A Storm in ISP Safe Harbor Provisions: The Shift From Requiring Passive-Reactive to Active-Preventative Behavior and Back

VOJTECH MLYNAR*

INTRODUCTION

There has been a storm in the safe harbor for Internet Service Providers (ISPs). Since the formation of the Internet, ISPs have been under pressure to assume more liability for information they transmit or store. For example, interested parties, trying to put ISPs in the same position as offline content publishers, pushed for a strong liability regime for online defamatory content and copyright infringement.[1] However, subjecting ISPs to this sort of liability regime arguably stifles the rapidly growing online environment.[2] Thus, policy makers in the United States and the European Union (EU) adopted safe harbors for ISPs in certain contexts.[3] As long as an ISP did not exercise editorial control over the content posted by a third-party user it remained immune from liability.[4]

From then on, global developments regarding ISP liability have been very different. Courts in the United States generally offer consistent interpretations of the safe harbor rules. The United States Court of Appeals for the Second Circuit recently confirmed the strong protection given to ISPs in *Viacom Int'l, Inc. v. YouTube*[5]—a well known case alleging "massive" and "brazen" copyright infringement by a video-sharing website.[6] However, European courts cannot consistently agree on the

---

*Mgr. Vojtech Mlynar, graduate of Charles University School of Law (Czech Republic), 2014. He was an international exchange student at the University of San Francisco School of Law during the spring of 2014.

1. *See infra* Part II.A.

2. 47 U.S.C. § 230(b) (2012). *See also* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) ("It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.").

3. *See* 47 U.S.C. § 230(c)(2)(A) (2012) ("No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."); Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); Council Directive 2000/31, 2000 O.J. (L 178) [hereinafter Directive 2000/31].

4. *See* Cubby v. CompuServe, Inc., 776 F. Supp. 135, 142–43 (S.D.N.Y. 1991) (finding CompuServe not vicariously liable, in part because it maintained no editorial control over the content of publication).

5. 676 F.3d 19 (2d Cir. 2012).

6. *Id.*

interpretation of ISP safe harbor provisions in the EU. This Article describes developments pertaining to ISP liability in the EU shaped by the decisions of European courts, and the global consequences of such decisions.

During the early 2000s, copyright owners applied pressure on ISPs by testing the scope and limits of the safe harbor provisions. They attempted to force ISPs to take a more active approach to copyright policing in the online environment and to actively prevent copyright violations (the "active-preventive" approach), rather than act as passive and neutral third parties that only react to copyright violations upon notification (the "passive-reactive" approach).[7] Initially, copyright owners appeared to be winning the battle in the EU due to the European courts' imposition of stricter liability standards and new monitoring duties.[8] In some EU member states, the national courts required ISPs to play an active-preventive role in copyright policing, pushing online intermediaries into the role of a *de facto* publisher, and held them liable for content posted online by their users.[9] Recently, however, higher judicial authorities in the EU pushed back, and reinstated effective safe harbors for ISPs.[10]

Today, new pressures are building up. Instead of concentrating on the ISPs' editorial control over content, the focus is now on the Internet's infrastructure. The Internet consists of an endless number of interconnected networks,[11] and its boundlessness poses numerous legal challenges. For example, policing copyright infringement on a per-website basis usually does not stop copyright infringement since the culprit can simply change its network location and continue infringing. Alternatively, it may be more effective to cut access to parts of the Internet where copyright violations frequently occur. Blocking access to parts of the Internet seems easier to enforce because courts and enforcement agencies have the authority to effectively control local entities that provide Internet access because businesses are established and exist according to national laws, thus are easily identifiable and liable to persecution. Copyright owners recently asked European courts to issue website-blocking injunctions, and the decision by the EU's highest court confirmed the validity of these requests[12]—once again questioning ISP protection under the EU safe harbor.

This Article discusses the history and recent developments pertaining to ISP liability for copyright infringement in the EU. Part I explains the role of an ISP and outlines the legal framework in the EU that provides safe

---

7. *See infra* Parts I, II.

8. *See infra* Part II.A.

9. Lafesse v. MySpace, Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, June 22, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1965. *See infra* Part II.A.

10. *See infra* Part II.B.

11. *Internet*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet (last modified Dec. 8, 2014).

12. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-0000 ¶ 32 (Mar. 27, 2014).

harbor provisions for ISP liability. Part II describes the judicial decisions by EU member states that eroded the safe harbor rules, and explains how the EU Court of Justice subsequently overturned these decisions.[13] Part II examines the latest judgments issued by the Court of Justice concerning the new rules (or lack thereof) for website-blocking injunctions. Part III provides examples of voluntary collaboration between ISPs and content owners, which may be the best method to effectively combat online piracy and be beneficial to all parties. Finally, Part IV explores the potential consequences of the new developments for the online environment—focusing on users' privacy. This Article concludes that although copyright enforcement on the Internet is a legitimate and important goal, such enforcement and prevention may impact other realms of the online environment, and impede the democratic and open nature of the Internet—something that is too often overlooked in the online-piracy debate.

I. ISP'S ROLE IN THE INTERNET

ISPs are the basic players of the Internet. These companies provide access to the Internet and other related services.[14] The Internet would not work without ISPs because there would be no search engines, no places to store website data, no easy way to transmit information over networks, and virtually no available means for individual users to connect to the Internet. Without ISPs, the Internet would resemble its early days when it functioned as a mere communication and research network directly connecting a small number of computers, and was limited to users with sufficient technological skill.

A. ISP PRIMER

To simplify and distinguish between the two main roles ISPs play in the Internet's environment, this Articles divides them into two categories: access and content. Access ISPs provide basic infrastructure for the Internet.[15] Their main job is to provide access to communications networks and facilitate transmission of information between various points within these networks.[16] Content ISPs are best described as online content

13. The Court of Justice of the European Union is the highest judicial institution of the European Union in matters of EU law. The court consists of twenty-eight judges (one judge from each member state), and nine Advocates General who present detailed opinions on the cases brought before the court. The Court of Justice adjudicates, among other things, on references for preliminary rulings—questions referred to the Court of Justice by courts from the EU member states regarding interpretation of EU law. This procedure aims to provide uniform interpretation of EU law throughout all member states.

14. *ISP*, DICTIONARY.COM, http://dictionary.reference.com/browse/isp (last visited Oct. 6, 2014).

15. *Internet Service Provider*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_service_provider#Access_providers (last modified Dec. 4, 2014) (describing Access Providers as a subcategory of ISPs).

16. Access ISPs can be further divided into tier-groups, based on the potential reach of their networks and the amount of traffic they handle. Tier 1 consists of large "backbone" network operators, and Tiers 2–3 are local distributors or "interconnectors." Large telecommunication companies often act as both Tier 1 and Tier 2 access ISPs (e.g., AT&T, Sprint, Deutsche Telekom, or Telefónica).

providers. Content ISPs offer a diverse range of Internet services, but their primary function is to store online data.[17] Content ISPs provide space on hard drives permanently connected to the Internet. Users can input a URL to connect to a drive and access the stored data. Data is presented in various forms to the end-user, e.g., email accounts, traditional websites, photo or video sharing services, social media, cloud computing applications, or file-sharing servers.

Access and content ISPs create the Internet's infrastructure and its substance. One cannot exist without the other.[18] Due to their indispensable role, policy makers recognize the need to protect ISPs. The following section outlines the main legislation protecting ISPs in the EU.

B. THE EU LEGAL PROTECTION FRAMEWORK

To protect online intermediaries and secure the Internet's growth, the EU adopted legislation concerning ISP liability at the turn of the new millennium. Section 4 of the European Council Directive 2000/31 (the "eCommerce Directive")[19] introduced safe harbor provisions to protect online intermediaries from traditional liability for information passing through and residing on their networks. Prior to the eCommerce Directive, the U.S. Congress adopted a similar statute—the Digital Millennium Copyright Act (DMCA).[20] These two pieces of legislation effectively grant global immunity from copyright infringement for ISPs,[21] so long as they remain passive and neutral as to the content they host.

The eCommerce Directive prohibits imposing general content monitoring obligations on ISPs.[22] It does not require ISPs to actively manage passing traffic or police content residing on their networks.[23] Instead, the statutory framework is based on a passive-reactive approach. An ISP is only obligated to intervene when it gains actual knowledge about an infringing activity, which typically occurs when a copyright owner notifies the ISP of the violation.[24] Otherwise, an ISP remains neutral and

---

Interestingly, while in the 'off-line' utilities sector governments often require backbone infrastructure operators (Tier-1) to act as separate entities in order to ensure fair competition and non-discriminatory access to main networks, no such regulation exists for the online environment. *See, e.g.*, Council Directive 2009/73, art. 9, 2009 O.J. (L 211) (describing common rules for the internal market in natural gas).

17. Storing online data is also referred to as "hosting."

18. Roles of access and content ISPs may overlap and one entity may provide both services, e.g., Comcast's (access ISP) Xfinity service offering online video-on-demand streaming, or Google's (content ISP) Fiber service offering ultra fast Internet connection to individual households in selected cities.

19. Directive 2000/31, *supra* note 3, § 4 (describing the liability of intermediary service providers).

20. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

21. *See, e.g.*, Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries*, 49 JURIMETRICS J. 375 (2009).

22. Directive 2000/31, *supra* note 3, at art. 15.

23. *Id.*

24. *Id.*

passive.[25]

Both the eCommerce Directive and the DMCA divide ISP activity into three types of conduct: (i) mere conduit,[26] (ii) caching,[27] and (iii) hosting.[28] These activities are related to each other and an intermediary can engage in all of these activities at the same time.

1. Mere Conduit

The first type of conduct deals with situations where ISPs act as mere conduits, or carriers of transitory digital network communications. ISPs that act as mere conduits are not subject to liability for infringement of copyright when a third party uses its network to transmit copyrighted materials.[29] In order to qualify as a mere conduit, an ISP must satisfy the following: (1) the transmission of the copyrighted material has to be initiated and the recipient designated by a person other than an ISP; (2) the ISP cannot select or modify the information contained in the transmission; (3) the transmission must be handled by automated processes; and (4) the intermediate copies of the copyrighted material are not accessible by the general public and copies may not be maintained on the ISP's system or network for longer than reasonably necessary to facilitate the transmission.[30]

ISPs acting as mere conduits are protected from liability potentially arising from transmitted content, provided that they are only passively involved in the transmission. Most access ISPs act as mere conduits, because their main function is to transport data from one point on the network to another. Any interference with transmitted information, such as monitoring content, selecting recipients, or initiating the transmission, may result in a loss of safe harbor protection.

2. Caching

Caching is defined as the automatic, intermediate, and temporary storage of data on an ISP's server, performed for the sole purpose of effective transmission of information from one point on the network to another.[31] While transmitting information from point "A" to point "B," it may be necessary for an ISP to create several copies along the way. Other times, an ISP may create a temporary copy to facilitate faster access to

---

25. The wording of the DMCA and eCommerce Directive does not prevent ISPs from active content monitoring. However if ISPs do monitor, they will not be shielded from liability for third-party content, because they would gain actual knowledge about illicit content through their monitoring activities. Therefore, even though the DMCA and eCommerce Directive do not prohibit voluntary content monitoring, they create a strong incentive not to engage in such activity.

26. Directive 2000/31, *supra* note 3, at art. 12. The DMCA describes this type of conduct as "Transitory Digital Network Communications." 17 U.S.C. § 512(a) (2012).

27. Directive 2000/31, *supra* note 3, at art. 13; 17 U.S.C. § 512(b) (2012).

28. Directive 2000/31, *supra* note 3, at art. 14. The DMCA describes this type of conduct as "Information Residing on Systems or Networks at Direction of Users." 17 U.S.C. § 512(c) (2012).

29. 17 U.S.C. § 512(a) (2012).

30. *Id.* § 512(a)(1)–(4).

31. Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 120 (2002).

information stored on distant servers.[32] For example, if a user located in San Francisco wants to access a website stored on servers in Prague, an ISP may cache the content of the Prague website, i.e., create a copy on its servers located in the United States. As a result, users' requests do not need to travel back and forth from San Francisco to Prague each time they want to access the Prague website. Caching grants users faster access to information and allows ISPs to significantly reduce network workload and congestion.[33]

The eCommerce Directive includes specific provisions to maintain immunity for ISPs engaging in caching. An ISP making a copy of copyrighted material for the sole purpose of making the information's onward transmission more efficient will not be held liable for infringement so long as the ISP: (1) does not modify the information; (2) complies with conditions for third-party access set up by the content owner; (3) complies with the rules regarding the updating of information in accordance with established industry practices; (4) does not interfere with data providing statistics on the use of the information; and (5) promptly removes or disables access to copyright infringing material upon obtaining actual knowledge of the fact that the information has been removed from the initial source, has been disabled, or where such removal was ordered by an administrative authority.[34]

The last condition illustrates the EU's intention for ISPs to remain passive-reactive. As long as intermediaries act passively and neutrally by automatically caching data without monitoring its content, they will not be liable for copyright-infringing material in their caches. However, if they become aware of infringing content, they are required to react and expeditiously remove the illicit content from their systems.

3. Hosting

While transitory communication and caching deal with the temporary storage of information, hosting providers store third-party content for a potentially indefinite period of time. The liability-exemption framework again requires ISPs to maintain a passive-reactive approach to content. To be exempt from liability, an ISP that hosts data at the request of a third-party user: (1) must not have actual knowledge of illegal activity or infringing information;[35] (2) cannot receive any financial benefit directly attributed to the infringing activity;[36] and (3) must respond promptly to remove or disable access to material that is claimed to be infringing or to be the subject of infringing activity.[37] In the absence of actual knowledge,

---

32. *Id.*

33. *See, e.g.*, *Web Application/Caching*, DOCFORGE, http://docforge.com/wiki/Web_application/Caching (last visited Oct. 22, 2014) (providing a more detailed explanation of 'caching' and its benefits).

34. Directive 2000/31, *supra* note 3, at art. 13(1)(a)–(e); 17 U.S.C. § 512(b)(2)(A)–(E) (2012).

35. Directive 2000/31, *supra* note 3, at art. 14(1)(a); 17 U.S.C. § 512(c)(1)(A)(i) (2012).

36. 17 U.S.C. § 512(c)(1)(B) (2012).

37. Directive 2000/31, *supra* note 3, at arts. 14(1)(b), 31; 17 U.S.C. § 512(c)(1)(C) (2012).

the eCommerce Directive may still find an ISP liable for infringement if it is aware of facts or circumstances from which infringing activity is apparent.[38] The last requirement, also included in the DMCA and referred to as "red flag" knowledge,[39] turns on whether an ISP was subjectively aware of facts that would have made the infringement "'objectively' obvious to a reasonable person."[40]

Contrary to mere conduit and caching, hosting ISP liability protection does not require intermediaries to remain fully passive. To a certain extent, ISPs offering hosting services can modify information uploaded on its servers without piercing their liability shield. Indeed, modification is often necessary to ensure proper functioning of hosting services.[41] When a hosting provider interacts with stored data in a neutral manner,[42] it can still be shielded from liability—provided its involvement does not lead to actual knowledge or awareness of infringing information.

4. Notice-and-Takedown Procedures

As previously mentioned, online intermediaries cannot be required to perform general monitoring of content residing on or passing through their systems.[43] Instead, hosting providers typically follow a notice-and-takedown procedure when dealing with infringing activities.[44] This procedure allows copyright owners to bring infringing material to an ISP's attention and requires the ISP to react expeditiously to remove or block access to infringing material.[45] While the DMCA provides detailed rules specifying the elements of these notifications,[46] the eCommerce Directive lacks such guidance and forces the individual member states to interpret the requirements. As a result, notice-and-takedown procedures are inconsistent across the EU, and sometimes even within the territories of a member state.[47] This inconsistency not only directly conflicts with goal of a

38. Directive 2000/31, *supra* note 3, at art. 14(1)(a).

39. Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233 (2008).

40. Viacom Int'l, Inc. v. YouTube, 676 F.3d 19, 31 (2d Cir. 2012); Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500, 520 (S.D.N.Y. 2013).

41. For example, among other things, a hosting provider can automatically resize images or change text formatting of a user's website. ISPs may also automatically change a website layout depending on a device used to access a website (e.g., smart-phone, tablet or computer).

42. There is no clear delineation between neutral interaction and data management that may lead to actual knowledge about data content. The extent to which an ISP may manage data hosted on its servers is subject to ongoing debate. *See* Patrick Van Eecke, *Online Service Providers and Liability: A Plea for a Balanced Approach*, 48 COMMON MKT. L. REV. 1455, 1481 (2011).

43. *See supra* Part I.B.

44. 17 U.S.C. § 512(c)(1)(C) (2012) ("[U]pon notification of claimed infringement . . . [the ISP] responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.").

45. *See id.*

46. *Id.* § 512(c)(3).

47. Notwithstanding the fact that there is no uniform notice-and-takedown procedure, EU rules and case law provide minimum requirements for ISPs. Article 5(1)(c) of the eCommerce Directive requires service providers to supply recipients of their service with contact information. According to the Court of Justice ruling, in addition to e-mail address service providers must provide "other information which allow them to be contacted rapidly and communicated with in a direct and effective manner." Case C-298/07, Bundesverband der Verbraucherzentralen und Verbraucherverbände v.

comprehensive regime stated in the eCommerce Directive,[48] but also creates significant legal uncertainty for Internet intermediaries, who wish to provide uniform services across the EU.[49]

II. SHIFT FROM REQUIRING ISPS TO BE PASSIVE-REACTIVE TO ACTIVE-PREVENTIVE AND BACK

Although the DMCA and the eCommerce Directive both feature nearly identical provisions regarding ISP liability, their scope and meaning have been interpreted differently. While the wording of both statutes requires ISPs to remain neutral, taking a passive-reactive approach to copyright infringements, the judicial interpretation of these rules produced very different outcomes among the EU member states. The following section examines important judicial decisions affecting ISPs' neutral positions, and the push toward a more active-preventive role in online copyright policing. Also, this section addresses the EU Court of Justice's response to this push, which reinstituted the passive-reactive interpretation of safe harbor provisions.

A. A PUSH TOWARDS ACTIVE-PREVENTIVE ACTION

All EU member states transposed the rules introduced in the eCommerce Directive into their national legislation.[50] While the purpose of the eCommerce Directive was to ensure uniform treatment of Internet intermediaries throughout the EU, it has failed to fulfill its intended goal, and creates significant differences between each EU member state.

1. French Courts Lead the Way—Arguably in the Wrong Direction

In *Lafesse v. MySpace*[51] the French Court of Paris held the social networking company, MySpace, liable for copyright infringement despite the fact that MySpace acted as a typical hosting service.[52] The court found that MySpace allowed its users to create personalized webpages, offered special tools for uploading content, and generated profits from

deutsche internet versicherung AG, 2008 E.C.I.R. I-07841, ¶ 4.

48. Directive 2000/31, *supra* note 3, at recital 1 ("[T]he development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples.").

49. In January, 2012 the EU Commission launched public consultation on notice-and-takedown procedures. The purpose of consultation was to gather opinions of different parties and establish best practices. Results of these conclusions have not yet been published. *See Notice-and-Action Procedures*, EUROPEAN COMM'N, http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm (last updated Mar. 10, 2014).

50. Generally, legal rules stipulated in Directives are not directly applicable. Instead, the EU member states must transpose these rules into their national legislation in standard legislative processes applicable in each country. *See* Verbiest, Spindler, Riccio & Van der Perre, *Study on liability of Internet Intermediaries*, European Commission—Markt/2006/09/E Service Contract ETD/2006/IM/E2/69 (Nov. 12, 2007).

51. Lafesse v. MySpace, Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, June 22, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1965.

52. *Id.*

advertisements placed alongside videos uploaded by users.[53] The court found that these factors were sufficient to consider MySpace a publisher,[54] and thus liable for infringing content uploaded by its users.[55] The court's decision makes it clear that it viewed MySpace as stepping outside the safe harbor provisions of Article 14 of the eCommerce Directive, and therefore not eligible for liability protection.

One month later, the same French Court of Paris decided *Nord-Ouest Production v. Dailymotion, UGC Images*.[56] The court held that Dailymotion, a video-sharing website, was not a publisher despite the similarities of its services to MySpace's including commercial advertising alongside uploaded videos.[57] Although the court considered Dailymotion to be a content ISP, the ruling was catastrophic for online intermediaries. The court ruled that Dailymotion was not protected from liability because it must have known that the illegal content was present on its website.[58] With these two rulings, the Court of Paris essentially created a duty for service providers to implement technical measures to prevent all unlawful activities on its website.[59]

2. Requiring Take-Down/Stay-Down Procedures—Going Further in the Wrong Direction

In *Zadig Productions v. Google Inc.*,[60] a French documentary producer brought suit for copyright infringement against Google Video.[61] The Court of Paris held Google liable for copyright infringement, despite the fact Google had complied with notice-and-takedown procedures.[62] The court agreed with the plaintiff's argument that once a hosting provider is notified of specific instances of infringement, it has a duty to prevent future re-postings of the same infringing content.[63] Google argued that it was exempt from liability under "Article 6-2 of the Law of 21 June 2004," because it had no knowledge of the specific subsequent infringement, and, upon receiving formal notice, it acted expeditiously to remove the illicit

---

53. *Id.*

54. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995) ("[O]ne who repeats or otherwise republishes a libel is subject to liability as if he had originally published it.").

55. Lafesse v. MySpace, Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, June 22, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1965.

56. Nord-Ouest Production v. Dailymotion, UGC Images, Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, 3e ch., 2e sec., July 13, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=1977.

57. *Id.*

58. *Id.*

59. Nicolas Jondet, *The Silver Lining in Dailymotion's Copyright Cloud*, JURISCOM.NET (Apr. 19, 2008), http://juriscom.net/wp-content/documents/da20080419.pdf.

60. Zadig Productions v. Google Inc., Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, Oct. 19, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2072.

61. *Id.*

62. *Id.*

63. *Id.*

content.[64] However, the court agreed with the plaintiff and imposed a duty on Google to implement all technical means necessary to avoid further dissemination of illicit content.[65] To avert this holding being in direct conflict with Article 15's prohibition of imposing a general monitoring obligation on intermediaries, the court considered the measures imposed on Google to be a "targeted and temporary surveillance" aimed at avoiding damage caused by specific content.[66] The court in *Zadig* required Google to adopt technological controls that actively prevent, rather than passively react to alleged infringing content. Subsequent decisions of the French Court of Appeals confirmed this duty—referred to as "take-down/stay-down"[67]—in a number of other cases where Google was the defendant.[68]

3. Imposing an Active Monitoring Obligation

In *Scarlet Extended SA v. Société belge des auteurs,compositeurs et éditeurs SCRL (SABAM)*,[69] the Brussels Court of First Instance ordered the access ISP, Scarlet, to implement technical measures which would make it impossible for its subscribers to send or receive music files held by SABAM through peer-to-peer file sharing software.[70] Unlike the French cases, which targeted content ISPs, *SABAM* was the first European case where the court imposed an active monitoring obligation on an access ISP. Because the ruling of the Belgian court contradicted the prohibition on general monitoring contained in Article 15 of the eCommerce Directive,[71] the Belgian appellate court referred the matter to the EU Court of Justice for a preliminary ruling.[72]

Court decisions in some of the EU member states put considerable pressure on ISPs operating in Europe to take a more active-preventive approach against online copyright infringements. Consequently, ISPs that wish to provide uniform services throughout the EU must accept the more stringent requirements imposed by some of the stricter jurisdictions. Moreover, ISPs face a high level of legal uncertainty because it is unclear

---

64. *Id.*

65. *Id.*

66. de Beer & Clemmer, *supra* note 21, at 400.

67. *See, e.g.*, Jane C. Ginsburg, *Take Down/Stay Down: RIP in France? But Little Solace for Google*, MEDIA INSTITUTE (Aug. 6, 2012), http://www.mediainstitute.org/IPI/2012/080612.php; Zohar Efroni, *Take Down Stay Down*, CENTER FOR INTERNET & SOCIETY (May 14, 2007), http://cyberlaw.stanford.edu/blog/2007/05/take-down-stay-down.

68. Craig R. Smith, *A World of Copyright Confusion on the Web*, NATIONAL L.J. (Oct. 20, 2011), http://www.lalaw.com/news-events/news/upload/CRS-ARTICLE-NLJ-20-OCT-2011-2.pdf (listing all the cases where Google was the defendant).

69. Case C-70/10, Scarlet Extended SA v. Société belge des auteurs,compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 (Nov. 24, 2011); *see also* SABAM v. S.A. Scarlet, District Court of Brussels (Mady, Bourrouilhou, & Hughes, trans.), 25 CARDOZO ARTS & ENT. L.J. 1279 (2008).

70. *Id.* at 1291.

71. In the questionable reasoning, the Belgian judges who issued the injunction seemed to argue that they do not have to consider prohibition on general monitoring since it only applies to decisions concerning ISP's liability, whereas injunctive relief does not examine liability issues. Moreover, the judges argued that "blocking and filtering certain information" does not amount to monitoring. *See id.* at 1289–90; Van Eecke, *supra* note 42, at 1459–61.

72. *See infra* Section II.B.

whether courts in other member states would follow the strict liability standard imposed by some member states, and notably the French courts.

B. REVERTING BACK TO PASSIVE-REACTIVE

1. The Proportionality Test

The EU Court of Justice has not received many opportunities to interpret ISP liability and the protection offered by the eCommerce Directive. *Productores de Musica de Espana (Promusicae) v. Telefónica de Espana SAU*[73] was the first case where the Court of Justice dealt specifically with obligations imposed on ISPs.

Promusicae, the Spanish organization of producers and publishers of musical and audiovisual recordings, brought suit against Telefónica, an access ISP, to require that it turn over records identifying users who were allegedly infringing Promusicae's copyrights through file sharing software.[74] Promusicae sought to obtain these records to launch a civil lawsuit against the individual users.[75] Telefónica was permitted to maintain these records pursuant to the EU Data Retention Directive,[76] which requires access ISPs to store user-identifying data[77] that can be used by law enforcement authorities to combat serious crimes.[78] The court stated that EU law required these disclosures to be available only for criminal proceedings and member states were not required to lay down similar exceptions for civil-law disputes, such as the enforcement of Promusicae's copyrights.[79] However, the court did not preclude member states from creating national legislation that had similar disclosure requirements for civil-law cases.[80]

The Court of Justice established a proportionality test, emphasizing that any legislation enacted must be proportionate to the seriousness of the infringement and strike a fair balance between competing fundamental rights protected by EU law.[81] In this case, the balancing focused on the fundamental right to property and the right to privacy.

2. The French Courts Attempt to Change Course

Recently, France's highest civil court, the Court de Cassation, rejected the take-down/stay-down rule developed in *Google Inc. v. Bac Films*.[82] The

73. Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271.

74. *Id.* at ¶ 29–31.

75. *Id.* at ¶ 30–31.

76. Council Directive 2006/24, 2006 O.J. (L 105) [hereinafter Data Retention Directive] (discussing the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks).

77. *Id.* at art. 5 ("Categories of data to be retained.").

78. *Id.* at rec. 21.

79. Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271 ¶ 51.

80. *Id.* at ¶ 53.

81. *Id.* at ¶ 49.

82. Cour de Cassation [Cass.] [supreme court for judicial matters] 1e civ., July 12, 2012, Bull.

court ruled that the duty to prevent the reposting of infringing content is equivalent to imposing a general obligation to monitor content, and is therefore prohibited by Article 15 of the eCommerce Directive.[83] This ruling was a victory for ISPs governed by French law, however, its impact may be limited since many ISPs continue to engage in voluntary content screening.[84]

Moreover, the court's decision signaled a disturbing development for online intermediaries. Previously, Google Videos allowed users to search for video clips across the Internet.[85] A search on Google would return a list of results allowing a user to either select a link that would redirect the user to a third-party website or play a video directly on Google's search interface. The content of the videos played directly on the Google search interface still resided on third-party servers, but through deep-linking[86] and framing[87] Google made the video accessible without the need to visit the original hosting website. The *Bac Films* court held that Google could be liable for the unlawful reproduction and public performance of copyrighted works played from its search interface.[88] The court recognized that although the infringing content was stored on third-party servers, Google made the content accessible directly through its website, and those actions surpassed providing "simple technical functionality," therefore exceeding the eCommerce Directive's protected actions.[89]

The French court in a later case adopted the same reasoning in a decision regarding the Google Autocomplete[90] search term function.[91] The court's requirement that ISPs provide "simple technical functionality" in order to qualify for the liability exemption does not reflect the wording of the eCommerce Directive and may impede services intermediaries offer in

---

civ. I, No. 831 (Fr.).

83. *Id.*

84. *See infra* Part III.

85. GOOGLE VIDEOS, https://www.google.com/videohp?gws_rd=ssl (last visited Oct. 7, 2014). Google no longer offers this option in its Video search. Its service now functions as a simple search engine. To access videos, users are redirected to third-party hosting websites. The 'original' system is still used in Google Images search where a user can see large picture thumbnails and decide whether she wants to access an image through the website hosting the image (by clicking on the "Visit page" button) or access the image file directly from Google's search interface (by clicking on the "View image" button).

86. *Deep Link*, WEBOPEDIA, http://www.webopedia.com/TERM/D/deep_link.html (last visited Oct. 7, 2014) (defining a 'deep link' as a "hyperlink either on a Web page or in the results of a search engine query to a page on a Web site other than the site's home page").

87. *Framing (World Wide Web)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Framing_(World_Wide_Web) (last modified June 29, 2014) (describing a 'frame' as "a part of a web page or browser window which displays content independent of its container, with the ability to load content independently").

88. Cour de Cassation [Cass.] [supreme court for judicial matters] 1e civ., July 12, 2012, Bull. civ. I, No. 831 (Fr.).

89. *Id.*

90. *Autocomplete*, GOOGLE, https://support.google.com/websearch/answer/106230?hl=en (last visited Oct. 7, 2014).

91. Cour de cassation [Cass.] [supreme court for judicial matters] 1e civ., July 12, 2012, Bull. civ. I, No. 832 (Fr.); *see also* Ginsburg, *supra* note 67 (discussing the decision in Google France v. Bac Films).

the Web 2.0 environment.[92]

The Court of Justice recently addressed the linking issue in *Svensson v. Retriever Sverige AB*.[93] In this case the Court of Justice held that hyperlinking to freely available copyrighted content cannot be considered an unlawful "communication to the public," as defined by the EU InfoSoc Directive.[94] Therefore, ISPs are not liable for copyright infringement through links to content residing on third-party websites or servers, unless they are aware that the link leads to illicit content, or the link would make it possible "to circumvent restrictions put in place by the site on which the protected work appears in order to restrict public access to that work [only] to the . . . site's subscribers."[95] The Court of Justice's decision clarifies that the passive-reactive approach also applies to hyperlinking material, and grants important protections for ISPs regarding content residing on third-party websites.[96]

3. ISPs Have No Obligation to Monitor Content

In response to the Belgian court's requirement for the access ISP to block transfers of music files through peer-to-peer sharing software in *Scarlet*,[97] the Court of Justice held that an ISP cannot be ordered to install filtering and blocking systems to prevent the transfer of potentially infringing files.[98] The court reasoned that such requirement would require ISPs "to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It . . . would require the ISP to carry out general monitoring, something which is prohibited by [the eCommerce Directive]."[99] The Court of Justice recalled the proportionality test from its decision in *Promusicae*, and also relied on language from the Charter of Fundamental Rights of the European Union:[100]

> Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.[101]

---

92. *Web 2.0*, WEBOPEDIA, http://www.webopedia.com/TERM/W/Web_2_point_0.html (last visited Oct. 22, 2014).

93. Case C-466/12, Svensson v. Retriever Sverige AB, 2014 E.C.R. I-0000 (Feb. 13, 2014).

94. Council Directive 2001/29, 2001 O.J. (L 167/10) [hereinafter InfoSoc Directive] (harmonizing certain aspects of copyright and related rights in the information society).

95. Case C-466/12, Svensson v. Retriever Sverige AB, 2014 E.C.R. I-0000 ¶ 31 (Feb. 13, 2014).

96. *See id.*

97. *See supra* Part II.A.3.

98. Case C-70/10, Scarlet Extended SA v. Société belge des auteurs,compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 (Nov. 24, 2011).

99. *Id.* at ¶ 40.

100. Charter of Fundamental Rights of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 1 [hereinafter EU Fundamental Rights Charter].

101. Case C-70/10, Scarlet Extended SA v. Société belge des auteurs,compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 ¶ 50 (Nov.

Following *Scarlet*, SABAM brought action against Belgian social media platform, Netlog, again asking the court to impose a broad filtering injunction.[102] Although factually similar to the previous action, content ISPs as well as legal practitioners paid close attention[103] to the Court of Justice's decision because it was not clear whether the court would extend the *Scarlet* reasoning concerning an access ISP to services offered by content ISPs. The court ultimately applied *Scarlet*'s reasoning, and held that the injunction violated the 'no obligation to monitor' principle of the eCommerce Directive because it was not proportionate to the seriousness of the infringement.[104] The court additionally found that the Belgian injunction was improper because it impinged on fundamental freedoms set out in the EU Fundamental Rights Charter, such as the ISPs' freedom to conduct business, users' rights to personal data protection, and the freedom of information.[105]

Both *SABAM* rulings are significant because they effectively draw a boundary for courts of the EU member states in imposing injunctions against online intermediaries. The Court of Justice rejected the shift toward active-preventive behavior of ISPs and set a course for uniform interpretation of the eCommerce Directive. However, practical impacts of the Court of Justice's rulings remain to be seen.

4. Germany—Rebel Without a Cause

In August 2013, more than one year after the Court of Justice's decision in *Netlog*, which prohibited placing general filtering and blocking obligations on ISPs, the German court in *GEMA v. RapidShare AG*[106] held that RapidShare—a provider of an online file-hosting service—had a duty to actively monitor its service for copyright infringement.[107] Although RapidShare complied with notice-and-takedown procedures and had a number of anti-infringement measures already in place,[108] the court found RapidShare guilty of inducing copyright infringement.[109] Consequently, the

---

24, 2011).

102. Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 E.C.R. I-00000, 2 C.M.L.R. 18 (2012), *available at* http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=EN.

103. *See, e.g.*, Monica Horten, Sabam v. Scarlet-*Will the ECJ Open Europe to Filtering Orders?*, IPTEGRITY.COM (Jan. 13, 2011), http://www.iptegrity.com/index.php/internet-trials/603-sabam-v-scarlet-will-the-ecj-open-europe-to-filtering-orders.

104. Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 E.C.R. I-00000, 2 C.M.L.R. 18 (2012), *available at* http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=EN.

105. *Id.* at ¶ 44–51.

106. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, ENTSCHEIDUNGSSAMMLUNG DES BUNDESGERICHTSHOF IN ZIVILSACHEN [BGHZ] (Ger.).

107. *Id.*

108. For example, RapidShare used basic filtering technologies, an infringement-reporting interface for copyright owners, and maintained a special 'abuse team' to monitor copyright infringement.

109. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, ENTSCHEIDUNGSSAMMLUNG DES BUNDESGERICHTSHOF IN ZIVILSACHEN [BGHZ] (Ger.). The German court found RapidShare liable because it did not implement "all possible" measures to effectively prevent its' users from sharing copyrighted content. The measures used by RapidShare

court required RapidShare to employ additional anti-infringement measures and conduct market monitoring to actively search for links to infringing files using publicly available resources, such as search engines, discussion forums, and social media sites.[110]

The German court acknowledged the protections for ISPs under the eCommerce Directive, but relied on Recital 48, which permits member states to "requir[e] service providers, who host information provided by [their users], to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities."[111] Although there is little doubt that RapidShare's services were predominantly used for illegal file sharing,[112] the measures imposed by the German court can hardly be reconciled with the Court of Justice's *SABAM* decisions. The Court of Justice has not currently responded to the *RapidShare* ruling.

C. WEBSITE BLOCKING—BACK TO ACTIVE-PREVENTIVE?

While the *SABAM* decisions concerned blocking access to specific content uploaded or transferred by users, a recent judgment of the Court of Justice took a step further. In *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*,[113] the Austrian court asked the Court of Justice to decide whether access ISPs can be required to block access to infringing websites altogether.[114] The Austrian court previously issued an injunction requiring an ISP to block access to a third-party website that infringed upon the plaintiffs' copyrights.[115] The infringing third-party website was hosted on servers located outside of the EU, thus outside of the Austrian court's jurisdiction.[116] This required the plaintiffs to bring the case against the Austrian access ISP, UPC, in order to prevent its subscribers from accessing the third-party website.[117]

Plaintiffs based their claim on provisions of EU law, which require member states to ensure that copyright holders can "apply for an injunction against intermediaries whose services are used by a third party to infringe a

(including use of a data-filter program) were in the court's view insufficient and RapidShare failed to prove it has undertaken "all reasonable steps" to prevent sharing of copyrighted content. *Id.*

110. *Id.*

111. Directive 2000/31, *supra* note 3, at rec. 48.

112. A majority of RapidShare users used its services predominantly for downloading copyrighted content. RapidShare incentivized sharing activity by offering free memberships and financial benefits for users whose files reached a high number of downloads. However, while sharing copyrighted content without permission is generally illegal in all EU member states, in some EU jurisdictions, including the Czech Republic, it is legal to download copyrighted content for personal use.

113. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000 (Mar. 27, 2014).

114. *Id.*

115. *Id.* at ¶ 12.

116. *See id.* at ¶ 23.

117. *Id.*

copyright or related right."[118] The ISP argued liability should only be imposed on content ISPs that make infringing materials available online, and should not apply to access ISPs merely connecting end-users to the Internet.[119] The ISP further claimed that content owners should seek remedies against the actual infringer—the website operator.[120] The Court of Justice rejected this distinction and ruled it legal under EU law to impose website-blocking obligations on access ISPs.[121] According to the court's reasoning, access ISPs must be considered intermediaries "whose services are used to infringe a copyright," and therefore may be subject to a website-blocking injunction.[122]

The court went on to assess the impact on fundamental rights and freedoms enshrined in the EU Fundamental Rights Charter.[123] The court concluded that a website-blocking order does not infringe these rights as long as the choice of appropriate blocking-measures is left to the ISPs, and Internet users still receive access to lawful content.[124]

This decision puts ISPs in a difficult position. As a result of simply connecting its subscribers to the Internet, every access ISP in the EU is now considered "an intermediary whose services are used to infringe a copyright."[125] ISPs are confronted with a dilemma when courts impose injunctions. An injunction requires the ISP to adopt measures which are "sufficiently effective to ensure genuine protection" of copyrights,[126] yet also requires the ISP to "ensure compliance with the fundamental right of freedom of information for internet users."[127] If an ISP employs measures that are easy to circumvent, it would risk sanctions for non-compliance. However, if an ISP employs blocking measures that are too restrictive, it risks liability for violating its customers' freedoms.[128] The Court of Justice did not offer any guidance on resolving this dilemma. Consequently, it is

118. InfoSoc Directive, *supra* note 94, at art. 8(3).

119. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2014 E.C.R. I-00000 (Mar. 27, 2014).

120. In fact, the website at issue (kino.to) ceased operation in June 2011—long before the Court of Justice's judgment—following enforcement action of the German police forces against its operators. *See id.* at ¶ 13.

121. *Id.*

122. *Id.* at ¶ 32.

123. *Id.* at ¶ 47 ("In the present case, it must be observed that an injunction such as that at issue in the main proceedings, taken on the basis of Article 8(3) of Directive 2001/29, makes it necessary to strike a balance, primarily, between (i) copyrights and related rights, which are intellectual property and are therefore protected under Article 17(2) of the Charter, (ii) the freedom to conduct a business, which economic agents such as internet service providers enjoy under Article 16 of the Charter, and (iii) the freedom of information of internet users, whose protection is ensured by Article 11 of the Charter.").

124. *Id.* at ¶ 54–64.

125. Copyright owners do not even need to demonstrate some of the ISP's customers were actually accessing an infringing content. For a court to issue a blocking-injunction it merely suffice the possibility of accessing an infringing website exists. *See id.* at ¶ 36.

126. *Id.* at ¶ 62–63.

127. *Id.* at ¶ 55.

128. The Court of Justice stated that the national procedural rules must provide a possibility for the ISPs customers to assert their rights before the court once blocking measures taken by the ISP are known. *See id.* at ¶ 57.

the responsibility of the individual member state's national courts to determine whether a proper balance is struck between the two opposing duties. This may result in different standards for ISPs across EU member states.

Surprisingly, the court did not discuss the monitoring prohibition of Article 15 of the eCommerce Directive. Advocate General Villalón analyzed Article 15 and the imposition of an injunction, arguing that the injunction only concerns a specific website, and thus is not considered a monitoring obligation.[129] It could be concluded from the decision that the Court of Justice simply viewed the access ISPs as best situated to put an end to copyright infringement on international websites in situations where other remedies may not be effective or available to copyright holders. While access ISPs are in a better position to effectively police copyright infringement, the Court of Justice's logic shifts responsibility for copyright monitoring onto neutral parties who are required to incur significant costs and expend substantial resources in complying with these injunctions. Even before the *UPC Telekabel Wien* ruling, courts in the United Kingdom and France ordered access ISPs to block off-shore peer-to-peer file sharing websites.[130] In some instances, the blocked websites functioned as mere aggregators, providing links to video-streams hosted on other websites.[131] In all of these cases, the courts argued that in the absence of an alternative and effective method of relief for copyright holders, requiring access ISPs to block infringing websites is justified. With the support of the Court of Justice, copyright holders will likely take full advantage of the newly available blocking mechanism, even in countries where judges have been reluctant to issue website-blocking injunctions.[132] Such website-blocking requirements will likely become a widely implemented remedy in the EU.

1. The Effectiveness of Website-Blocking

Although courts issue blocking injunctions to provide copyright holders with a form of relief, it is hard to assess the effectiveness of the blocking measures. For example, website owners as well as end-users can

---

129. *Id.* at ¶ 77–78.

130. *See, e.g.*, Twentieth Century Fox Film Corp. & Ors v. British Telecomm. PLC, [2011] EWHC 1981 (Ch), July 28, 2011, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html (U.K.); Dramatico Ent. Ltd. v. British Sky Broad. Ltd., [2012] EWHC 268 (Ch), Feb. 20, 2012, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html (UK); The Football Ass'n Premier League Ltd. v. British Sky Broad. Ltd. & Ors, [2013] EWHC 2058 (Ch), July 16, 2013, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2013/2058.html (UK); APC et autres v. Auchan Telecom, Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, Nov. 28, 2011, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3935.

131. *See* The Football Ass'n Premier League Ltd. v. British Sky Broad. Ltd. & Ors, [2013] EWHC 2058 (Ch), July 16, 2013, ¶ 6, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2013/2058.html (UK).

132. *See, e.g.*, EMI Records (Ireland) Ltd. & Ors v. UPC Commc'ns Ireland Ltd., [2010] IEHC 377, Oct. 11, 2010, ¶ 138, *available at* http://www.bailii.org/ie/cases/IEHC/2010/H377.html (refusing to issue an injunction due to lack of statutory support for such measure, although he found the relief to be merited on the facts).

easily circumvent a blocked domain name and IP address of an illicit website.[133] The Dutch Court of Appeals recognized this inefficiency in *Zigo B.V. v. Stichting Bescherming Rechten Ent. Industrie Nederland Brein*,[134] which was decided prior to the Court of Justice's ruling in *UPC Telekabel Wien*. The Dutch court observed that blocking had only minimal impact on user behavior, and ordered the injunction at issue be lifted immediately.[135] While the Dutch court's decision demonstrates that courts pay attention to the practical effects of issued injunctions, it is not beyond the courts' power to additionally require the ISP to implement measures that make website-blocking more effective.

Furthermore, blocking entire websites creates the risk of blocking legitimate non-infringing content.[136] A website with an equal amount of illicit and legitimate content should not be regarded as dedicated to infringement, nor should it be subjected to blocking injunctions. Courts must determine how much legitimate content is necessary to prevent blocking injunctions. Also, courts must assess whether the infringing content generates the majority of the website's traffic.[137] Again, these important questions are left for the courts of the individual member states to decide.

III. GROWING COLLABORATION BETWEEN ISPS AND CONTENT-OWNERS

While ISPs and copyright content owners stand on opposite sides of the courtroom, outside the judicial environment their positions are less adversarial. Over the past few years, collaboration between Internet intermediaries and content owners has grown worldwide. ISPs try to convince the public that their main interest is to preserve the free and open nature of the Internet.[138] The idea behind this is that it is essential for online intermediaries to be immune from liability for third-party content,

---

133. Websites may easily relocate their content to a different server with a new IP address and domain name. Users have various options to circumvent blocking measures. *See Internet Censorship Circumvention*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_censorship_circumvention (last modified Oct. 3, 2014).

134. Hof's-Den Haag 28 januari 2014, (unpublished) (Ziggo B.V./Stichting Bescherming Rechten Ent. Industrie Nederland Brein) (Neth.), *available at* http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2014:88 (indicating that BREIN is a Dutch entity encompassing authors, artists, filmmakers and software designers).

According to the study of Dutch researches relied upon in the courts ruling, only 4 to 6 percent of users have decreased their downloading activity as a result of the blocking. *See* Cyrus Farivar, *Blocking Doesn't Work: Dutch Court Lifts Pirate Bay Ban*, ARS TECHNICA (Jan. 28, 2014), http://arstechnica.com/tech-policy/2014/01/blocking-doesnt-work-dutch-court-lifts-pirate-bay-ban/.

135. Hof's-Den Haag 28 januari 2014, ¶ 5.25–5.26 (unpublished) (Ziggo B.V./Stichting Bescherming Rechten Ent. Industrie Nederland Brein) (Neth.), *available at* http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2014:88.

136. *See infra* Part IV.C.

137. Jane C. Ginsburg, *Copyright Enforcement in the EU: The Return of Website Blocking*, MEDIA INSTITUTE (Dec. 30, 2013), http://www.mediainstitute.org/IPI/2013/123013.php.

138. *See* Andy Greenberg, *CEO of Internet Provider Sonic.net: We Delete User Logs After Two Weeks. Your Internet Provider Should, Too.*, FORBES (June 22, 2012).

otherwise ISPs would decline to offer even simple web-services such as discussion forums, and the progression of the Internet and related technologies would cease. Despite seeking immunity, many ISPs are interested in active content monitoring.

Traditional content industries have consistently been reluctant to embrace new technologies and new methods for content distribution.[139] This also holds true in the online environment, and the court decisions favoring ISPs provide considerable leverage for online intermediaries to negotiate with copyright content owners. Although the motivations of each party may be different, voluntary collaboration between ISPs and content owners has often produced similar outcomes as to what content owners strive to achieve through litigation.

A. OPPORTUNITIES FOR MONETIZING CONTENT

The video 'fingerprinting'[140] technology YouTube uses to battle copyright infringement is an example of how collaboration is beneficial for both copyright content owners and ISPs.[141] YouTube scans each video users upload and compares its digital fingerprint with reference files stored in its database. If a match is found, YouTube applies the policy chosen by the copyright owner of the matched reference file. Examples of chosen policies include blocking the uploaded video, placing commercials over the video, or even leaving the video intact. All videos uploaded on YouTube are subject to this process. This self-imposed procedure essentially creates an active monitoring system, which is precisely what copyright content owners are seeking through litigation.[142] Despite YouTube successfully defending itself against claims requiring it to actively prevent reposts of infringing videos,[143] it nevertheless deploys similar monitoring measures voluntarily and worldwide.

Two motivations explain why YouTube or other ISPs would engage in voluntary content monitoring. First, implementing a notice-and-takedown system comes at a cost. When an ISP receives a notice of potential copyright infringement it must allocate resources to assessing the validity of the claims and to administer the takedown. Second, fingerprinting

139. *See, e.g.*, Lawrence Lessig, *Laws That Choke Creativity*, TED (Mar. 2007), *available at* http://www.ted.com/talks/larry_lessig_says_the_law_is_strangling_creativity.

140. A file's fingerprint is a unique line of code generated based on file type, content and size.

141. *See Copyright on YouTube*, YOUTUBE, http://youtube.com/yt/copyright/?rd=1 (last visited Oct. 8, 2014). YouTube's reference file database includes over 3 million 'fingerprints.' Each minute, users upload roughly twenty-four hours of video on YouTube, therefore every day, the Content ID Match processes over 100 years of video content.

142. *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); Zadig Productions v. Google Inc., Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, Oct. 19, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2072.

143. *See, e.g.*, *Viacom Int'l, Inc.*, 676 F.3d at 19; Zadig Productions v. Google Inc., Tribunal de Grande Instance [TGI] [ordinary court of original jurisdiction] Paris, Ordonnance de référé, Oct. 19, 2007, *available at* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2072; Cour de Cassation [Cass.] [supreme court for judicial matters] 1e civ., July 12, 2012, Bull. civ. I, No. 831 (Fr.).

uploaded content allows ISPs to generate more revenue by adjusting advertising rates in accordance with the market value of the content.[144] If a content owner allows its video to be displayed with a commercial advertisement, it is likely to attract more viewers, and YouTube may set substantially higher prices for these commercials. Additionally, when YouTube identifies the actual content of a video clip, it may adjust the content of the displayed advertisements to target the appropriate viewing demographic. YouTube then shares the collected revenue with the content owner as a reimbursement for a copyright license.[145] This monetizing scheme could not exist without cooperation between YouTube and the copyright content owners.

However, due to the passive requirement in the safe harbor provisions, once YouTube obtains a direct financial benefit from copyright infringing content it could lose its immunity and be liable for contributory infringement.[146] If an ISP wants to fully realize the economic value of the content it hosts on its website, the best option is to reach an agreement with the content owners.

In March 2014, YouTube's trend of collaborating with content owners was confirmed in its final litigation settlement with Viacom.[147] Viacom accused YouTube of inducing infringement to make a profit.[148] Viacom lost its initial case[149] and on appeal,[150] and then lost again on remand in the district court.[151] However, both companies ultimately reached a seemingly friendly settlement. In a joint statement, the two companies stated, "This settlement reflects the growing collaborative dialogue between our two companies on important opportunities, and we look forward to working more closely together."[152]

B. MANAGING THE CONTENT

Another example of a company engaging in voluntary active file monitoring is Dropbox. Dropbox recently started preventing its users from sharing copyrighted content in publicly accessible links.[153] Similar to

144. Ginsburg, *supra* note 67.

145. YouTube expressly states "monetization" as one of the options available to copyright owners. *How Content ID Works*, GOOGLE, https://support.google.com/youtube/answer/2797370 (last visited Oct. 22, 2014).

146. *See supra* Part I.B.

147. *Viacom Int'l, Inc.*, 676 F.3d at 19.

148. *Id.* at 21.

149. *Id.*

150. *Id.* at 42.

151. Viacom Int'l, Inc. v. YouTube, Inc., 970 F. Supp. 2d 110, 123 (S.D.N.Y. 2013).

152. Jonathan Stemple, *Google, Viacom Settle Landmark YouTube Lawsuit*, REUTERS (Mar. 18, 2014), http://www.reuters.com/article/2014/03/18/us-google-viacom-lawsuit-idUSBREA2H11220140318.

153. *See, e.g.*, Kyle Orland, *Dropbox Clarifies Its Policy on Reviewing Shared Files for DMCA Issues*, ARSTECHNICA (Mar. 31 2014), http://arstechnica.com/tech-policy/2014/03/dropbox-clarifies-its-policy-on-reviewing-shared-files-for-dmca-issues/; *Important Note on Copyrighted Material*, DROPBOX, https://www.dropbox.com/en/help/167 (last visited Oct. 22, 2014).

YouTube, Dropbox compares a file's fingerprint with digital fingerprints of files it has previously taken down through its notice-and-takedown procedure.[154]

Dropbox does not engage in active file monitoring with the intent to profit, rather the company tries to prevent unnecessary duplication of large files on its servers to save hard-drive space and reduce bandwidth.[155] In practice, Dropbox is actively preventing users from sharing copyrighted content that has already been reported as illegal by content owners. This practice essentially engages in active monitoring to prevent reposts of infringing content.

C. COLLABORATION OF ACCESS ISPS AND CONTENT OWNERS

Content owners and access ISPs are also collaborating. In 2008, the British access provider Virgin Media, in cooperation with the British Recording Industry Association (BPI), launched an educational campaign that sent warning letters to its customers who allegedly downloaded illegal files.[156] Later that year, with pressure from the British government, five major access ISPs signed a Memorandum of Understanding[157] together with content owners and the government. The memorandum stated that in addition to issuing warning letters to users, access ISPs would implement penalties such as network connection slow-down for persistent infringers.[158]

In 2011, large content owners' associations[159] and major access ISPs[160] in the United States established the Center for Copyright Information (CCI).[161] The CCI represents itself as an educational initiative,

---

154. *See* Greg Kumparak, *How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff)*, TECHCRUNCH (Mar. 30, 2014), http://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/.

155. *See* Orland, *supra* note 153.

156. Although Virgin Media claimed its campaign is merely educational, the first round of letters (around 800) featured a large red sticker stating: "Important—if you don't read this, your broadband could be disconnected." *See* Claudine Beaumont, *Virgin Media Blames 'Administrative Oversight' for Threats on Warning Letters*, TELEGRAPH (July 4, 2008), http://www.telegraph.co.uk/technology/3357777/Virgin-Media-blames-administrative-oversight-for-threats-on-warning-letters.html. Virgin Media later removed the sticker and blamed its placement on envelopes on an administrative mistake. *See id.* The company expressed it had no intention of disconnecting its customers from the Internet. *See id.*

157. *See Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing*, Dep't of Bus. Enter. & Regulatory Reform, July 2008, *available at* http://webarchive.nationalarchives.gov.uk/20080726153746/http:/www.berr.gov.uk/files/file47139.pdf; *Net Firms in Music Pirates Deal*, BBC (July 24, 2008), http://news.bbc.co.uk/2/hi/technology/7522334.stm.

158. *See Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing*, Dep't of Bus. Enter. & Regulatory Reform, July 2008, *available at* http://webarchive.nationalarchives.gov.uk/20080726153746/http:/www.berr.gov.uk/files/file47139.pdf.

159. For example, Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA), Independent Film and Television Alliance (IFTA), and American Association of Independent Music (A2IM).

160. For example, AT&T, Cablevision, Comcast, Time Warner Cable, and Verizon.

161. *Center for Copyright Information*, WIKIPEDIA, http://en.wikipedia.org/wiki/Center_for_Copyright_Information (last modified July 1, 2014).

but, more importantly, serves as a cooperation platform for the Copyright Alert System (CAS).[162] The CAS is a reporting system set up between participating content owners and ISPs.[163] Content owners scan the Internet and look for illegal sharing of their content, and if they spot an alleged infringer, they report the IP address to a participating ISP.[164] The ISP then matches the IP address with a physical person in its customer database and sends a standardized warning letter.[165] ISPs maintain records of alleged illegal downloaders, and if a user continues engaging in infringing activity the ISP will send more severe warnings and then ultimately reduce the connection speed of an alleged infringer.[166] This practice is coined as the notice-and-slowdown procedure.[167]

D. COLLABORATION ARGUABLY BENEFITS EVERYONE

The rising collaboration between content owners and online intermediaries has the potential to benefit all parties, including Internet users. YouTube's collaboration practices, for example, benefit users by continuing to provide access to content that would otherwise be blocked had the copyright owner simply demanded its removal. It is also becoming increasingly easier and cheaper for Internet users to access copyrighted content online through new streaming services.[168] These services arguably make illegal music and video sharing inconvenient and unnecessary.[169]

IV. POTENTIAL HARMS OF ACTIVE-PREVENTIVE ISPS

Although the aforementioned trends seem positive, they could also have a negative impact on Internet users and the general functionality of the Internet. Even if adopted voluntarily, new measures employed by ISPs represent a significant departure from the passive-reactive role envisioned in the eCommerce Directive and the DMCA.

---

162. *Id.*

163. *What is a Copyright Alert?*, CENTER FOR COPYRIGHT INFO., http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/ (last visited Oct. 8, 2014).

164. *Id.*

165. *Id.*

166. *Id.*; Center for Copyright Information, Memorandum of Understanding, at § 4.G. (July 6, 2011); *What is a Copyright Alert?*, CENTER FOR COPYRIGHT INFO., http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/ (last visited Oct. 8, 2014).

167. *See, e.g.*, de Beer & Clemmer, *supra* note 21; Van Eecke, *supra* note 42.

168. For example, various free or subscription-based music and video streaming services, such as Spotify, Pandora, iTunes Radio, Netflix, or Hulu.

169. *See, e.g.*, Hayley Tsukayama, *Music Piracy on the Decline as Digital Music Sales Grow*, WASHINGTON POST (Feb. 26, 2013), http://www.washingtonpost.com/business/technology/music-piracy-on-the-decline-as-digital-music-sales-grow/2013/02/26/5ca43fe2-804b-11e2-b99e-6baf4ebe42df_story.html; Sophie Curtis, *Spotify and Netflix Curb Music and Film Piracy*, TELEGRAPH (July 18, 2013), http://www.telegraph.co.uk/technology/news/10187400/Spotify-and-Netflix-curb-music-and-film-piracy.html.

A. IMPACT ON USER PRIVACY[170]

ISPs have the unique ability to gather a massive amount of sensitive information about their users. ISPs can easily record, store and retrace every action of their users. A seemingly modest sample of Internet activity records such as websites visited, links clicked, and search terms entered, nevertheless establish a detailed user-profile. Records of online activity provide reliable information about a user's personality, ranging from their nationality, interests, place of residence, work and educational background, political beliefs, health concerns, or even sexual preferences and fantasies.

Although most individuals have a basic understanding of the scope of information collected by online intermediaries, the amount of data given to online service providers is usually underestimated.[171] However, content ISPs are limited by the fact that they can only track users' activities on their servers. For example, once a user leaves Google's website, Google cannot continue to track any activity on a third-party site.[172] Thus, content ISPs' monitoring abilities are limited and users can maintain at least a certain level of privacy by separating their conduct in various online environments.

By contrast, access ISPs can monitor all of its users' activities because traffic exchanged between a user and the Internet must pass through the access ISP's network.[173] This ability to accumulate mass amounts of user data likely explains the recent attempts to shift responsibility for policing copyright content onto access ISPs.[174] Access ISPs are simply in the best position to monitor and regulate content passing through its Internet network. As seen from the court decisions and initiatives, ISPs can implement measures to prevent future re-postings of certain content, filter certain types of data transfers, block access to websites, or slow down

---

170. This Article does not deal with the important topic of online surveillance employed by government agencies and its implications for online intermediaries. *See, e.g.*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008); PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014); Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program*, 12 COLO. TECH. L.J. 309 (2014).

171. *See* Chris Jay Hoofnagle, Ashkan Soltani, Nathan Good, Dietrich James Wambach & Mika Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273 (2012).

172. Due to advances in technology and lack of stricter privacy rules for the online environment, content ISPs are now able to considerably erode this concept and track users across multiple services (e.g., DoubleClick services owned by Google). In this regard (compared to the U.S.) the EU legislation imposes much stricter obligations on online intermediaries. *See, e.g.*, Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281 (2012).

173. Arguably, there is some information an access ISP will not be able to monitor, or, more accurately, that would be much harder for an access ISP to collect. For example, it cannot track users when they connect through the network of a different access ISP, e.g., at the workplace, in a cafe, or on a bus stop through their smartphone. Conversely, a content ISP can track its users regardless of the place they connect from because users 'sign in' to their profiles. An access ISP cannot read the content of user's emails (while Google does) and may have a hard time distinguishing between individual persons in a household it connects (which is not a problem for Whatsapp because each user has a unique ID).

174. *See supra* Part III.C.

selected types of data transfers.

In order to receive and send information on the Internet, a user must go through an access ISP and no longer has the option to adjust user behavior between different intermediaries or decide what to disclose to a particular entity. Regarding access ISPs, a user's only choice is either allow the ISP to gather information or not use the Internet. Until now, access ISPs did not engage in active monitoring because they lacked the necessary technical means,[175] or were prevented from doing so by privacy legislation.[176] More importantly, safe harbor provisions of the eCommerce Directive and the DMCA provided strong disincentives for access ISPs to engage in content monitoring since a passive-neutral approach would insulate them from illicit conduct on their networks.[177] Removing the passive-neutral requirement would seriously threaten users' privacy by incentivizing or requiring access ISPs to engage in content monitoring.

B. MAINTAINING NETWORK NEUTRALITY[178]

The debate over network neutrality is principally concerned with the treatment of data transfers over the Internet. Access ISPs, which own and maintain the Internet's infrastructure, argue that they should be allowed to differentiate between various types of traffic passing through their networks. They want to charge extra fees to content ISPs for the fast and reliable delivery of content to their subscribers.[179] Access ISPs point to possible network congestion and the lack of incentive for investment in faster network infrastructure as justification for the imposition of an additional fee.[180]

Advocates of network neutrality believe that access ISPs should not

---

175. Scanning passing traffic in real time requires considerable computing power. For a long time, the volume of traffic passing through ISPs networks overwhelmed ISPs' ability to effectively monitor. In the last decade, advances in computing speeds have overcome this difference and for some ISPs real-time traffic monitoring is now possible. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009).

176. *See* Council Directive 95/46, 1995 O.J. (L 281).

177. *See supra* Part II.B.

178. *See, e.g.*, Timothy Wu, *Copyright' s Communications Policy*, 103 MICH. L. REV. 278, 279 (2004); Christopher Marsden, *Net Neutrality Law: Past Policy, Present Proposals, Future Regulation?*, Proceedings of the United Nations Internet Governance Forum: Dynamic Coalition on Network Neutrality (Oct. 25, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335359.

See Ensure Open Access for Internet Service Suppliers and Ban Roaming Fees, Say MEPs, European Parliament Press Relies, EUROPEAN PARLAMENT (Apr. 3, 2014), http://www.europarl.europa.eu/news/en/news-room/content/20140331IPR41232/html/Ensure-open-access-for-internet-service-suppliers-and-ban-roaming-fees-say-MEPs; Brian Fung, *Everything You Should Know About the FCC's New Net Neutrality Proposal*, WASHINGTON POST (Apr. 24, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/24/everything-you-should-know-about-the-fccs-new-net-neutrality-proposal/.

179. Some content creates more Internet traffic than others and some content is more traffic-sensitive than the other. According to the study conducted by Canadian Internet monitoring firm Sandvine, in 2013, over 50% of downstream Internet traffic on fixed Internet networks in Northern America was produced by Netflix (31.6%) and YouTube (18.1%). *See* Sandvine Global Internet Phenomina Report (2014), *available at* https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf.

180. de Beer & Clemmer, *supra* note 21, at 408.

discriminate against individual content providers or applications, because it would disrupt the freedom and democratizing nature of the Internet.[181] If access ISPs are free to decide what content will pass through and at what speed, they would effectively become gatekeepers of the Internet.[182] Preferential data treatment could stifle innovation and impair content delivery from smaller and non-commercial intermediaries that could not afford to pay for the faster data treatment.[183] Access providers could also use different data treatment to discriminate against specific content or applications and intimidate competing producers.[184]

Potential implications on users' privacy also cause concern in regards to network neutrality. In order to differentiate and manage Internet traffic, an access ISP would necessarily have to engage in detailed data scanning—deep-packet-inspection.[185] Instead of looking only at the surface-layer information of a particular data packet (i.e., its origin and its destination), an access ISP would instead deeply examine each piece of data to find out if it qualifies for fast-lane treatment. The right to privacy would be compromised in this process because the ISP would not only be able to see the source and destination of each data packet, but also the content it carries.

C. CRIMINALIZING THE USER

Monitoring user activity inherently assumes that users engage in illegal conduct. The fundamental standard of justice—innocent until proven guilty—would transform into being guilty until proven innocent[186] due to the ease of monitoring users' activity and ability to locate and prove specific instances of infringement. Although advanced scanning technology may mitigate privacy concerns,[187] the fact that all actions are being monitored may be enough to cause substantial discomfort among Internet users, and would have a chilling effect on expression and speech.[188]

---

181. Ian Tuttle, *'Net Neutrality'? No Thank You*, NATIONAL REVIEW ONLINE (Nov. 10, 2014), http://www.nationalreview.com/corner/392462/net-neutrality-no-thank-you-ian-tuttle.

182. *See id.*

183. *See id.*

184. *See, e.g.*, Jon Brodkin, *Netflix Performance on Verizon and Comcast Has Been Dropping for Months*, ARS TECHNICA (Feb. 10, 2014), http://arstechnica.com/information-technology/2014/02/netflix-performance-on-verizon-and-comcast-has-been-dropping-for-months/; Jon Brodkin, *Why YouTube Buffers: The Secret Deals that Make—and Break—Online Video*, ARS TECHNICA (July 28, 2013), http://arstechnica.com/information-technology/2013/07/why-youtube-buffers-the-secret-deals-that-make-and-break-online-video/.

185. Ohm, *supra* note 175, at 1468.

186. Clay Shirky, *Why SOPA is a Bad Idea*, TED (Jan. 17, 2012), http://www.ted.com/talks/defend_our_freedom_to_share_or_why_sopa_is_a_bad_idea.

187. *See, e.g.*, *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs: Hearing Before the S. Comm. on the Judiciary*, 110th Cong., 1st Sess. 154 (2007) (testimony of Kim A. Taipale) (discussing similar issues regarding government surveillance programs).

188. *See* Brief for Nat'l Rifle Ass'n of Am., Inc. as Amici Curiae Supporting Plaintiff, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-03994 (WHP)), 2013 WL 5221413 (providing arguments concerning possible violation of the First Amendment to the U.S. Constitution due to 'chilling effects' of government surveillance on the freedom of speech and the freedom of assembly).

Additionally, automated monitoring systems may be able to identify copyrighted materials, but they cannot determine whether the user obtained a necessary license or whether the activity is covered by the fair-use doctrine—something even experienced lawyers and judges have difficulty assessing.[189] Thus, the potential negative effects on individual freedoms of expression and speech outweigh the positives associated with automated monitoring and blocking.[190]

CONCLUSION

Initially, judicial decisions in EU member states disrupted the effectiveness of the ISP safe harbor provisions. However, the EU Court of upheld the EU's safe harbors provisions and protect passive-reactive ISPs from liability for contributory copyright infringement. But in its recent judgment, the Court of Justice demonstrated sympathy for European content owners. Although the consequences of the Court of Justice's ruling in *UPC Telekabel Wien* remain to be seen, it has caused some unrest in safe harbor jurisprudence.

Preventing copyright infringement on the Internet may seem futile. Frustration among copyright content owners often results in litigation against online intermediaries rather than the individual perpetrators. In the discussion about ISP liability, both the content owners and ISPs present legitimate arguments. ISPs provide the infrastructure and services that facilitates copyright infringement and they often benefit—though not always intentionally—from infringing activity. In the most extreme cases, ISPs treat the safe harbors offered by the eCommerce Directive and the DMCA as an insurance policy against the content owners' claims.[191] However, imposing a strict one-size-fits-all liability standard on ISPs could seriously undermine the free, open, and innovative nature of the Internet. Additionally, policing copyright infringement is costly. For many ISPs, monitoring every piece of content is not financially feasible or technically possible. Moreover, content monitoring has serious implications for Internet users' rights to privacy and freedom of speech.

Copyright owners are now realizing that litigation is not the most effective way to solve their problems. Instead, content owners and ISPs are finding a common ground and collaborating. These initiatives and collaborations may be beneficial for all parties, including Internet end-users. Declining levels of illegal file-sharing demonstrate positive effects of these measures, and Internet users are utilizing the new online services that

189. *See* Cariou v. Prince, 714 F.3d 694 (2d Cir. 2013) (providing a recent dispute pertaining to the scope of transformative use and the scope of the fair-use doctrine in transformative art).

190. Hannibal Travis, *Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law*, 84 NOTRE DAME L. REV. 331 (2008).

191. These 'extreme' cases include various file hosting/sharing services, whose main source of revenue is apparently based on attracting users by facilitating illegal file sharing. A notable example of massive copyright violation facilitated by an ISP is the well-known PirateBay website, famous for its entertaining responses to notice-and-takedown demand letters. *Legal Threats Against the Pirate Bay*, PIRATE BAY, http://thepiratebay.se/legal (last visited Oct. 22, 2014).

are often produced as a result of the collaboration agreements.

Today, the debate concerning the role of ISPs revolves around copyright infringement. Consequently, courts and policy makers should be mindful of the repercussions copyright enforcement policies could have on other aspects of the Internet, including issues of privacy, freedom of information, and network neutrality. A policy that focuses solely on copyright infringement and fails to recognize other important issues could transform the Internet into a very different place. To ensure the Internet remains free, open, and innovative, it is necessary to move beyond the copyright debate.