate speech,[144] the Court saw "no reason to hold that [the notice-and-take-down] system could not have provided a viable avenue to protect the commercial reputation of the plaintiff."[145] In this case, MTE—the Hungarian association of Internet service providers—posted an article highlighting unethical business practices by a real estate company, which prompted negative comments.[146] In Pihl v. Sweden, the ECHR confirmed the previous reasoning—and that size matters—by rejecting the claims of an applicant who had been the subject of a defamatory online comment published on a blog. The Court reasoned that no proactive monitoring *à la* Delfi was to be imposed against the defendant because although the comment had been offensive, it had not amounted to hate speech or an incitement to violence; it had been posted on a small blog run by a non-profit association; it had been taken down the day after the applicant had made a complaint; and it had only been on the blog for around nine days."

31 Still, proactive and automated monitoring and filtering—although narrowly applied—gets singled out by the ECHR as a privileged tool to tame the "untamable monster" or the "internet threat," as mentioned previously.[147] Anonymity becomes a possible representation of the "untamable monster" to be slayed, rather than a feature of online freedom of expression to be nourished.[148] Interestingly,

130 See ECHR, Press Release ECHR 205 (2015) (16 June 2015) <http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-5110487-6300958&filename=003-5110487-6300958.pdf>.

131 See *Delfi AS* (n 13) § 16.

132 ibid § 16-17.

133 ibid § 18.

134 ibid § 13-14.

135 ibid § 19.

136 ibid § 20.

137 See Delfi N 3-2-1-43-09 (*Riigikohus* [Supreme Court], 10 June 2009) (Estonia) <http://cyberlaw.stanford.edu/page/wilmap-estonia>.

138 ibid § 59.

139 See, for my detailed comments of each relevant principle stated in the decision, Giancarlo Frosio, 'The European Court Of Human Rights Holds Delfi.ee Liable For Anonymous Defamation' (*CIS Blog*, 25 October 2013) <https://cyberlaw.stanford.edu/blog/2013/10/european-court-human-rights-holds-delfiee-liable-anonymous-defamation>.

140 See *Delfi AS* (n 13) § 144-146. A strikingly similar standard was also adopted by an older decision of the Japanese Supreme Court. See Animal Hospital Case (Supreme Court, 7 October 2005) (Japan) <https://cyberlaw.stanford.edu/page/wilmap-japan> (finding Channel 2, a Japanese bulletin board, liable on the rationale that—given the large amount of defamatory and "unreliable" content in threads found on its site—it was not necessary for Channel 2 to know that each thread was defamatory, but it was sufficient that Channel 2 had the knowledge that there was a risk that such transmissions/posts could be defamatory).

141 See *Delfi AS* (n 13) § 147-151.

142 ibid § 152-159.

143 See *Magyar Tartalomszolgáltatók Egyesülete and Index.Hu v Hungary* N 22947/13 (ECHR, 2 May 2016) § 91.

144 ibid § 64.

145 ibid § 91.

146 ibid § 11.

147 See Delfi AS (n 13) § 110; infra Untameable Monsters, Internet Threats and Value Gaps.

148 See Nicolo Zingales, 'Virtues and Perils of Anonymity:

the Court seems to set a threshold for proactive monitoring based on popularity as in the *Baidu* case. Delfi—the Court noted in imposing its "higher-than-average risk" standard—could have realized that the article might have caused negative reactions because readers and commenters had a great deal of interest in the matter, as shown by the above average number of comments posted on the article.[149] In the process, over-enforcement—caused by automated filtering—challenges freedom of expression.[150] Again, the role of intermediaries is blurred with that of entities obligated to police the net for infringing activities. But is it their role?

E. Legislation

32 Legislatively mandated proactive monitoring obligations to curb online copyright infringement might soon follow in the footsteps of voluntary measures already adopted by major platforms and case law. For reasons of space, this article touches only briefly on these proposals, which nonetheless must be mentioned for sake of structural completeness. A detailed review of these proposals, however, is included in other writings of this author cited below.

33 Proactive monitoring—and filtering—sits on top of the rightsholders' wish list both in the United States and Europe.[151] In particular, a recent proposal included in the *Copyright in the Digital Single Market Draft Directive* would impose on intermediaries the implementation of effective content recognition technologies to prevent the availability of infringing content.[152] The Commission's copyright proposal would require platforms that provide access to "large amounts" of user-generated content to incorporate an automated filtering system. The proposal specifically refers to technologies such as YouTube's Content ID or other automatic infringement assessment systems.[153] Apparently, the proposal would force hosting providers to develop and deploy filtering systems, therefore *de facto* monitoring their networks.[154]

34 Proactive monitoring and filtering obligations would also find their way in European policy through an update of the audio-visual media legislation. As part of its legislative intervention package, the Commission will tackle the proliferation on online video sharing platforms of content that is harmful to minors and of hate speech with its proposal for an updated Audio-visual Media Services Directive.[155] Video hosts can be regulated like broadcasters if they step outside of their passive hosting role by organizing hosted content. The AVMS draft directive lists new obligations to remove and possibly monitor for hate speech. This specific-sector regulation would ask platforms to put in place measures to protect minors from harmful content and to protect everyone from incitement to hatred.[156] Apparently, the AVMS revision might erode the eCommerce directive's no monitoring obligations for video platforms by asking Member States to "ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to violence or hatred'.[157]

35 It is worth noting, however, that a heated debate is occurring in the European Parliament regarding the implementation of the Commission's proposals. Finally, the reform as approved by the Parliament might differ consistently from the proposals.[158]

Should Intermediaries Bear the Burden?' (2014) 5(3) JIPITEC 155, 155-171.

149 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and Tsotsoria § I.2.

150 See Martin Husovec, 'ECHR Rules on Liability of ISPs as a Restriction of Freedom of Speech' (2014) 9(2) JIPLP 108.

151 See Joint Supplemental Comments of American Federation of Musicians et al to U.S. Copyright Office, In the Matter of Section 512 Study: Notice and Request for Public Comment, Docket No 2015-7 (28 February 2017) (the Recording Industry Association of America and 14 other groups calling for stronger regulations that would require internet service providers to block pirated content).

152 See Commission, 'Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market' COM(2016) 593 final (14 September 2016) art 13.

153 ibid.

154 I remand for a detailed analysis of this proposal to two recent works of mine. See Frosio (n 7) <https://goo.gl/HNkHZV>; Frosio (2017a) (n 8).

155 See Commission, Proposal for a Council Directive amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final.

156 ibid art 6 and 28.

157 See Proposal for a Directive of the European Parliament and the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final (25 May 2016) art 6.

158 So far, the Committee on the Internal Market and Consumer Protection (IMCO) approved an opinion on the proposed reform. See Committee on the Internal Market and Consumer Protection (IMCO), Opinion for the Committee on Legal Affairs on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 16 June 2017, PE 599.682v02-00, IMCO_AD(2017)599682. Also, the Culture and Education Committee (CULT) has a draft opinion in place to be voted on. See Culture and Education Committee (CULT), Draft opinion on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 6 February 2017, PE 595.591v01-00, CULT_PA(2017)595591. Finally, the Committee on Legal Affairs (JURI) also released

F. Fundamental Rights Implications

36 As stated by multiple authorities,[159] general filtering and monitoring obligations would be inconsistent with the Charter of Fundamental Rights of the European Union.[160] As an overall point, in *Google v. Vuitton*, the Advocate General of the CJEU pointed at the fact that general rules of civil liability (based on negligence)—rather than strict liability IP law rules—suit best the governance of the activities of Internet intermediaries:

> *[l]iability rules are more appropriate, [. . .] Instead of being able to prevent, through trade mark protection, any possible use – including, as has been observed, many lawful and even desirable uses – trade mark proprietors would have to point to specific instances giving rise to Google's liability in the context of illegal damage to their trademarks.*[161]

37 According to this argument, a negligence-based system would serve users fundamental rights. As Van Eecke mentioned, "the notice-and-take-down procedure is one of the essential mechanisms through which the eCommerce Directive achieves a balance between the interests of rightholders, online intermediaries and users."[162] Although imperfect as it is, a notice-and-take-down mechanism embeds a fundamental safeguard for freedom of information as long as it forces intermediaries to actually consider the infringing nature of the materials before coming to a final decision whether to take them down. Replacing knowledge or notice-and-take-down with filtering and monitoring obligations would by default bring about chilling effects.

38 In *Netlog* and *Scarlet Extended*, the CJEU explained that filtering measures and monitoring obligations would fail to strike a 'fair balance' between copyright and other fundamental rights.[163] In particular, they would undermine users' freedom of expression.[164] Users' freedom to receive and impart information would be struck by the proposal. Automatic infringement assessment systems might undermine the enjoyment of users' exceptions and limitations.[165] DRM effects on exceptions and limitations have been highlighted by copious literature.[166] Similar conclusions apply to this scenario. Automated systems cannot replace human judgment that should flag a certain use as fair—or falling within the scope of an exception or limitation. Also, complexities regarding the public domain status of certain works might escape the discerning capacity of content recognition technologies. At the present level of technological sophistication, false positives might cause relevant chilling effects and negatively impact users' fundamental right to freedom of expression. In the own words of the European Court of Justice, these measures:

> *could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends*

a draft opinion and will vote on its amendments later this year. See Committee on Legal Affairs (JURI), Draft opinion on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market, 10 March 2017, PE 601.094v01-00, JURI_PR(2017)601094.

159 See C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85. See also Christina Angelopoulos, 'On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market' (2017) 38-40 <https://juliareda.eu/wp-content/uploads/2017/03/angelopoulos_platforms_copyright_study.pdf>; Christina Angelopoulos, 'Sketching the Outline of a Ghost: the Fair Balance between Copyright and Fundamental Rights in Intermediary Third Party Liability' (2015) 17 Emerald Insight 72 (noting that fair balance is the appropriate conflict resolution mechanism in case of fundamental rights clashes and balancing excludes the imposition of filtering obligations on intermediaries for the purpose of copyright enforcement, but allows blocking); Stefan Kulk and Frederik J. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 EIPR 791, 791-794; Darren Meale, '(Case Comment) SABAM v Scarlet: Of Course Blanket Filtering of the Internet is Unlawful, But This Isn't the End of the Story' (2012) 37 Europ Intell Prop Rev 429, 432; Evangelia Psychogiopoulou, '(Case Comment) Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers After Scarlet' (2012) 38 EIPR 552, 555.

160 See Charter of Fundamental Rights of the European Union, C326/391 (26 October 2012) [hereinafter EU Charter].

161 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 and Others, C-238/08, joined cases, § 123 (CJEU, 23 March 2010) (Advocate General Opinion).

162 Van Eecke (n 52) 1479-1480.

163 See Netlog (n 5) § 55.

164 See Charter of Fundamental Rights of the European Union, C326/391 (26 October 2012) art 8 and 11.

165 See Leron Solomon, 'Fair Users or Content Abusers? The Automatic Flagging of Non-Infringing Videos by Content ID on Youtube' (2015) 44 Hofstra L Rev 237; Corinne Hui Yun Tan, 'Lawrence Lessig v Liberation Music Pty Ltd - YouTube's Hand (or Bots) in the Over-zealous Enforcement of Copyright' 36(6) (2014) EIPR 347, 347-351; Justyna Zygmunt, To Teach a Machine a Sense of art – Problems with Automated Methods of Fighting Copyright Infringements on the Example of YouTube Content ID, Machine Ethics and Machine Law E-Proceedings, Jagiellonin University, Cracow, Poland, November 18-19, 2016, pp. 55-56; Zoe Carpou, 'Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users' (2016) 39 Colum J L & Arts 551, 564-582.

166 See Giancarlo F. Frosio, *COMMUNIA Final Report on the Digital Public Domain* (report prepared for the European Commission on behalf of the COMMUNIA Network and the NEXA Center) (2011), 99-103, 135-141 <http://www.communia-project.eu/final-report> (discussing most of the relevant literature and major threats that technological protection measures pose for fair dealings, privileged and fair uses).

on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned.[167]

39 Similar points have been highlighted by miscellaneous scholarship. Enforcing online behaviour through automated or algorithmic filtering and fair use does end up inherently in a poor trade-off for fundamental and users' rights. Julie Cohen and Dan Burk argued that fair use cannot be programmed into an algorithm, so that institutional infrastructures will always be required instead.[168] Although changes in technology move fast and unpredictably, since fair use is at heart an equitable doctrine, the assumption that, judgment is not programmable might still remain valid for some time. Indeed, the capacity of neural networks to develop more accurate models of many phenomena—maybe even some or most fair uses—might change these assumptions in the future. In general, it was noted that "the design of copyright enforcement robots encodes a series of policy choices made by platforms and rightsholders and, as a result, subjects online speech and cultural participation to a new layer of private ordering and private control."[169] According to Matthew Sag, automatic copyright filtering systems—upon which private agreements between rightholders and online platforms are predicated—"not only return platforms to their gatekeeping role, but encode that role in algorithms and software."[170] In turn, automatic filtering supersedes the safe harbour system and fair use only nominally applies online.[171] In practice, private agreements and automatic filtering determine online behaviour far more "than whether that conduct is, or is not, substantively in compliance with copyright law."[172]

40 Residual critiques point at the negative externalities on innovation that this new regime would have. The ECJ emphasized the economic impact on ISPs regarding filtering and monitoring obligations. The ECJ assumed that monitoring all the electronic communications made through the network, without any limitation in time, directed to all future infringements of existing and yet to create works "would result in a serious infringement of the freedom of the hosting service provider to conduct its business."[173] Hosting providers' freedom of business would be disproportionally affected since an obligation to adopt filtering technologies would require the ISP to install a complicated, costly and permanent system at its own expense.[174] In addition, according to the ECJ, this obligation would be contrary to Article 3 of the Enforcement Directive, providing that "procedures and remedies necessary to ensure the enforcement of the intellectual property rights [. . .] shall not be unnecessarily complicated or costly [and] shall be applied in such a manner as to avoid the creation of barriers to legitimate trade."[175] UPC Telekabel also raised the issue—but less clearly—of cost of enforcement in the context of access providers. It noted that imposing costs on the access provider would limit their freedom to conduct a business, in particular by requiring to "take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions,"[176] even though he is not the perpetrator of the infringement which has led to the adoption of that injunction.[177] Finally, however, UPC Telekabel came down with a mixed response by suggesting that access providers "can choose to put in place measures which are best adapted to the resources and abilities available,"[178] although they should "not be required to make unbearable sacrifices."[179] Notably, the Paris Court of Appeal in *Allostreaming*—which was mentioned earlier—disregarded these arguments, while imposing costs of blocking and delisting on online intermediaries alone. Similarly, *Dafra* and *Mosley* denied Google "technical impossibility" defense and claims against proactive monitoring based on cost efficiency arguments.

41 Finally, apparently, the unqualified deployment of filtering and monitoring obligations will impinge also on the service user's right to protection of personal data. In the SABAM cases, the ECJ has authoritatively already outlined the inappropriateness of these measures against fundamental rights also in this scenario. As the ECJ concluded:

requiring installation of the contested filtering system would involve the identification, systematic analysis and processing

167 Netlog (n 5) § 50.

168 See Dan Burk and Julie Cohen, 'Fair Use Infrastructure for Copyright Management Systems' (2000) Georgetown Public Law Research Paper 239731/2000 <https://ssrn.com/abstract=239731>.

169 See Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 Notre Dame L Rev, at 1.

170 ibid 1.

171 ibid.

172 ibid.

173 Netlog (n 5) § 46.

174 ibid.

175 See Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, 2004 O.J. (L 195) 16 (Corrigendum) Art. 3.

176 C-314/12 *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH et al* (2014) ECLI:EU:C:2014:192 § 50.

177 ibid § 53.

178 ibid § 52.

179 ibid § 53.

> *of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified.*[180]

42 Supposedly, secrecy of communication or the right to respect for private life[181] could be also impinged upon by filtering technologies, according to the European Court of Human Rights, which tends to be critical of systems to intercept communications, especially when they monitor content of communications.[182]

G. Conclusions

43 This paper has been investigating the death of "no monitoring obligations," a well-marked trend in intermediary liability policy. In search of the culprit, this investigation has taken us all over the world to courts engaged in landmark fights with "untamable monsters." This paper explored upcoming law reform, which seeks to dismantle a twenty year old negligence-based intermediary liability system to protect the "value gap." Evidence-based analysis has also led to private ordering enforcing proactive monitoring and filtering. The death of no monitoring obligation—or at least the great danger that it's facing—finds explanation in all these factors' synergic actions.

44 Proactive monitoring obligations and filtering challenge the "fair balance" between fundamental rights in intermediary liability; either horizontal or vertical,[183] there are plenty of options to be pursued. Still, turning to proactive and automated filtering—and rejecting knowledge-and-take-down—seems hardly capable of achieving the desired "fair balance." Current Internet policy—especially in Europe—is silently drifting away from a fundamental safeguard for users' fundamental rights online, which has been guarding against any "invisible handshake" between rightholders, online intermediaries, and governments. The *Delfi* dissenting opinion reminds us that "in putting pressure and imposing liability on those who control the technological infrastructure (ISPs, etc.), [governments] create an environment in which collateral or private-party censorship is the inevitable result."[184] Professor Jack Balkin labels this process moving towards intermediaries' private ordering as "collateral censorship," which "occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech."[185] This liability, in turn, gives A "strong incentives to over-censor."[186] Historically, imposing liability on intermediaries served the censorship machine of the established power. Printing privileges—born as an innovation policy and a trade regulation—grew into a censorial tool. In this sense, online intermediary liability regulation might be following a similar path. Of course, the reason to impose liability would be always compelling enough. Today, it's the "untamable monster" of networked digital distribution and the "value gap." Yesterday, the English *Stationers' Charter* ordered that no one could exercise the art of printing but the ninety-seven "beloved and faithful" Stationers because the King and Queen manifestly perceived that:

> *certain seditious and heretical books rhymes and treaties are daily published and printed by divers scandalous malicious schismatical and heretical persons, not only moving our subjects and lieges to sedition and disobedience against us, our crown and dignity, but also to renew and move very great and detestable heresies against the faith and sound catholic doctrine of Holy Mother Church.*[187]

45 The death of "no-monitoring obligations" fits within a broader move towards enlisting online intermediaries as the Internet police. This is also achieved through the promotion of private ordering and voluntary enforcement schemes, which is a strategy prominently endorsed as part of the EU Digital Single Market Strategy. As I argue elsewhere, the intermediary liability discourse is shifting towards an intermediary responsibility discourse.[188] This process might be pushing an amorphous notion of responsibility that incentivizes intermediaries' self-intervention. Finally, intermediary responsibility does morph into algorithmic responsibility. The emergence of proactive monitoring obligations—and the automated or algorithmic enforcement they bring about—would be a conspicuous move in that direction. Looking for the answer to the machine in the machine might help taming the "monster" that Justice Salomão evoked, but at what price? Due process and fundamental guarantees

180 Netlog (n 5) § § 49.

181 See Charter (n 164) Art. 7.

182 See Kulk and Frederik J. Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 34 EIPR 791, 793-794.

183 Christina Angelopoulos and Stijn Smet, 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability' (2016) (8(2) Journal of Media Law 266, 266 (arguing that "automatic takedown and notice-and-stay-down are applicable exclusively to child pornography.").

184 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and TsoTsoria, § I.2.

185 Jack M. Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296, 2309.

186 See Delfi AS (n 13) Joint Dissenting Opinion of Judges Sajò and Tsotsoria § I.2.

187 *See* Stationers' Charter (1557) *in* I *A Transcript of the Registers of the Company of Stationers of London 1557-1640* (E. Arber, 1875-94) xxviii, xxx-xxxi.

188 See Frosio (n 8).

get mauled by algorithmic enforcement, trampling over fair uses, the public domain, right of critique, and silencing speech according to the mainstream ethical discourse. The upcoming reform—and the broader move that it portends—might finally slay "no monitoring obligations" and fundamental rights, rather than the untameable monster. Ultimately, the current and proposed enforcement strategies are assuming to slay the untameable monster with potions and enchantments, rather than empirical evidence.