Liability for Providing Hyperlinks to Copyright-Infringing Content: International and Comparative Law Perspectives

Jane C. Ginsburg[*] and Luke Ali Budiardjo[**]

Abstract

Hyperlinking, at once an essential means of navigating the Internet, but also a frequent means to enable infringement of copyright, challenges courts to articulate the legal norms that underpin domestic and international copyright law, in order to ensure effective enforcement of exclusive rights on the one hand, while preserving open communication on the Internet on the other. Several recent cases, primarily in the European Union, demonstrate the difficulties of enforcing the right of communication to the public (or, in US copyright parlance, the right of public performance by transmission) against those who provide hyperlinks that effectively deliver infringing content to Internet users. This article will first address the international norms that domestic laws of states member to the multilateral copyright agreements must implement. It next will explore how two of the most significant regional or national copyright regimes, the EU and the US, have coped with the question of linking, and then will consider the relationship of the emerging approaches to copyright infringement with national and regional laws instituting limited immunity for copyright infringements committed by internet service providers. We will conclude with an assessment of the extent to which the outcomes under US and EU regimes, despite their apparently different approaches, in fact diverge.

Table of Contents

[*] Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia Law School. Thanks for comments and suggestions to Susy Frankel, Daniel Gervais and Sam Ricketson.
[**] Columbia Law School class of 2018.

Hyperlinks connect Internet users to content residing on the Internet. "Simple" links take the user to a website's home page from which she may navigate to specific works; "deep" and "in-line" or "framing" links[1] bring the user directly to the content the user seeks, in the latter case by

[1] The terms "in-line linking" and "framing" are conceptually very similar. Generally, "in-line linking" or "embedded linking" refers to the process of importing a piece of content from another website through a hyperlink. "Framing" is a more specific term that refers to the combination of materials from different sources on a single website through in-line hyperlinks, but may refer specifically to uses in which the imported content is presented independently through a "gateway" or "independently scrollable frame[]." See Mark Sableman, Link Law Revisited: Internet Linking Law at Five Years, 16 Berkeley Tech. L.J. 1273, 1297--1299 (2001). For clarity, this article will use the term "in-line linking" to refer to both practices.

presenting the content "framed" by the website the user first consulted to locate the requested works. Linking, at once an essential means of navigating the Internet, but also a frequent means to enable infringement of copyright, challenges courts to articulate the legal norms that underpin domestic and international copyright law, in order to ensure effective enforcement of exclusive rights on the one hand, while preserving open communication on the Internet on the other. Several recent cases, primarily in the European Union, demonstrate the difficulties of enforcing the right of communication to the public (or, in US copyright parlance, the right of public performance by transmission) against those who provide hyperlinks that effectively deliver infringing content to Internet users. This article will first address the international norms that domestic laws of states member to the multilateral copyright agreements must implement. It next will explore how two of the most significant regional or national copyright regimes, the EU and the US, have coped with the question of linking, and then will consider the relationship of the emerging approaches to copyright infringement with national and regional laws instituting limited immunity for copyright infringements committed by internet service providers. We will conclude with an assessment of the extent to which the outcomes under US and EU regimes, despite their apparently different approaches, in fact diverge.

PART I: INTERNATIONAL STANDARD

Because hyperlinks enable users to access content residing on the internet, one may conceptualize the provision of a hyperlink as a form of making works available to the public. The 1996 WIPO Copyright treaties introduced the "making available" right in order to modernize the exclusive right of communication to the public under the Berne Convention,[2] to make it suitable for implementation in the digital environment.[3] The Berne Convention includes rights of communication to the public by primary and secondary transmission by wired and wireless means, but does not consolidate these rights into a single comprehensive and coherent article. Rather, the 1971 Paris text disperses the communication to the public right across a variety of dispositions, leaving several gaps both as to subject matter covered by the right, and as to the exclusive rights conferred. Despite those gaps, it is clear that the communication to the public right reaches acts both of initial and re-communication of works; article 11bis, for example, concerns third parties' free-to-air and wired retransmissions of broadcasts of protected works.[4] It is, arguably, less clear that the Berne Convention's right of communication to the public extended to individualized "pull" technologies, in addition to transmissions simultaneously communicated to the public ("push" technologies).[5]

[2] Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, amended Oct. 2, 1979, 828 U.N.T.S. 221 [hereinafter Berne Convention].

[3] Mihaly Ficsor, Horace S. Manges Lecture: Copyright for the Digital Era: The WIPO "Internet" Treaties, 21 Colum. J.L. & Arts 197, 209--211 (Spring 1997) (noting that the "making available" provision in the WIPO Copyright Treaty was meant in part to "clarif[y]" the concepts of distribution and communication to the public in the context of digital transmissions).

[4] See Berne Convention, supra note 2, art. 11bis(2)(ii): "any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one"

[5] See discussion in Sam Ricketson and Jane C. Ginsburg, International Copyright And Neighboring Rights: The Berne Convention And Beyond, ¶¶ 12.47-12.51 (2006) [hereafter Berne Book].

Article 8 of the WIPO Copyright Treaty (WCT) fills in the Berne Convention blanks with respect both to subject matter and scope of the communication to the public right.[6] All initial and subsequent transmissions of works of authorship to the public come within the scope of the exclusive right. Article 8 contributes further detail to the communication to the public right, by specifying that the right of communication to the public includes a right of "making available to the public of [literary and artistic] works in such a way that members of the public may access those works from a place and at a time individually chosen by them."[7] This right targets individualized on-demand ("pull") communications (by any technical means), for it makes clear that the members of the public may be separated both in space and in time.[8] The WCT does not define the "public" to whom the works are made available, but it states that the "public" is comprised of "members," and, thus implies that the "public" need not be populous, although the greater the numbers to whom a work is made available, the more apparent the conclusion that the making available was to "the public."[9] Certainly, simply offering the work on an undiscriminating basis, so that any member of the general public may access the work, should come within the scope of the right.[10] Even a more narrowly-defined class of intended recipients, such as the fans of a particular musician, or students of 20th-century photorealist painting, may appeal to an audience potentially too large for a "family circle" or similar exclusion.

It is not necessary that the offer be accepted: as the phrase "may access" establishes, "making available" embraces incipient as well as effected communications.[11] Similarly, because the right targets individualized transmissions, the relevant measure is not whether the number of *recipients* exceeds that of a family circle, but whether the number of *persons to whom access to the content is offered* exceeds that of a family circle. The work is "made available" even if only one member of that public, or indeed none, in fact demand the work's delivery.

---

[6] WIPO Copyright Treaty, art. 8, Dec. 20, 1996, 36 I.L.M. 65 (1997) [hereinafter WCT]. Similar solutions were adopted in the WIPO Performance and Phonograms Treaty, arts. 10 & 14, Dec. 20, 1996, 36 I.L.M. 76 (1997) [hereinafter WPPT].

[7] WCT, supra note 6, art. 8.

[8] Jorg Reinbothe & Silke Von Lewinski, The WIPO Treaties on Copyright: A Commentary On The WCT, The WPPT, And The BTAP ¶ 7.8.36, at 140 (2015) (noting that Art. 8 WCT "cover[s] all situations involving an individual time and place of access" including both "pull-technology, which requires the user to 'demand' that a work be transmitted to his terminal," and "push-technology, by which the works are 'pushed' to the email address of the user and may be accessed by him at this address at any time and from any place").

[9] Id. at ¶ 7.8.39 ("If works are made available in the framework of a social network, a chat group, or mailing list, the question of whether the works are made available 'to the public' depends on the characteristics of the groups of persons to whom the works are made available and on the definition of 'public' under the relevant national law . . . . In most cases, such groups will constitute a 'public' . . . [but] the electronic mailing of a work . . . to one particular person does not constitute making available 'to the public' . . . .").

[10] Id. at ¶ 7.8.39 ("Beyond doubt, the making available of works on a home page or any server that may even be accessed through broader networks, in particular over the internet, is an act of making available to the public.").

[11] Memorandum Prepared by the Chairman of the Committees of Experts, CRNR/DC/4, P 10.10 (August 30, 1996), in Records of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, at 204 (1999) [hereinafter WCT Basic Proposal I], ("The relevant act is the making available of the work by providing access to it. What counts is the initial act of making the work available, not the mere provision of server space, communication connections, or facilities for the carriage and routing of signals. It is irrelevant whether copies are available for the user or whether the work is simply made perceptible to, and thus usable by, the user."); Reinbothe & Von Lewinski, supra note 7, at 137 (noting that "the mere wording of Article 2, part 2 WCT" shows that the "act of making available to the public only needs to allow that members of the public 'may access' the work" and that, accordingly, "users do not necessarily need to access the work in order to trigger the making available right").

The technological means of "making available" are irrelevant; Unlike the Berne Convention articles differentiating wired and wireless transmissions, WCT article 8 is expressed in technologically neutral terms.[12] Moreover, member States may comply with the right either through local communication rights, or, for those countries who have applied the distribution right to temporary digital copies, through the right to distribute copies, as the United States urged during the drafting period.[13] In adopting what came to be known as the "umbrella solution," allowing Member States to implement the making available right through any domestic law exclusive right or combination of them, the drafters opted for an approach of juridical as well as technological neutrality.[14]

As an instance of the communication to the public right, the scope of the making available right's coverage of on-demand access encompasses both initial and secondary transmissions.[15] It thus covers both the provision of direct access and at least certain forms of indirect access to literary and artistic works. The extent to which the making available right reaches intermediated on-demand access to works, particularly via hyperlinks, requires examination. Consider the following scenarios: (1) a user enters the URL of a website in order to access works stored on the site. Here, the user directly contacts the initial source of the transmission of the requested content. In the second two scenarios, by contrast, the user contacts an intermediary who will direct her to a third-party source site from which the requested content will be transmitted. (2) A website aggregates links to other websites from which users can download unauthorized copies of recorded music. Some links are identified by the name of the music file; clicking on these links takes the user directly to another website and automatically downloads the named file from that third-party website to the user's hard drive. (3) Other links are identified by the names of the third-party websites; clicking on these sends the user to the named website, from which she

[12] See WCT Basic Proposal I, supra note 11, at 10.14 ("The technology used may be analog or digital, and it may be based on electromagnetic waves or guided optical beams. The use of the non-restrictive term 'any' in front of the word 'communication' in [Article 8], and in certain provisions of the Berne Convention, emphasizes the breadth of the act of communication.'"); Ficsor, supra note 3, at 210 (noting that the "making available" right is "described in a neutral way, free from specific legal characterization (for example, as making available a work to the public by wire or by wireless means, for access); [is not] technology-specific and, at the same time, [expresses] the interactive nature of digital transmissions."); Reinbothe & Von Lewinski, supra note 7, at 138 ("The technical means of making the work available are irrelevant.") (emphasis omitted).

[13] See WIPO, Records of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions (Geneva 1996) vol. II at 675, ¶ 301, available at ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_348e_v2.pdf [hereinafter 1996 Records] ("[The United States delegation] stressed the understanding . . . that [the new "making available" right] might be implemented in national legislation through application of any particular exclusive right, . . . as long as the acts described in those Articles were covered by such rights.").

[14] For extensive discussion of the "umbrella solution," by the coiner of the term, see Ficsor, supra note 3, at 204-09, 496-509. See also Reinbothe & Von Lewinski, supra note 7, at 102-03 & n. 15.

[15] Reinbothe & Von Lewinski, supra note 7, at 132--32 ("[A]ny new act of making available a work via the internet, for example through a separate upload or link on a second website to the one here the work was originally made available, or through a search engine, represents a new act of making available to the public.") (citations omitted); Association Littéraire et Artistique Internationale (ALAI), New Public Report and Opinion at 9 (Sept. 17, 2014) [hereinafter ALAI New Public Opinion], http://www.alai.org/en/assets/files/resolutions/2014-opinion-new-public.pdf ("Article 11bis(1)(ii) of the Berne Convention brings within the general scope of the communication to the public right secondary transmissions made by a different communication entity; the text may be said to support a requirement of a new communicator in the case of a new transmission of a prior broadcast.").

may navigate to and elect to download a variety of files. In (3), the linking site does not directly send digital files of the recorded music to users who access the linked-to site.

From the user's point of view, the experience of (1) and (2) to acquire the file is the same; either way, she contacts the first site and receives the file without the apparent further intervention of another website operator. In (3), the user knows she is being taken to another site, from which she may download files of recorded music. In all three scenarios, the websites on which the content is stored are making works available to the public; whether the members of the public enter the site's URL to gain access to the works directly from the source site, or whether the members of the public access the works on the source site through the intermediary of a link, either way the source site will be communicating the works to members of the public. But, in cases (2) and (3), is the first-accessed site, by providing a link that routes the user directly (2) or indirectly (3) to the content residing on the source site, also "making [the files] available" to the members of the public who, through the intermediary of the link, contact the source site? Does it matter whether the user knows that the file is coming from the site she contacted, or from some other site? Put another way, does it matter that in (2) the content appears to the user to be coming from the linking site, while in (3) it is apparent that the linked-to site is offering the content?

The text of the Article 8 (and Articles 10 and 14 of the WIPO Performances and Phonograms Treaty (WPPT)) "making available" right may supply an answer.[16] It gives authors the exclusive right of allowing members of the public to access literary and artistic works (and recorded performances) "from a place and at a time individually chosen by them." The "place" contemplated most likely refers to the physical place where the member of the public is located (for example, at home) when she requests the content. The text also implies that the "place" is one to which the content will be sent, and that "place" might be anywhere the member of the public and her receiving device (for example, a cell phone, notebook, or laptop computer) are located. But the text might also be read to refer to the networked "place," e.g., website, that the user contacts in order to gain access to the work.[17] Applying that interpretation, in scenario (3), the connection between accessing the first site and the communication of the work may be too attenuated, because the user knows that the site from which she is receiving the work is no longer the site she first contacted. The linked-to site becomes the place from which the user chooses to access the work, rather than the linking site. In scenario (2), by contrast, the place from which the user appears to be accessing the music is the site the user initially contacted, which is the only site she chose. Accordingly, though the ultimate source of the communication is not the linker's site, the linker will be making the work available to a user who has "chosen" to access the content from the linker's site.[18]

[16] The following analysis elaborates on an approach proposed in Berne Book, supra note 5 at ¶¶ 12.60-12.61.

[17] Nothing in the Records of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions, (WIPO 1996), indicates that the language "from a place and at a time individually chosen by them" received special attention, apart from general endorsement of its adaptability to digital communications. See 1996 Records, supra note 13.

[18] While this interpretation might suggest that the website from which the content is in fact (despite appearances) emanating is not "making [that content] available" to the user who obtains the content via a deep or in-line link, it will not matter to the source site's liability for "making available" that some content recipients are not aware of the source: so long as the source website can be contacted directly or via a simple link, it is still making content available to users in general.

Under this approach, then, the WCT "making available" right will reach certain, but not all, acts of secondary communication of content residing on third-party websites. Notably, this interpretation of the WCT views the act of making available from an economic perspective: the site from which the user chooses to access the content reaps the economic benefits of the user's choice, for example, by exposing her to that site's advertising, or simply by prolonging the user's visit to that website.[19] This interpretation of the WCT also comports with a functional view: the operation "feels" to the user as if she is receiving the content from the intermediary.[20]

PART II: EU LAW ON LIABILITY FOR HYPERLINKING

The European Union has incorporated the WCT making available right verbatim in article 3(2) of the 2001 Information Society Directive.[21] Article 3 covers the right of communication to the public. The Court of Justice of the European Union (CJEU) in *Svensson v. Retriever Sverige AB*, held hyperlinking to be a form of "making available," even though providing a link simply furnishes a means to access a work offered from a third-party site.[22] That the linker may be an intermediary, and that no communication will result unless the user clicks on the link, did not dissuade the court from holding links within the ambit of "making available": "[T]he provision, on a website, of clickable links to protected works published without any access restrictions on

[19] Some commentators have noted that the CJEU's interpretation of Directive 2001/29/EC (which implements the art. 8 WCT "making available" right in the EU) takes a similar "economic" approach, focusing not on "the legal monopoly of the authors," but on "whether the [defendant] *economically exploits* the copyright protected subject matter." Matthias Leistner, Europe's Copyright Law Decade: Recent Case Law of the European Court of Justice and Policy Perspectives, 51 Common Market L. R. 559, 570 (2014). Cf. Reinbothe & Von Lewinski, supra note 7, at 133 (noting that "[t]he right of making available to the public must be interpreted according to its purpose, [which is] to cover important acts of interactive exploitation on digital networks [of] the [copyright holder's] exclusive right" and that because the aim of the "making available" provision is "to grant the author the right to exploit his work by way of communication to the public," the right should not be limited to allow actors to design business models "conceived to avoid the application of these rights by using certain technical designs"); Mihaly Ficsor, The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation 205 (2002) ("[I]n those cases where digital delivery resulting in copies becomes a normal way of exploiting works and other productions, it will not be sufficient to grant owners of rights a simple right to remuneration . . . . In such a case, an exclusive right of authorization should be granted.').

[20] Some WCT signatories have declined to adopt this functional view, and have refused to impose direct liability on such intermediary actors who do not actually "store and serve" the content to the user. Perfect 10 v. Google, 416 F.Supp.2d 828, 843--45 (C.D. Cal. 2006). See also infra section III.A (discussing the "server rule" adopted in the U.S.). For example, in the U.S., a site which provides a hyperlink which, when clicked, causes the automatic download an infringing file from a third-party website cannot incur direct copyright liability, even if the user may not understand that the linking site is not actually providing the work. See id. However, the *travaux préparatoires* of the WCT indicate that the "relevant act is the making available of the work by *providing access to it*" and that technical processes like "the mere provision of server space" are less relevant that the "initial act of making the work available." WCT Basic Proposal I, supra note 11, at 10.10 (emphasis supplied). Therefore, these technically-based approaches to hyperlinking liability may not be wholly consistent with the policy behind the "making available" right. See infra section III.A.iii.c (discussing the tension between the "making available" right and the current state of U.S. law).

[21] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 [hereinafter Directive 2001/29].

[22] Case C-466/12, *Svensson v. Retriever Sverige AB* (13 Feb. 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.

another site, affords users of the first site direct access to those works. . . . [A] work is made available to a public in such a way that the persons forming that public may access it, irrespective of whether they avail themselves of that opportunity)."[23]

That said, the CJEU in fact curtailed the reach of the making available right with respect to hyperlinks by further holding that even though hyperlinks are a "communication to the public," when hyperlinks offer to recommunicate content already available on another website, the link, to be actionable, must either reach the public by a different technological means than the initial communication, or must reach a "new public" not contemplated by the rightholder in authorizing the initial communication.[24] Because the Court determined that all internet users constituted the same "public," at least when the originating site did not limit access to the content, the "new public" criterion as applied in *Svensson* effectively excluded links to unrestricted websites from the scope of the communication-to-the-public right. In a subsequent decision, *GS Media BV v. Sanoma Media Netherlands BV*,[25] involving the provision of links to an *unlawful* source, the Court imposed an additional, and subjective, criterion of knowledge of the illicit character of the targeted site. In both cases, copyright scholars have criticized the Court's reasoning,[26] notably because the "new public" criterion lacks legal basis in the international copyright treaties.[27] Nonetheless, the knowledge condition in particular, however debatable, avoided a potentially oppressive application of copyright to the great majority of internet users who are unaware that the sites to which they may be supplying links are illicit.

As a result of these decisions, it appeared that in the case of secondary communications, at least via hyperlinks, the Court of Justice, by imposing a knowledge criterion, was calling into question the nature of the communication to the public right (and therefore of copyright in general). After all, proof of a violation of a "true" property right does not require the rightholder to establish that

---

[23] Id. at ¶¶ 18-20:

> 18 In the circumstances of this case, it must be observed that the provision, on a website, of clickable links to protected works published without any access restrictions on another site, affords users of the first site direct access to those works.
>
> 19 As is apparent from Article 3(1) of Directive 2001/29, for there to be an 'act of communication', it is sufficient, in particular, that a work is made available to a public in such a way that the persons forming that public may access it, irrespective of whether they avail themselves of that opportunity (see, by analogy, Case C 306/05 SGAE [2006] ECR I 11519, paragraph 43).
>
> 20 It follows that, in circumstances such as those in the case in the main proceedings, the provision of clickable links to protected works must be considered to be 'making available' and, therefore, an 'act of communication', within the meaning of that provision.

[24] Id. at ¶ 24.

[25] Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016), http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.

[26] See, e.g., Pierre Sirinelli, Alexandra Bensamoun, Josée-Anne Benazeraf, *Le droit de communication au public*, Revue Internationale du droit d'auteur 207 (Jan. 2017); Mattias Leistner, *Closing the Book on Hyperlinks: A Brief Outline of the CJEU's Caselaw and Proposal for European Legislative Reform* 39 EIPR 327 (2017); P. B. Hugenholtz et S. C. van Velze, *Communication to a New Public? Three Reasons Why EU Copyright Law Can Do Without a 'New Public'*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811777 (19 July 2016); ALAI New Public Opinion, supra note 15; ALAI, Opinion of ALAI's Executive Committee on the Right of communication to the public; the Advocate General's Opinions in Filmspeler Case C-527/15 and Ziggo Case C-610/15 (Mar. 27, 2017), http://www.alai.org/en/assets/files/resolutions/170327-opinion-filmspeler-ziggo.pdf.

[27] See ALAI New Public Opinion, supra note 15.

the defendant knew that he was violating an exclusive right. The court's later decisions, however, suggest that the Court has gradually achieved a European harmonization of the law on derivative liability (i.e., liability in the second degree) for violation of the right of communication to the public by hyperlinking and other indirect means of providing access to protected works.[28] Moreover, harmonization at the EU level was necessary given both the lack of uniformity regarding secondary liability across the national laws of the member states,[29] and the growing economic importance of furnishing the means to access infringing sources (without serving as the initial source of the infringing communication).[30]

II.A. Harmonization of the law of communication to the public as applied to the facilitation of infringement by hyperlinking and other means

Both of the CJEU's later cases concerned facilitation of illicit communications to the public: in *Stichting Brein v Wullums (Filmspeler)*[31] though the sale of a device which connected to a television screen and which was supplied with hyperlinks pointing to illicit internet streaming sites, and in *Stichting Brein v. Ziggo*[32] through the services of The Pirate Bay (TPB), a P2P BitTorrent indexation site that enabled internet users to locate audiovisual works in the hard disks of other participants in the P2P network and to make unauthorized copies.[33] In both cases, the Court distinguished between an act of communication to the public and "[t]he mere provision

[28] Cf. Alain Strowel, Note on *Svensson*, A&M 2014/3-4 at 224, 232 (raising the question of a "complete harmonization of the right of communication to the public.").

[29] See the Conclusions of Advocate General Szpunar in Case C-610/15, *Stichting Brein v. Ziggo*, at ¶ 3:

> The European Commission, whose opinion appears to me to be shared by the United Kingdom of Great Britain and Northern Ireland, contends that liability for sites of this type is a matter of copyright application, which can be resolved not at the level of EU law but under the domestic legal systems of the Member States. Such an approach would, however, mean that liability, and ultimately the scope of the copyright holders' rights, would depend on the very divergent solutions adopted under the different national legal systems. That would undermine the objective of EU legislation in the relatively abundant field of copyright, which is precisely to harmonise the scope of the rights enjoyed by authors and other rightholders within the single market. That is why the answer to the problems raised in the present case must, in my view, be sought rather in EU law.

See also, Birgit Clark and Julia Dickenson, *Theseus and the Labyrinth? An Overview of "Communication to the Public" Under EU Copyright Law*, 39 EIPR 265, 277 (2017) (adverting to "real challenges of not having a common conception of secondary liability within the EU legal framework").

[30] See, e.g., Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM (2016) 593 final (14/09/2016), recitals 37-39. See also, *L'Oréal v. eBay*, C-324/09 (2011) (online auctions platform bringing together buyers and sellers of counterfeit perfumes); *Google France v. Vuitton*, C-236/08 à C-238/08 (2010) (AdWords, links to sites selling infringing imitations of Vuitton bags).

[31] Case C-527/15, *Stichting Brein v Jack Frederik Wullems* [Filmspeler] (Apr. 26, 2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523515.

[32] Case C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV* (June 14, 2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523658.

[33] *Ziggo* concerned a request under art. 8 of the InfoSoc Directive 2001/29 to direct an access provider to block access to The Pirate Bay website. Article 8, titled "Sanctions and remedies", provides, at ¶graph 3:

> Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

Ziggo, as an access provider, was an intermediary within the scope of art. 8, and its services were used by The Pirate Bay, but it was necessary to establish that TPB was violating the right of communication to the public.

of physical facilities for enabling or making a communication [which] does not in itself amount to communication within the meaning of this Directive."[34] In both cases, the decisions turned on the characterization of an act of communication, all subsequent elements of a secondary communication to the public having been established: that the communication was made to (1) a "public" composed of an indeterminate but fairly large number of recipients; (2) a "new public" not taken into account by the rightowner when it initially communicated the work to the public (defendants in both cases were facilitating access to infringing locations, thus the rightowner did not envision a "public" accessing the work from those locations) and (3) defendants' knowledge of the illicit character of the source of the communication (websites in *Filmspeler*; "sharing" files of the P2P network's participants in *Ziggo*).

The "new public" criterion as applied in *Svensson* protected all those who supplied links (of any kind, including framing links) to a site authorized by the copyright owner, whom the Court deemed to have taken all internet users into account at the time of the first unrestricted posting of the work to the site. But, as the Court recognized in *Filmspeler*, the notion of an accounted-for public makes no sense when the source toward which the links point is illicit.[35] Nonetheless, the risk of finding a vast number of internet users to be copyright infringers led the Court in *GS Media* to seek a "fair balance"[36] that enabled it to engraft onto the "new public" requirement an additional criterion of knowledge that the linked-to content was infringing. By contrast, in *Filmspeler* and *Ziggo*, by transposing the knowledge criterion to the first stage of the analysis, in order to determine whether, as a result of the "deliberate character of [its] intervention,"[37] the defendant had committed an act of communication in the first place, the Court achieved the balance sought in *GS Media*. Inquiry into defendant's deliberate intervention allowed the court to distinguish the unconscious acts of simple internet users, without requiring recourse to the increasingly complex concept of a "new public" in order to avoid undesirable consequences.

In *Filmspeler* the Court evoked the "essential role" of the person who effects an act of communication, together with that person's intentional intervention, in making a protected work accessible.[38] But "essential" does not mean "indispensable." In fact, even if the purchasers of the Filmspeler set top box could have obtained unauthorized access to the works by other means, the knowing facilitation of access sufficed for the commission of an act of communication (as opposed to the simple furnishing of the means to make a communication). The Court emphasized that the defendant had loaded his media player with links to illicit sites "with full

[34] Directive 2001/29, supra note 21, at Recital 27.

[35] See *Filmspeler*, Case C-527/15, at ¶ 48 ("However, the same finding cannot be deduced from those judgments failing such an authorisation.").

[36] See Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016) at ¶¶ 44--48, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.

[37] *Ziggo*, Case C-610/15, at ¶ 26.

[38] See *Filmspeler*, Case C-527/15 at ¶ 31:

> "Amongst those criteria, the Court has emphasised, above all, the essential role played by the user. The user makes an act of communication when he intervenes, in full knowledge of the consequences of his action, to give access to a protected work to his customers and does so, in particular, where, *in the absence of that intervention, his customers would not, in principle, be able to enjoy the broadcast work* (see, to that effect, judgments of 31 May 2016, Reha Training, C‑117/15, EU:C:2016:379, paragraph 46, and of 8 September 2016, GS Media, C‑160/15, EU:C:2016:644, paragraph 35 and the case-law cited)." (emphasis supplied).

knowledge of the consequences of his conduct."[39] Because the pre-installed links, once activated by the multimedia player's users, "offer its users direct access to protected works without the consent of the copyright holders," the Court ruled that supplying the device "must be regarded as an act of communication within the meaning of Article 3(1) of Directive 2001/29."[40]

As for the "new public" criterion, after citing its decision in *GS Media,*[41] the Court simply observed: "In the present case, it is common ground that the sale of the 'filmerspeler' multimedia player was made in full knowledge of the fact that the add-ons containing hyperlinks pre-installed on that player gave access to works published illegally on the internet."[42]

In *Ziggo,* the Court reinforced *Filmspeler*'s lesson: those who knowingly facilitate unauthorized access to protected works play an "essential role" in their communication, and therefore themselves commit an act of communication.[43] As in *Filmspeler,* the Court emphasized that

---

[39] See id. at ¶ 41:

> "In the same way, it must be held that the present case does not concern a situation of the 'mere' provision of physical facilities for enabling or making a communication. As the Advocate General noted in paragraphs 53 and 54 of his opinion, Mr. Wullems, *with full knowledge of the consequences of his conduct*, pre-installs onto the 'filmspeler' multimedia player that he markets add-ons that specifically enable purchasers to have access to protected works published — without the consent of the copyright holders of those works — on streaming websites and enable those purchasers to watch those works on their television screens (see, by analogy, judgment of 7 December 2006, SGAE, C‑306/05, EU:C:2006:764, ¶ 42). *That intervention enabling a direct link to be established between websites broadcasting counterfeit works and purchasers of the multimedia player, without which the purchasers would find it difficult to benefit from those protected works*, is quite different from the mere provision of physical facilities, referred to in recital 27 of Directive 2001/29. In that regard, it is clear from the observations presented to the Court that the streaming websites at issue in the main proceedings *are not readily identifiable by the public* and the majority of them change frequently." (Emphasis supplied)

[40] See id. at ¶ 42:

> "Consequently, it must be held that the provision of a multimedia player such as that at issue in the main proceedings enables, in view of the add-ons pre-installed on it, access via structured menus to links that those add-ons which, when activated by the remote control of that multimedia player, *offer its users direct access to protected works* without the consent of the copyright holders and must be regarded as an act of communication within the meaning of Article 3(1) of Directive 2001/29." (Emphasis supplied)

[41] See id. at ¶ 49.

[42] Id. at ¶ 50. In the same paragraph, the Court also observes that Filmspeler's conduct justified the presumption of knowledge which, per *GS Media,* flows from the lucrative character of the link: "As was noted in paragraph 18 above, the advertising of that multimedia player specifically stated that it made it possible, in particular, to watch on a television screen, freely and easily, audiovisual material available on the internet without the consent of the copyright holders." Id.

[43] See *Ziggo,* Case C-610/15, at ¶ 36--39:

> "[T]he fact remains that those operators, by making available and managing an online sharing platform such as that at issue in the main proceedings, intervene, *with full knowledge of the consequences of their conduct*, to provide access to protected works, by indexing on that platform torrent files which allow users of the platform to locate those works and to share them within the context of a peer-to-peer network. In this respect, as the Advocate General stated, in essence, in point 50 of his Opinion, without the aforementioned operators making such a platform available and managing it, the works *could not be shared by the users or, at the very least, sharing them on the internet would prove to be more complex*.
>
> "The view must therefore be taken that the operators of the online sharing platform TPB, by making that platform available and managing it, *provide their users with access to the works*

TPB's administrators "intervene, with full knowledge of the consequences of their conduct, to provide access to protected works." TPB's intervention consisted of "indexing on that platform torrent files which allow users of the platform to locate those works and to share them within the context of a peer-to-peer network." The index "classif[ies] the works under different categories, based on the type of the works, their genre or their popularity, within which the works made available are divided, with the platform's operators checking to ensure that a work has been placed in the appropriate category. In addition, those operators delete obsolete or faulty torrent files and actively filter some content." By classifying the works, TPB's administrators must have been aware that protected works were at issue, as the Court later pointed out.[44] Without that intervention, "the works could not be shared by the users or, at the very least, sharing them on the internet would prove to be more complex." Thus, to commit an act of communication, it suffices to facilitate an access that nonetheless could otherwise, albeit less easily, have been obtained.

As for the element of knowledge tied to the "new public" criterion, the Court reiterated the facts that led it to reject the characterization of TPB as a mere furnisher of means. In fact, TPB's administrators had been alerted that they were facilitating access to infringing content. Far from purging its index, TPB instead incited its users to make copies. Given that "a very large number of torrent files on the online sharing platform TPB relate to works published without the consent of the rightholders," TPB "could not be unaware" that its platform was providing access to infringing copies.[45] Curiously, although TPB was a profit-seeking venture, the Court, albeit

---

> *concerned. They can therefore be regarded as playing an essential role in making the works in question available*.
>
> "Finally, the operators of the online sharing platform TPB cannot be considered to be making a 'mere provision' of physical facilities for enabling or making a communication, within the meaning of recital 27 of Directive 2001/29. It is clear from the order for reference that that platform indexes torrent files *in such a way that the works to which the torrent files refer may be easily located and downloaded by the users* of that sharing platform. Moreover, it is clear from the observations submitted to the Court that, in addition to a search engine, the online sharing platform TPB offers an index classifying the works under different categories, based on the type of the works, their genre or their popularity, within which the works made available are divided, with the platform's operators checking to ensure that a work has been placed in the appropriate category. In addition, those operators delete obsolete or faulty torrent files and actively filter some content.
>
> In the light of the foregoing, the making available and management of an online sharing platform, such as that at issue in the main proceedings, must be considered to be an act of communication for the purposes of Article 3(1) of Directive 2001/29." (emphasis supplied)

[44] See id. at ¶ 45.

[45] See id.:

> "In the present case, it is apparent from the observations submitted to the Court, first, that the operators of the online sharing platform TPB were informed that this platform, which they make available to users and manage, provides access to works published without authorisation of the rightholders and, second, that the *same operators expressly display, on blogs and forums available on that platform, their purpose to make protected works available to the users, and encourage the latter to make copies of those works*. In any event, it is clear from the order for reference that the operators of the online sharing platform TPB *could not be unaware that this platform provides access to works published without the consent of the rightholders*, given that, as expressly highlighted by the referring court, a *very large number of torrent files on the online sharing platform TPB relate to works published without the consent of the rightholders*. In those circumstances, it must be held that there is communication to a 'new public' (see, to that effect,

generally observing that such a goal "is not irrelevant,"[46] did not apply the rebuttable presumption of knowledge announced in *GS Media*[47] and reiterated in *Filmspeler*[48] relative to those who furnish hyperlinks for profit-making purposes. Nonetheless, in *Ziggo*, because it was so clear that TPB was acting in full knowledge of the illicit nature of the communications that it was facilitating, there was no need to resort to a presumption.

The analyses of knowledge with respect to facilitation of the act of communication, and of knowledge respecting the "new public" criterion may differ to some extent. On the one hand, the facts that led to characterizing TPB as engaging in an act of communication (rather than simply supplying devices or services) indicated that TPB knew with specificity which works were at issue (or at least implied a level of knowledge allowing it to classify those works by category). On the other hand, in the context of the "new public" criterion, the Court stressed that TPB "could not have been unaware" of the infringing nature of the Torrent files; this statement appears to require only a general knowledge of the infringing activities of the P2P network's participants.

The level of specificity of knowledge required to determine whether one who facilitates an act of communication herself commits such an act is important. The higher the level of specificity, the harder it will be to prove that the intermediary, including a commercial actor, engages in an act of communication. Because the question of "who commits" a copyright-implicating act comes at the outset of the analysis, there will be no inquiry into the level of knowledge required for the assessment of whether the communication was made to a "new public" if the court finds the defendant not to have committed an act of communication in the first place. For example, it may be easier to prove that the facilitator of an infringing act generally knew that the site toward which it was directing internet users contained infringing content, than to show that the facilitator knew precisely what works users would find on the site. Moreover, a requirement of specific knowledge of particular infringements invites avoidance of liability through automation, so that only the "bot" and not the person who designed the bot would "know" to which works the facilitator enables access. The Court's statements in *Ziggo* regarding the level of knowledge are inconsistent, as we have seen. *Filmspeler*, however, supports the interpretation that a general knowledge of infringement will suffice, because the facts evoked by the Court concern the illicit character of the sites toward which the links directed the device's users, without stating that the supplier of the device knew specifically which films the linked-to sites offered.[49]

---

judgment of 26 April 2017, Stichting Brein, C‑527/15, EU:C:2017:300, ¶ 50)." (Emphasis supplied)

[46] Id. at ¶ 29.

[47] Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016) at ¶¶ 49--51, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.

[48] Case C-527/15, *Stichting Brein v Jack Frederik Wullems* [Filmspeler] (Apr. 26, 2017) at ¶ 49, http://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523515.

[49] See id. at ¶ 16 ("On that player, Mr Wullems installed an open source software, which makes it possible to play files through a user-friendly interface via structured menus, and integrated into it, without alteration, add-ons available on the internet, created by third parties, some of which specifically link to websites on which protected works are made available to internet users without the consent of the copyright holders.").

Ziggo did not concern hyperlinking but rather the furnishing of other means to access infringing copies of works. One may therefore conclude that the Court has generalized the analysis of who commits an act of communication beyond the context of hyperlinks in order to establish harmonized norms of liability for facilitation of infringement that result in the direct liability of the facilitator for violation of the right of communication to the public. In other words, the Court has practically harmonized the "very divergent solutions" to the doctrine of derivative liability adopted by different EU member states, now ensuring that the standard applicable to a claim of facilitation of infringement of the right of communication to the public will be the same across all EU member states.[50] Indeed, in the context of the facilitator of a violation of the right of communication to the public committed by the initial infringer, a requirement of knowledge can clarify the "role of the user" and thus allow the judge to determine when a facilitator should itself be held liable for its own act of communication to the public. It is the facilitator's "deliberate intervention"[51] for the purpose of making the infringing work more accessible to the public that renders the intermediary liable for an illicit communication. By contrast, when the facilitator has not taken an action "aimed directly at enabling purchasers to access copyright-protected works on the internet without the consent of right holders,"[52] it has not played a "decisive role" in the illicit communication. Hence the affirmation in Advocate General Szpunar's conclusions in *Ziggo* that "the decisive role in the communication to the public of a given work cannot be attributed to [the defendant] if it is unaware that the work has been made available illegally."[53] "Deliberate intervention" and "decisive role" imply an element of knowledge when liability for an act of communication to the public is based on a re-communication rather than on an initial illicit communication.[54]

One might object that this analysis appears to conflate a deliberate act with an intention to promote copyright infringement. An intermediary might knowingly decide to facilitate access to a work, or to a site containing works, without necessarily knowing that the access is illicit. Nonetheless, in the case of access training on a particular work, one can assume that if the work is a well-known film or recorded musical composition, the facilitator will be able to recognize the title and realize that it identifies a protected work whose availability on the target site was not authorized.[55] The same analysis pertains to a site containing many protected works. By contrast, it would be more difficult to infer bad intent when the work or the targeted site do not enjoy the same celebrity as the works at issue in *Filmspeler* and *Ziggo*.

In light of this caselaw, it is appropriate to synthesize the harmonized criteria that undergird a violation of the right of communication to the public. We will distinguish criteria applicable to any communication, initial as well as by retransmission or facilitation, from criteria applicable to retransmissions or facilitations of access to an initial communication.

---

[50] See the Conclusions of Advocate General Szpunar in *Ziggo*, Case C-610/15, at ¶ 3.
[51] *GS Media*, Case C-160/15, at ¶ 50; *Ziggo*, Case C-610/15, at ¶ 26.
[52] See the Conclusions of Advocate General Sánchez Bordona in *Filmspeler*, Case C-527/15, at ¶ 50.
[53] See the Conclusions of Advocate General Szpunar in *Ziggo*, Case C-610/15, at ¶ 51.
[54] The Court should in fact have been inquiring into whether three was a new *communication* (when it is made by one who did not make the initial communication), rather than whether there is a new *public*, see Berne Convention, supra note 2, art. 11*bis*; ALAI New Public Opinion, supra note 15.
[55] Cf. *EMI Christian Group v. MP3.com*, 844 F.3d 79, 93 (2nd Cir. 2016) (reasonable jury could find that sharing platform should have been aware that there were no authorized MP3 files either of recordings from major labels issued before 2007, or of any songs by the Beatles).

II.A.i. Criteria applicable to all communications to the public by making available

There must be an act of communication, including by making available (offering access to works): "it is sufficient, in particular, that a work is made available to a public in such a way that the persons forming that public may access it, irrespective of whether they avail themselves of that opportunity."[56]

That act of communication must be made to the public: "The concept of the 'public' refers to an indeterminate number of potential viewers and implies, moreover, a fairly large number of people."[57]

The commercial nature of the communication may be taken into account: "the profit-making nature of a communication, within the meaning of Article 3(1) of Directive 2001/29, is not irrelevant."[58] Indeed, one may assume that one who seeks economic benefit from an act of communication will not limit the intended recipients to a sole circle of family and social acquaintance.

II.A.ii. Criteria specific to the intermediaries who facilitate unauthorized access to works by hyperlinking or other means

The "essential," "decisive," or "deliberate" role of the intermediary,[59] "in full knowledge of the consequences of his action" – that is, knowing that it is facilitating infringement[60] – is what distinguishes the commission of an act of communication from the simple supplying of means. This role may be performed by one whose intervention makes works more easily accessible, even when members of the public might have obtained access by other means.[61]

II.A.iii. Is the "new public" still a relevant criterion*?*

When an intermediary, through the same means of communication (e.g., the internet), facilitates *access to a work from a legal source to which the public has unrestricted access*, application of the "new public" criterion will preclude the characterization of the intervention as an act of communication.[62]

[56] Case C-466/12, *Svensson v. Retriever Sverige AB* (13 Feb. 2014) at ¶ 19, http://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.
[57] Case C-527/15, *Stichting Brein v Jack Frederik Wullems* [Filmspeler] (Apr. 26, 2017) at ¶ 32, http://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523515.
[58] Id. at ¶ 34; Case C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV* (June 14, 2017) at ¶ 29, http://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523658.
[59] *Filmspeler,* Case C-527/15, at ¶ 49; *Ziggo,* Case C-610/15, at ¶ 26.
[60] *Filmspeler,* Case C-527/15, at ¶ 31; *Ziggo,* Case C-610/15, at ¶¶ 26, 34.
[61] *Filmspeler,* Case C-527/15, at ¶ 41; *Ziggo,* Case C-610/15, at ¶ 36.
[62] *Svensson,* Case C-466/12, at ¶¶ 24--28.

By contrast, this criterion does not apply if the intermediary employs a different technical means of communication,[63] even if the initial source of the communication is lawful.[64]

The application of the "new public" criterion in *Svensson* assumes that the source to which access is facilitated is legal[65] or that the intermediary is not circumventing an access restriction applied by the source website.[66]

The illegality of the source does not, however, necessarily result in rejecting the "new public" criterion, but instead adds to that criterion a further consideration: the intermediary's knowledge of the illegality of the source.[67] This knowledge is presumed when the intermediary acts with a profit motive.[68]

But in order for the person who facilitates access to a communication initially emanating from an illegal source to be considered to have committed an act of communication (rather than a simple furnishing of means) in his own right, he must have acted "in full knowledge of the consequences of his action."[69] But knowledge of the illicit activity that characterizes the "new public" under *GS Media* will already have been taken into account at the first stage of the analysis, according to *Filmspeler* and *Ziggo*. Hence the doubts about the pertinence of the "new public" criterion in the case of intermediaries who furnish unauthorized access to works.

II.B. Comparison with international norms

If the "new public" criterion is receding into redundancy or irrelevance, the tension between EU caselaw and the international norms of the Berne Convention and WIPO Copyright Treaties should diminish as well. The treaties supply no basis for the criterion; the closest text is Berne art. 11bis(2)(ii) which addresses secondary transmissions of broadcasts "made by an organization other than the original one."[70] In other words, the "new" entity is not the receiving public, but

[63] Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016) at ¶ 37, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.
[64] Case C-607/11, *ITV Broadcasting Ltd v. TVCatchUp Ltd* (7 Mar. 2013) at ¶ 39, http://curia.europa.eu/juris/liste.jsf?num=C-607/11&language=EN.
[65] *GS Media, C*-160/15, at ¶ 43.
[66] Id. at ¶ 50.
[67] Id. at ¶ 44-49.
[68] Id. at ¶ 51. Also see *Filmspeler,* Case C-527/15, at ¶¶ 49 & 51. Recently, German courts have declined to extend this rebuttable presumption to search engines, even though they presumably provide links with a profit motive. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] Sept. 21, 2017, I ZR 11/16; LG Hamburg [Regional Court of Hamburg], June 1, 2017, 308 O 151/17. This approach, which creates considerable tension with the authoritative language in *GS Media*, will be welcomed by some commentators who have argued that the presumption of knowledge should be "cautiously adapted for different key internet actors, such as search engines (which as a service aggregating massive amounts of content in an automated way would only have to show minimal general precautions to rebut the assumption), different aggregators (which would also only have to show minimal reasonable precautions to rebut the assumption), or persons posting individual links (which might be subject to more intensive duties of care . . .)." See Dr. Matthias Leistner, Closing the Book on the Hyperlinks: A Brief Outline of the CJEU's Case Law and Proposal for European Legislative Reform, 39 European Intellectual Property Review 327, 331 (2017).
[69] *Filmspeler,* Case C-527/15 at ¶ 31.
[70] Berne Convention, supra note 2, at art. 11*bis*(2)(ii).

the person engaging in the subsequent transmission. Once it is clear that the treaty contemplates not a different public, but a different provider of the communication, it should be apparent that providers of hyperlinks that render works (or more precisely, broadcasts of works) accessible to members of the public come within the scope of the right of communication to the public.

The CJEU's other innovations in defining a communication to the public by "making available" warrant comparison with our analysis of hyperlinking under WCT article 8. We have suggested that the supplier of a hyperlink may be making a work available for individualized access if the link communicates the work directly to the user, rather than taking the user to another site from which the user may navigate her way to the work.[71] In other words, deep links and framing links will make works available, while simple links will not (simple links make available the *site* from which the work is offered). Deep and framing links come within the making available right because the sites on which these links are found are the sites from which the user chooses to access the work; because the user will not experience the access as emanating from a third-party site, she cannot have chosen to request a communication of the work from an unknown location. The CJEU has declined to distinguish simple links from deep and framing links,[72] but its requirement that the linker play an "essential," "decisive," or "deliberate" role in making the work available, "in full knowledge of the consequences of his action" may in practice extend only to those linkers whose intervention delivers the work directly to the user. Our proposed WCT analysis has focused on the choice of the user, while the CJEU approach examines the conduct of the linker, but the two inquiries can be reconciled: the linker's "deliberate intervention" to enhance individual access to the works makes it possible for the user to choose to access the work from the linker's site. Without a given linker's offer of access to the work, a user seeking to stream or download that content would choose another provider's "place" from which to access the work.

It is now appropriate to consider the relationship between the harmonized European law of the liability of facilitators of access to illicit works or sources, and the harmonized European law of the *non*-liability of facilitators of unauthorized access established by the EU eCommerce Directive 2000/31.[73]

II.C. *Filmspeler* and *Ziggo*: The flip side of the coin of art. 14 of the eCommerce Directive?

While the European law of liability for facilitation of infringement by enabling access to third-party infringing communications was not harmonized before *Filmspeler* and *Ziggo*, the same is not true of the criteria for *non*-liability of certain intermediaries who facilitate access to third-party infringements. Article 14 of the eCommerce Directive 2000/31 provides a safe harbor from

[71] See supra note 18 and accompanying text.
[72] See Case C-348/13, BestWater Int'l GmBH v. Michael Mebes (21 Oct. 2014), http://curia.europa.eu/juris/liste.jsf?num=C-348/13.
[73] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 17/07/2000 P. 0001 – 0016 [hereinafter Directive 2000/31]. For a different view of the relationship between the CJEU's recent caselaw and the eCommerce Directive, see Eleonora Rosati, THE CJEU Pirate Bay judgment and its impact on the liability of online platforms, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006591 (forthcoming EIPR 2017)

liability for certain "information society services."[74] When the intermediary provides a service "that consists of the storage of information provided by a recipient of the service . . . the service provider is not liable for the information stored at the request of a recipient of the service" provided that:

> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent. . . [75]

As a threshold matter, it is not immediately clear that providers of hyperlinks qualify in the first place for the art. 14 non-liability provision. While some search engine activities (specifically, advertising services provided by search engine companies[76]) might qualify under art. 14, it does not follow that the provision of links by either a search engine or an individual actor corresponds to the criteria of art. 14.[77] Providers of hyperlinks do not necessarily "stor[e] information provided by a *recipient* of the service." Rather, in many hyperlinking contexts, the hyperlinks at issue will have been provided by the operator of the website (for example, search engines will themselves find and index links to websites on the internet, or a blogger might provide a link to another website when curating the content on her website).

EU member state authorities and commentators appear to agree that the safe harbor provisions of the eCommerce Directive do not cover information location tools like search engines or hyperlinks, but that EU member states are free to create additional safe harbors through national

[74] Directive 2000/31, supra note 73, at art. 14.

[75] Id. These conditions of non-liability do not include an obligation "actively" to seek out infringing content. On the contrary, according to art. 15, "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

[76] In *Google France v. Louis Vuitton*, the CJEU applied the art. 14 immunity provision to Google's AdWords product, which allows advertisers to display their advertisements in a "sponsored links" section of Google's search results when internet users search for particular keywords. See Joined Cases C-236/08 to C-238/08, *Google France SARL v. Louis Vuitton Malletier SA* (Mar. 23, 2010), http://curia.europa.eu/juris/document/document.jsf?docid=83961&doclang=en. The CJEU ultimately held Google to be within the scope of non-liability provision of art. 14, but this decision rested in part on the observation that Google stored not only links, but "the keywords selected by the advertiser" and "the accompanying commercial message" that allegedly infringed the plaintiff's trademarks. Id. at ¶ 111. Although Google may have suggested the keywords its customers selected, formally at least, the keyword links were "provided by a recipient of the service" and thus qualified under the language of art. 14 of the eCommerce Directive. Google's search engine (in contrast to its advertising service) may in fact involve the storage of much *less* --- a search engine need only store a link to an indexed webpage, and such a link may not be "provided by a recipient of the service," but instead created through Google's web crawler technology. Similarly, the provider of an individual link by an actor who is not a search engine may not store anything other than a simple URL address, which the website creator (rather than a "recipient of the service") provided.

[77] The German Federal Supreme Court has noted, in dicta, that a search engine may be liable for copyright infringement only once it had obtained knowledge of the unlawful nature of the data it had stored and then did not act expeditiously to remove or to disable access to that data --- mirroring the language of the eCommerce Directive. See *Vorschaubilder I* [Google Image Search], Bundesgerichtshof [German Federal Supreme Court], Case I ZE 69/08 [2010] GRUR 628. Also see Birgit Clark, Google Image Search Does Not Infringe Copyright, says Bundesgerichtshof, 5 J. Intell. Prop. L & Practice 553 (2010) (noting that this decision implies that search engines could claim safe harbor under the eCommerce Directive).

law for search engines or hyperlink providers.[78] While the parallel safe harbor legislation in the United States (the DMCA, which was passed two years before the passage of the eCommerce directive[79]) does provide a specific safe harbor for "information location tools," the eCommerce Directive neglects to provide such a safe harbor.[80] The eCommerce Directive does, however, require the submission of a report to "analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services."[81]

Once past the question whether the eCommerce Directive applies at all to linking activities, one will recognize a certain parallelism between the conditions for a violation of the right of communication to the public by facilitation, and those of the non-liability of service providers covered by the eCommerce Directive. In both cases, the lack of knowledge of the illicit activity excludes liability. But the Directive sets out only the conditions of *non*-liability; it was up to the EU member States to draw the negative inference, and to decide whether (or not) effective knowledge resulted in the liability of those who facilitate access to infringing content. The CJEU has now filled this gap by taking on the task of assessing the liability of facilitators, not only for "information society services" covered by the Directive, but also for any internet intermediary.

By putting the facilitator's knowledge up front in the analysis, the Court has procedurally anticipated the criteria of the eCommerce Directive, but has also extended them to intermediaries who do not qualify to invoke the Directive. For example, Filmspeler would not be an "information society service" because it was selling physical devices (set top boxes). And even if it could have been considered a service provider, the links it loaded onto the media player were not "information stored at the request of a recipient of the service," that is, by Filmspeler's customers, but were furnished by the service itself. Nonetheless, its liability will depend on the assessment of its level of knowledge, just as its non-liability would have depended on the same

[78] First Report on the Application of the eCommerce Directive at 13 (Nov. 21, 2003), http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2003/0702/COM_COM(2003)0702_EN.pdf [hereinafter First Report] ("Whilst it was not considered necessary to cover hyperlinks and search engines in the Directive, the Commission has encouraged Member States to further develop legal security for internet intermediaries."); Id. at 13 n.69 (noting that Spain and Portugal have "opted for the model of Article 14 ["hosting" safe harbor] both for search engines and hyperlinks" and that Austria and Lichtenstein have "opted for the model of Article 12 ["mere conduit" safe harbor] for search engines and of Article 14 ["hosting" safe harbor] for hyperlinks"). For example, the Austrian E-Commerce Act provides safe harbor for "[a] service provider which provides users with a search engine or other electronic aids to search for third-party information" and "[a] service provider which provides access to third-party information by means of an electronic link." See Federal Act Governing Certain Legal Aspects of Electronic Commercial and Legal Transactions (E-Commerce Act – ECG), Jan. 1 2002, https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2001_1_152/ERV_2001_1_152.pdf. See also First Report, supra, at 88 for an overview of the additional safe harbor regimes applicable to search engines or linkers implemented in Austria, Hungary, Spain, and Portugal. French courts appear to have achieved a similar result, see SAIF v Google, Cour d'appel [CA] [Court of Appeals] Paris, civ., Jan. 26, 2011, 08/13423, http://juriscom.net/wp-content/documents/caparis20110126.pdf (holding Google Image Search to be a mere neutral provider of tools – links --- employed by users, and holding that the mere fact that Google was "aware that [its] automatic indexing is likely to infringe on copyrighted works is not sufficient to engage its liability insofar as the services are ready to de-index upon notification").

[79] Online Copyright Infringement Liability Limitation Act (OCILLA), 17 U.S.C. § 512(d).

[80] See First Report, supra note 78, at 13 (noting that coverage of hyperlinks and search engines "was not considered necessary" when drafting the eCommerce Directive).

[81] Directive 2000/31, supra note 73, art. 21(2).

assessment if it had qualified for the immunity established by the eCommerce Directive. Similarly, the liability of a hyperlink provider, who does not "stor[e]" "information . . . at the request of a recipient of [its] service" and thus may be ineligible for the art. 14 safe harbor, may depend on the same assessment of the provider's level of knowledge.

There is one difference in the analyses regarding the placement of the burden of proof. Because art. 14 of the eCommerce Directive limits the service provider's liability, the beneficiary of the limitation should bear the burden of proving compliance with its conditions. By contrast, when the question of knowledge becomes part of the case in chief, the rightholder bears the burden of establishing every element of the claim, including that the defendant acted with knowledge that it was facilitating infringement. That said, the rebuttable presumption that the Court imposed on commercial actors in the context of the "new public" analysis in *GS Media* could also apply to the analysis of the deliberate intervention of the intermediary in the commission of an act of communication. In that case, profit-seeking defendants will be required to prove their lack of knowledge. As a result, commercial actors will receive the same treatment under the analysis of liability for facilitation of infringing communications as under the analysis of non-liability of "information society services" covered by the eCommerce Directive.

Given the debate in the EU over whether art. 14 of the eCommerce Directive has resulted in a "value gap" that allows service providers, such as YouTube, to benefit from the commercial value of works of authorship without paying the rightholders,[82] one might inquire whether the effective transposition of the non-liability criteria from art. 14 to the analysis of the reach of the right of communication to the public under art. 3 of the InfoSoc Directive will further weaken that right. But basing the liability of facilitators of infringement on the concept of knowledge derived from art. 14 could in fact increase the predictability of the analysis of that liability. Indeed, looking at the facts in *Filmspele*r and *Ziggo* in the light of art. 14 and the CJEU's caselaw interpreting the eCommerce directive, notably in *Google France v. Vuitton*, C‑236/08 and C‑238/08 (2008), and *L'Oréal v. eBay*, C‑324/09 (2011), the same results would obtain, but with additional elements available to evaluate the defendants' knowledge.[83]

Google France and *L'Oréal* were trademark infringement cases involving in the first case the AdWords service, and in the second an online auction platform. Because the eCommerce Directive is transversal, the CJEU's caselaw illuminates (non) liability for copyright infringement as well. In both cases, the courts assessed whether the service played "an active role of such a kind as to give it knowledge of, or control over, the data stored."[84] The notion of "an active role" resembles the "deliberate intervention" that characterizes the commission of an

[82] See, e.g., Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM (2016) 593 final (14/09/2016), recitals 37-39; ALAI Resolution on the European proposals of 14 September 2016 to introduce fairer sharing of the value when works and other protected material are made available by electronic means (Feb. 18, 2017), http://www.alai.org/en/assets/files/resolutions/170218-value-gap-en.pdf.

[83] See Joined Cases C-236/08 to C-238/08, *Google France SARL v. Louis Vuitton Malletier SA* [Google France] (Mar. 23, 2010), http://curia.europa.eu/juris/document/document.jsf?docid=83961&doclang=en; Case C-324/09, *L'Oréal SA v. eBay International* (July 12, 2011), http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=565137.

[84] *Google France*, at ¶ 120; *L'Oréal,* at 113.

act of communication by facilitation. By contrast, "if the role played by that service is neutral, in the sense that its conduct is merely technical, automatic and passive," that neutrality indicates "a lack of knowledge or control of the data which it stores."[85] In applying these considerations to *Ziggo* and *Filmspeler*, it becomes clear that the contributions of these actors were far from "neutral." For example, the Court pointed out that the administrators of the Pirate Bay "expressly display, on blogs and forums available on that platform, their purpose to make protected works available to the users, and encourage the latter to make copies of those works."[86]

The neutrality required by the eCommerce Directive art. 14 caselaw resembles the notion of "making a mere provision of physical facilities for enabling or making a communication" that characterizes an act that will not be considered an act of communication under the caselaw on liability for facilitation of infringement of the right of communication to the public. Thus, in *Filmspeler*, the Court detailed the acts of the defendant that constituted "communications." The device allowed "a direct link to be established between websites broadcasting counterfeit works and purchasers of the multimedia player, without which the purchasers would find it difficult to benefit from those protected works, [this] is quite different from the mere provision of physical facilities."[87] In other words, Filmspeler "optimized" access to infringing content; that optimization, like the promotion of unlawful access, is an act whose lack of neutrality the Court emphasized in its eCommerce Directive caselaw.[88]

One should also recall that, according to art. 14, the knowledge that precludes immunity from liability is not only specific knowledge of the unlawful activity, but also "knowledge of facts or circumstances from which the infringing activity or information is apparent." The latter type of knowledge appears to correspond to the knowledge attributed to the administrators of The Pirate Bay: given that "a very large number of torrent files on the online sharing platform TPB relate to works published without the consent of the rightholders," they "could not be unaware"[89] that the files were infringing.

One might object that the symmetry between liability for facilitation of illicit communications and the Court's interpretation of the art. 14 eCommerce Directive criteria is imperfect because the former presumes the knowledge of commercial actors, while no similar presumptions accompany art. 14. Once might buttress the objection with the observation that one of the

[85] *Google France*, at ¶ 114.

[86] Case C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV* (June 14, 2017) at ¶ 45, http://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523658. The administrators had also "indexe[d] torrent files in such a way that the works to which the torrent files refer may be easily located and downloaded by the users of that sharing platform" with the goal of aiding users to find the files. Id. point 38. Cf. L'Oréal point 116: "Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31."

[87] Case C-527/15, *Stichting Brein v Jack Frederik Wullems* [Filmspeler] (Apr. 26, 2017) at ¶ 41, http://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523515..

[88] See *L'Oréal*, at ¶ 116, supra.

[89] *Ziggo*, Case C-610/15, at ¶ 45.

objectives of the eCommerce Directive was to protect "information society services" from liability for their users' unlawful acts, even though many of those services operate for profit.[90] But the critique is ill-founded. It overlooks the role of a rebuttable presumption of knowledge, which reverses the burden of proof and requires the commercial defendant to prove that it acted without knowledge of ensuing infringements. Moreover, because art. 14 derogates from the liability the services could otherwise incur, the services should bear the burden of conforming their conduct to the prerequisites for qualifying for the liability limitation. To the extent there is a disparity in treatment between the showing of an infringement case-in-chief, and the showing required to claim the immunity from liability, it favors non-commercial actors, for to establish their liability for infringement of the right of communication to the public, the rightholder will need to prove their knowledge of the illicit character of the source to which they facilitate access. By contrast, had art. 14 applied, the service, whether or not for-profit, would have to prove its lack of knowledge. Because art. 14 limits providers' liability,[91] its analysis comes after the prima facie case. If at the outset the absence of a presumption of knowledge would lead a court to decline to rule that a non-commercial defendant violated the right of communication to the public, then the court will never get to the question of whether the defendant satisfied the criteria for application of the eCommerce Directive's criteria.[92]

PART III: US LAW ON LIABILITY FOR HYPERLINKING

III.A. Direct Liability for Hyperlinking in the United States

III.A.i: Statutory basis for copyright coverage of hyperlinks

The author's exclusive rights under the US Copyright Act expressly include neither a "making available" right, nor a right of "communication to the public." The closest statutory analog to those rights in the context of hyperlinking is the right to display or perform a work publicly by transmission or other means of communication under Section 106 of the U.S. Copyright Act.[93] Section 101 of that act defines "[t]o perform or display a work 'publicly'" as "to transmit or otherwise communicate a performance or display of the work . . . to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."[94] The definition section also specifies that "[t]o 'transmit' a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent."[95] The statutory language is technologically neutral, on its face

[90] See, e.g., Directive 2000/31, supra note 73, at recital 2.
[91] Although art. 14 eCommerce Directive states that "the service provider is not liable for the information stored at the request of a recipient of the service," the service provider remains subject to injunctive relief under art. 8.3 Directive 2001/29, which provides that rightholders may obtain an "injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."
[92] We will consider the compatibility with international norms of the eCommerce Directive's liability limitations for service providers after we address the parallel regime in the US under section 512 of the Copyright Act, infra.
[93] 17 U.S.C. § 106.
[94] Id. § 101. Section 101 also defines the term "to transmit" as "to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent." Id.
[95] Id.

encompassing all means of direct and secondary communications of performances or displays of works. U.S. case law on hyperlinking, however, has introduced a limiting gloss.

III.A.ii: The Server Rule and *Perfect 10 v. Amazon*

In the U.S., a judge-made doctrine known as the "server test" or "server rule"[96] governs the treatment of hyperlinks under the Copyright Act. The Court of Appeals for the Ninth Circuit adopted the test in a 2007 case, *Perfect 10 v. Amazon*, and U.S. courts since then have almost unanimously followed it.[97] Under the "server rule," "the owner of a computer that does not store and serve . . . electronic information to a user is not displaying [or distributing] that information, even if such owner in-line links to or frames the electronic information."[98] Therefore, a defendant who provides a hyperlink of any kind (through simple linking, deep linking, framing, or in-line linking[99]) cannot incur direct copyright liability unless that defendant also "store[s] and serve[s]" the copyrighted material to which the link points.

In *Perfect 10 v. Amazon*, a copyright holder sued Google for copyright infringement, alleging that Google infringed its copyrighted images by (i) storing "thumbnail" copies of those images on Google servers, which were then presented to Google Image Search users in a list of search results, and (ii) presenting Google Image Search users with full-size versions of the images when those users clicked on a thumbnail image presented in the search results.[100] Google conceded that it had created and displayed the "thumbnail" copies of the images in question, and argued (successfully) that the creation of thumbnail images to enable users to easily search for images constituted fair use.[101] However, as the lower court noted, there was a fundamental distinction between the presentation of Google's "thumbnail" image copies (which were actually stored on Google servers) and the presentation of the full-sized images, which were *not* stored on Google servers but were instead served up to users through "framed" or "in-line" links which directed

[96] Perfect 10 v. Amazon, 508 F.3d 1146, 1159 (9th Cir. 2007).

[97] See id.; MyPlayCity Inc. v. Conduit Ltd., No. 10 Civ. 1615(CM), 2012 WL 1107648, at *12--14 (S.D.N.Y. Mar. 30, 2012) (holding that "merely providing a 'link' to a site containing copyrighted material does not constitute direct infringement of the holder's distribution right"). Only one available case has directly conflicted with the "server test" since the Ninth Circuit's opinion in *Perfect 10 v. Amazon*. See Live Nation Motor Sports, Inc. v. Davis, No. 3:06-CV-276-L, 2007 WL 79311 (N.D. Tex. 2007) (holding that a defendant may have infringed the plaintiff's copyright by framing media available on the plaintiff's website).

[98] Perfect 10 v. Google, 416 F.Supp.2d 828, 843--45 (C.D. Cal. 2006).

[99] The terms "in-line linking" and "framing" are conceptually very similar. Generally, "in-line linking" or "embedded linking" refers to the process of importing a piece of content from another website through a hyperlink. "Framing" is a more specific term that refers to the combination of materials from different sources on a single website through in-line hyperlinks, but may refer specifically to uses in which the imported content is presented independently through a "gateway" or "independently scrollable frame[]." See Mark Sableman, Link Law Revisited: Internet Linking Law at Five Years, 16 Berkeley Tech. L.J. 1273, 1297--1299 (2001). For clarity, this piece will use the term "in-line linking" to refer to both practices.

[100] Perfect 10, 508 F.3d at 1155--56.

[101] Id. at 1165 (noting that while "an image may have been created originally to serve an entertainment, aesthetic, or informative function, a search engine transforms the image into a pointer directing a user to a source of information" and thus "provides an entirely new use for the original work" which constitutes permissible fair use under 17 U.S.C. § 107).

the users' browsers to the server on which the images originally appeared, albeit while in-lining the destination site with information from the linking site .[102]

The lower court had adopted an interpretation of the Copyright Act under which Google would be found directly liable only for displaying and distributing the images it stored on its own servers, based on the "server test" whose adoption Google urged.[103] On appeal, Perfect 10 countered by pointing out that "[f]rom a user's perspective, viewing material within a 'frame' while on *google.com* is no different from viewing material stored on Google's own server."[104] The Ninth Circuit rejected Perfect 10's position and endorsed the lower court's logic. The Ninth Circuit contended that a link is, essentially "HTML instructions [constituting mere] lines of text," and that "[p]roviding these HTML instructions is not equivalent to showing a copy."[105] According to the court, "it is the [source] website publisher's computer that distributes [and displays] copies of the images by transmitting the photographic image electronically to the user's computer," and Google's HTML instructions "do not themselves cause infringing images to appear on the user's computer screen."[106]

Perfect 10 essentially precluded the argument that, under U.S. law, the provision of a link could constitute an act of direct infringement, even if a website's act of linking is done in a way that might "cause some computer users to believe they are viewing a single . . . webpage" rather than a link to a source website.[107] Since 2007, U.S. courts have held that the "server test" bars any finding of direct copyright liability for simple linking,[108] deep linking[109] or in-line linking.[110]

---

[102] Id. at 1161 (noting that when displaying the full-sized images, Google simply "provides HTML instructions that direct a user's browser to a website publisher's computer that stores the full-size photographic image").

[103] Perfect 10 v. Google, 416 F.Supp.2d 828, 843--45 (C.D. Cal. 2006). The lower court's adoption of the "server test" was based partially on an analysis of relevant precedent which implied that direct infringement in the internet context required that the defendant "use its hardware to either store the infringing images or move them from one location to another for display." See id. at 840--43 (quoting Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1168--69 (C.D.Cal. 2002)). The lower court also relied on other cases holding that hyperlinking does not necessarily constitute direct infringement of the reproduction or distribution rights. See Perfect 10 v. Google, 416 F.Supp.2d at 842 (citing Ticketmaster Corp. v. Tickets.com, Inc. No. CV 99-7643, 2000 WL 525390, at *2 (C.D. Cal. Mar. 27 2000), which held that "hyperlinking per se does not constitute direct copyright infringement because there is no copying," and Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918, at *4 (S.D.N.Y. Aug. 29, 2002), which held that linking to content does not implicate the distribution right)).

[104] Appellant Perfect 10, Inc. Third Brief on Cross-Appeal, Perfect 10 v. Google, 508 F.3d 1146 (9th Cir. 2007), 2006 WL 3023532 at section I.C (Aug. 22, 2006).

[105] Perfect 10 v. Amazon, 508 F.3d 1146, 1161 (9th Cir. 2007).

[106] Id. at 1161--62.

[107] Id. See also United States Copyright Office, Report on The Making Available Right in the United States 49 (February 2017) ("The Ninth Circuit's reasoning in Perfect 10 has been relied on to bar direct infringement claims for instances of inline linking and framing.").

[108] See, e.g., Pearson Educ., Inc. v. Ishayev, 963 F.Supp.2d 239, 250--51 (S.D.N.Y. 2013) (holding that a defendant who provided a link to its customers to a file sharing site which allowed for the download of an infringing copy of plaintiff's work did not commit an act of direct infringement, noting that "sending an email containing a hyperlink to a site facilitating the sale of a copyrighted work does not itself constitute copyright infringement").

[109] See, e.g., Ticketmaster Corp. v. Tickets.com Inc., No. CV 99–7654 HLH(BQRX), 2000 WL 525390, at *2 (C.D. Cal., Mar. 27, 2000) (noting that the defendant's deep linking to event pages on the Ticketmaster website did not constitute infringement because "hyperlinking does not itself involve a violation of the Copyright Act . . . since no copying is involved" and because "[t]he customer is automatically transferred to the particular genuine web page of the original author. . . [t]his is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently.").

U.S. courts instead characterize the provision of hyperlinks of any form as the *facilitation* of a user's access to infringing works, which "raises only [secondary] liability issues."[111]

III.A.iii: Analysis of the Server Rule

III.A.iii.a: The server rule, statutory authority and misplaced metaphors

The natural implication of the "server rule" is that the mere provision of a hyperlink of any kind cannot constitute an act of public performance or display and therefore cannot constitute a direct violation of the exclusive rights reserved to copyright holders under Section 106 of the U.S. Copyright Act.[112] Thus, despite the breadth and technological neutrality of those rights, the server rule effectively assumes that a hyperlink is not a "device or process" that "transmit[s] or otherwise communicate[s] a performance or display of a work . . . to the public."[113] This logic relies on a restrictive definition of "transmit or otherwise communicate," which it reads to include only those "device[s] or process[es]" which "cause infringing images to appear on the user's screen," by pushing data from the server on which the work is stored to the user's browser.[114] The statutory definition of "to transmit," however, is not so constrained. The statutory language includes within the definition of "transmit" "*any* . . . *process* . . . whereby images or sounds *are received* beyond the place from which they are sent."[115] The legislative history indicates that Congress intended to broaden the definition of public performances and displays to cover "not only the initial rendition or showing, but also any further act by which that rendition or showing is transmitted or communicated to the public.[116] The "process whereby images . . . are received" on a user's screen certainly includes the hyperlinks and HTML code which cause that image to appear. Even under a strictly technical approach, the process through which a user's browser displays a webpage begins not when the host server sends data to the user's browser, but when the clicked hyperlink instructs the user's browser to retrieve the data from the source server and provides the browser with the relevant URL address. As the Ninth Circuit explained: the hyperlink "gives the address of the image to the user's browser . . . [t]he browser then interacts with the [server which] causes an . . . image to appear on the user's computer screen."[117] The fundamental assumption underlying the server rule is that the first part of this process, which enables the browser to connect with the right server, is not part of the "process" at all.

By contrast, the inclusion of a catch-all category in the statutory definition ("transmit or *otherwise communicate*") indicates that the definition should be read broadly, not narrowly. The

---

[110] See, e.g., Perfect 10 v. Amazon, 508 F.3d 1146, 1159 (9th Cir. 2007); MyPlayCity, Inc. v. Conduit Ltd., No. 10 Civ. 1615(CM), 2012 WL 1107648 at *12--14 (S.D.N.Y. Mar. 30, 2012) (holding that an online platform which provided toolbars which incorporated in-line links to plaintiff's copyrighted games did not commit an act of direct infringement when it in-line linked to plaintiff's games without permission, noting that "merely providing a 'link' to a site containing copyrighted material does not constitute direct infringement of a holder's distribution right").
[111] Perfect 10 v. Amazon, 508 F.3d 1146, 1161 (9th Cir. 2007).
[112] 17 U.S.C. § 106.
[113] 17 U.S.C. § 101.
[114] Perfect 10, 508 F.3d at 1161.
[115] 17 U.S.C. §101 (emphasis supplied).
[116] See H.R. Rep. No. 94—1476 at 63.
[117] Perfect 10, 508 F.3d at 1161.

drafters of the bill intended the scope of the display right to be broad enough to include "[e]ach and every method by which the images . . . comprising a . . . display are picked up and conveyed" and "any act by which [an] initial performance or display is transmitted, repeated, or made to recur," including "any type of electronic retrieval system."[118]

In support of the server test, U.S. courts typically downplay the role of hyperlinks in content delivery. One court likened the provision of a hyperlink to "using a library's card index to get reference to particular items, albeit faster and more efficiently."[119] Another court described hyperlinking as the "digital equivalent of giving the recipient driving directions to another website on the Internet."[120] These metaphors naturally support the conclusion that a hyperlink does not constitute part of the "process" of content transmission --- in the view of most U.S. courts, hyperlinks, like "library's card index[es]" and "driving directions" merely supply the information necessary for third parties to make a transfer, but they are not part of the transfer itself. However, these metaphors overlook the range of functions that hyperlinks serve on the Internet.

Hyperlinks do provide information about the online location of the content which the user seeks to access. This *locational-information* function is, indeed, analogous to the function fulfilled by a "library's card index" or "driving directions" in that it connects two end-points which seek to communicate with each other, but does not itself constitute part of the process that communicates a work from point A (the source site) to point B (the user's device) --- the provision of locational information simply makes the communication possible. However, most hyperlinks are *clickable* when presented on the webpages, and therefore these hyperlinks also act as a *trigger* which, when clicked, commence the communication between two end-points. When a user clicks on a hyperlink on a webpage, or visits a webpage which utilizes an in-line link, the hyperlink (and the underlying HTML code) triggers the transfer of information between the server and the user's browser. In other words, the hyperlink, when clicked, *sets in motion the process* through which the ultimate communication is consummated. This is the fundamental difference between a URL which is printed on a page in a book (which provides only locational information, and which can be utilized only if a user enters the address into her browser) and a URL which is embedded in a website as hypertext (which typically appears as blue, underlined text).

From a purely technical perspective, then, a clickable link that appears as hypertext on a website consists of *more* than just locational information. A hyperlink becomes clickable on a website only when the website's HTML code includes an HTML "tag" and a portion of code which turns the URL address into a clickable button which will lead the user's browser directly to the linked-to website. For example, a hyperlink to www.copyright.gov will display as a clickable hyperlink on a webpage only when the webpage's code contains the script: "www.copyright.gov."[121] The code surrounding the URL address exists only to activate the process of communication between server and browser.

[118] H.R. Rep. No. 94-1476 at 64 (1976).
[119] Ticketmaster Corp. v. Tickets.com Inc., No. CV 99–7654 HLH(BQRX), 2000 WL 525390, at *2 (C.D. Cal., Mar. 27, 2000).
[120] Pearson Educ., Inc. v. Ishayev, 963 F.Supp.2d 239, 250--51 (S.D.N.Y. 2013). See also Perfect 10, 508 F.3d at 1161 ("The HTML merely gives the address of the image to the user's browser. The browser then interacts with the computer that stores the infringing image.").
[121] HTML Links, w3schools.com (last visited Oct. 11, 2017).

Moreover, hyperlinks are often disguised as text (i.e. "click here") or presented graphically as buttons on a website.[122] In these contexts, the "trigger" function of hyperlinks is particularly prominent --- the hyperlink still provides locational information to the user's browser, but the hyperlink is presented to the user as a way to start a process through which another website's home page (simple link), or a specific piece of content (deep link, in-line link) will be delivered to the user's browser.

Instead of the only partially accurate "library card" and "driving directions" metaphors, we propose a more precise analogy: telephone directory assistance services. These services (typically reached by dialing the numbers "411" on a telephone) first connect a caller to a directory assistance operator, who helps the user identify the phone number of the intended recipient --- thus providing the information necessary to connect two end-points (caller and recipient) and fulfilling a function analogous to the function served by "driving directions" or a "library's card index." However, most directory assistance services do more: if the caller requests, the directory assistance operator may re-direct the caller's phone line to the intended recipient's line, thereby setting in motion the technical process through which the two end-points in fact connect. Similarly, a hyperlink both provides locational information to a user's browser, and (when clicked) sets in motion the process through which the user's browser requests the source server to deliver the desired content.

The role that directory assistance plays in the ultimate transmission of information between two end-points is optional; the caller could simply bypass directory assistance if the caller knows the right number to call, just as the internet user can bypass the use of a hyperlink if the user knows the URL address of the website she intends to visit. But if a user does use directory assistance not only to identify the number but to place the call, it seems evident that the call-placement role played by the directory assistance operators is part of the "process" through which a telephone user reaches a recipient. Similarly, a clickable hyperlink must be considered part of the "process" through which a user accesses a piece of underlying content: after a user clicks a link, the HTML code embedded in the link begins the process of transmission by supplying the URL location of the content to the user's browser and instructing the browser to access that URL, after which the browser completes the process of retrieving the content from the source server.

Additionally, some hyperlinks provide a further function by presenting the underlying material in a specific manner or context, or by cutting out intermediary steps that would otherwise be necessary for the user to access the content. While it may be true that a "simple" link (i.e. a URL to the U.S. Copyright Office's home page) fulfills a function limited to sending the user to another site that will in turn provide information about the location of a particular piece of content, deep links and in-line links do more than provide locational information --- they instead *serve up* content directly to the user.[123] In-line links may be used to "frame" the content in a

[122] Connecting to Other Websites, Stanford University Libraries: Copyright & Fair Use (last visited Oct. 11, 2017) ("[A] website will connect to another in the form of a link (also known as a 'hypertext' link), a *specially coded word or image* that when clicked upon, will take a user to another Web page.") (emphasis supplied).

[123] ALAI, Report and Opinion on a Berne-compatible reconciliation of hyperlinking and the communication to the public right on the internet (June 17 2015), http://www.alai.org/en/assets/files/resolutions/201503-hyperlinking-report-and-opinion-2.pdf ("[In-line and deep] links offer the works to the public in such a way that the members of the public may access the works at a place and time chosen by them. Those who furnish these kinds of links make it

particular way on a website --- thus in-line links can deliver content directly to a user without the need to navigate to a new webpage, or can place content in a specific context alongside other content, or draw attention to a particular portion of the content (e.g., a particular page in an in-line linked PDF document). Similarly, deep links deliver the content to the user directly, stripping away the need to navigate through the source website to access that work. In other words, in-line and deep links not only fulfill the function of a "library's card index" by identifying the location of a piece of content --- these links take the metaphorical book off the library's shelf, place the book in the recipient's hands, and turn to a particular page.

Thus, the server rule rests on an under-inclusive reading of the term "process" under which the "process" begins at the physical origin of the content, and ends with the delivery of that content to the browser (thus excluding from the term "process" any preliminary steps which provide the user's browser with the location of the desired content, or set the process in motion by providing a button or a piece of code which begins the process of transmission). From a technological perspective, then, the "server rule," mischaracterizes the "process" contemplated by section 101. More importantly, setting aside the technological minutiae of the process through which clickable deep or in-line links cause a work's images or sounds to be received by the end user, it "makes no difference" to the user's experience of the work whether its delivery emanated directly from the source site, or arrived through the mediation of a link. [124] As the copyright holder noted in its arguments before the Ninth Circuit in *Perfect 10 v. Amazon*, the court's interpretive approach draws a legal line which completely ignores the user experience: the typical viewer of a website has no way of distinguishing content which is stored on the servers of the website operator (and which is thus being "displayed" under the logic of the server rule) and content which is pulled from a third-party server through an in-line link (which, according to the server rule, is not being displayed by the website operator).

In *American Broadcasting Companies, Inc. v. Aereo, Inc.*, the U.S. Supreme Court cast doubt on analyses that privilege technical characterization over user experience.[125] In *Aereo*, the Supreme Court held that a service which provided online access to broadcast television committed acts of "public performance" even though it used user-specific television antennae to send user-specific re-transmissions of televised content to each user. A significant part of the majority's analysis focused on comparing Aereo's product to traditional television cable delivery services (which do commit acts of "public performance"). The Court strongly de-emphasized the technical differences between the two services, and instead focused on the user experience:

> In terms of the Act's purposes, [the differences between Aereo's product and traditional cable services] do not distinguish Aereo's system from cable systems, which do perform 'publicly.' Viewed in terms of Congress' regulatory objectives, why should any of these technological differences matter? They concern the behind-the-scenes way in which Aereo delivers television programming to its

possible to bring the works directly to the computer or device screens of the user, or to download them directly to the computer or device, without further intermediation.")

[124] In a recent case, the Supreme Court made a similar observation, noting that "technological differences" that do not "significantly alter the [user's] experience" should not govern the interpretation of the public display and performance rights under §106. American Broadcasting Companies, Inc. v. Aereo, Inc., 134 S.Ct. 2498, 2508 (2014).

[125] 134 S.Ct. 2498, 2506 (2014).

> viewers' screens. They do not render Aereo's commercial objective any different from that of cable companies. Nor do they significantly alter the viewing experience of Aereo's subscribers. Why would a subscriber who wishes to watch a television show care much whether images and sounds are delivered to his screen via a large multi subscriber antenna or one small dedicated antenna, whether they arrive instantaneously or after a few seconds' delay, or whether they are transmitted directly or after a personal copy is made?[126]

Therefore, the *Aereo* Court's logic dismisses the kind of "technological differences" that underlie the server rule. The technical differences between Aereo's system of delivering content and the system used by traditional cable companies had no bearing on whether Aereo's actions fell within the statutory definition of "public performance." One might wonder why the technical differences between the delivery of a piece of content stored on a website's server, and the delivery of a piece of content in-line linked to that website should matter at all to the analysis of whether that website commits an act of "public performance or display" when most users of that website are completely unable to distinguish between the two.[127]

Furthermore, the assumption that a hyperlink does not fall within the definition of public performance or display may be conceptually inconsistent with other authoritative U.S. case law. Other appellate court cases (decided before the Ninth Circuit's decision in *Perfect 10 v. Amazon*) found that when an actor contributes to an overall process of content delivery to an end-user, that actor may have committed an act of public display or performance even though the actor's contribution to the process did not, standing alone, result in the delivery of content to a user. In other words, an actor commits a public performance or display when that actor carries out "any step in the process by which a protected work wends its way to its audience."[128] Moreover, the reasoning of more recent U.S. Supreme Court precedent may have implicitly cast further doubt on the logical underpinnings and statutory consistency of the server rule. In a different part of the Supreme Court's *Aereo* opinion, the Supreme Court held that an actor who takes a step which "simply enhances viewers' ability to receive" an existing public display or performance may commit an act of public performance or display.[129] If one concedes that a hyperlink "enhances viewers' ability to receive" a piece of already-available content by providing and acting on the

[126] Id. at 2508.

[127] At least one litigant in the U.S. has argued that this aspect of the Supreme Court's *Aereo* decision casts doubt on the "user-agnostic" logic of the server rule. See Memorandum of Law in Support of Plaintiff's Motion for Partial Summary Judgment on Liability at 13, Getty Images (US), Inc. v. Microsoft Corp., No. 1:14-CV-07114-DLC (SDNY, filed Jan. 16, 2015)) (arguing that the *Aereo* decision had "rejected the very sort of technical distinctions that underpinned the 'server test'"). The *Getty v. Microsoft* litigation settled shortly after Getty made this argument, and the court did not issue an opinion commenting on the continued validity of the server rule after *Aereo*. See Stipulation of Dismissal with Prejudice, Getty Images (US), Inc. v. Microsoft Corp., No. 1:14-CV-07114-DLC (S.D.N.Y. entered Apr. 7, 2015). In 2012, the Cour de Cassation accepted a similar argument based on the user's impression of the source of the work, and held that an unauthorized in-line link to a work on a third-party website was infringing because users may have been under the impression that the content was located on the linking website. See *Google France v. Bac Films, n° 11-13.666* (Jul. 12, 2012), https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000026181926.

[128] NFL v. Primetime 24, 211 F.3d 10, 13 (2d Cir. 2000). Also see David v. Showtime/The Movie Channel, Inc., 697 F.Supp.752, 758 (S.D.N.Y. 1988) ("Congress intended the definition of [public performance] to encompass each step in the process by which a protected work wends its way to [the public]").

[129] See American Broadcasting Companies, Inc. v. Aereo, Inc., 134 S.Ct. 2498, 2506 (2014).

locational information that allows a protected work to "wend[] its way to its audience" of internet users, it seems difficult to reconcile the server rule with this authority.

Given the logical and doctrinal inconsistencies underpinning the server rule, one might sense that other imperatives lent bad arguments more credibility than they deserved. One might suspect that a desire to avoid imposing direct copyright liability on the widespread practice of internet hyperlinking may have motivated the adoption of the rule in *Perfect 10 v. Amazon*. The lower court in the *Perfect 10* litigation noted that a contrary result would "ensnare AOL, Dell, Microsoft, and Netscape" with unexpected copyright liability, and other commentators had noted (before the *Perfect 10 v. Amazon* decision) that imposing direct liability on links would "have far-reaching limiting effects on the development of the World Wide Web" and that such a rule would impose liability on "every online service provider directly linking to copyrighted works."[130]

However, by responding to these concerns with a broad rule which precludes any direct liability for linking, the Ninth Circuit may have overlooked the possibility that other areas of Copyright law could have alleviated these unwanted outcomes. Section 512(d) of the Digital Millennium Copyright Act (DMCA) provides a safe harbor for actors who may otherwise have infringed copyright through the use of "information location tools, including a directory, index, *reference, pointer, or hypertext link*."[131] The Ninth Circuit could have recognized that actors who provide hyperlinks may be found directly liable for copyright infringement under the correct interpretation of the relevant statutory provisions, but that those defendants may claim protection under the DMCA's safe harbor provisions by proving compliance with the DMCA's safe harbor qualification requirements.[132]

Statutory safe harbors to one side, even were US courts to abandon the server rule, other issues remain for resolution before a court rules that a link to unauthorized content constitutes a violation of the § 106 display, performance, or distribution rights. Even assuming that a hyperlink is part of the "process" through which content is delivered, it is not clear whether the "process" itself must be realized (through an ultimate delivery of the content, beginning with the activation of a link) or whether it would suffice for that delivery merely to be incipient. In other words, is there a public performance or display if a link is simply posted, but never clicked? With respect to the exclusive right of distribution of a work in copies, U.S. case law is inconsistent on the question whether a violation of the right requires proof of an "actual download," or whether the "making available" of access to an online copy is sufficient to support an infringement claim.[133] By contrast, case law suggests that for claims of infringement of the

[130] Perfect 10 v. Google, 416 F.Supp.2d 828, 841 (2006) (quoting 4 Nimmer on Copyright § 12B.01[A][2] (2005); Matthew C. Staples, *Kelly v. Arriba Soft Corp.*, 18 Berkeley Tech. L.J. 69, 80--81 (2003).

[131] 17 U.S.C. § 512(d) (emphasis supplied).

[132] Qualifying for the DMCA's safe harbor requires that the defendant prove compliance with the particular requirements of the specific claimed safe harbor, which will be discussed below. See infra section IV.b.

[133] Compare London-Sire Records v. Does, 542 F.Supp.2d 153, 176 (D. Mass. 2008) (holding that "evidence and allegations, taken together, [can be] sufficient to allow a statistically reasonable inference that at least one copyrighted work was downloaded at least once" and that this inference is "sufficient to make out a prima facie case" of infringement); Atlantic Recording Corp. v. Howell, 554 F.Supp.2d 976, 985 (D. Ariz. 2008) (holding that "[t]he general rule, supported by the great weight of authority, is that infringement of [the distribution right] requires an actual dissemination of either copies or phonorecords"); Elektra Entertainment Group, Inc. v. Barker, 551

public display or performance rights, the plaintiff need not prove that an internet user in fact accessed the file at issue. The Copyright Office takes the position that the definition of to perform or display a work 'publicly' "is properly construed" to reach "offers to stream, rather than just completed transmissions," even though the issue has not been "squarely resolved by courts."[134] This interpretation arguably is inconsistent with the statutory language, whose reference to the *receipt* of a transmission in the statutory definition of public performance or display could suggest a completed transmission.[135] On the other hand, interpreting the statutory definition to preclude prospective receipt of performances or displays of works of authorship would create tension between that interpretation of the definition section and other sections of the copyright act, which cover both completed and incipient transmissions.[136] Moreover, such an interpretation would set the US at odds with the international norm: as we have seen, the "making available" right in the WCT and WPPT unambiguously covers prospective communications.[137] When the meaning of the domestic norm is in doubt, the *Charming Betsy* canon of statutory construction directs courts to interpret US law consistently with the nation's international obligations.[138]

III.A.iii.b: The server rule and its implications for in-line linking

Many software experts have long argued that the principle of "universal free linking" is fundamental to the proper functioning of the World Wide Web.[139] Before *Perfect 10 v. Amazon*, legal scholars noted their opposition to the use of copyright or other legal regimes to impose liability for linking, which they believed to be antithetical to the role of a link on the internet.[140]

F.Supp.2d 234, 243--45 (S.D.N.Y. 2008) (stating that the distribution right guaranteed by the Copyright Act may be infringed by an offer to distribute, although merely alleging that files were made available, without alleging that they were also distributed, is not enough to state a claim).

[134] See United States Copyright Office, Report on The Making Available Right in the United States 37 (February 2017), https://www.copyright.gov/docs/making_available/making-available-right.pdf; see also Cmty. Broad. Serv. v. Time Warner Cable, LLC, No. 07-139-B-W, 2008 WL 3200661, at *9--10 (D. Me. Aug. 7, 2008) (noting that the plaintiff alleging a performance "to the public" need only allege that the transmission "was capable of being viewed by a substantial number of people," and that the plaintiff "need not prove that a substantial number of people actually viewed the challenged transmission").

[135] See 17 U.S.C. §101 (defining public performance and display as a transmission "to the public . . . whether the members of the public capable of receiving the performance or display *receive it* in the same place or in separate places and at the same time or at different times.") (emphasis supplied).

[136] For example, Section 506 of the Copyright Act provides for criminal penalties for any person who commits an infringement "by the distribution of a work being prepared for commercial distribution, by *making it available* on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution." 17 U.S.C. § 506 (emphasis supplied). As David Carson, former General Counsel of the U.S. Copyright Office, has pointed out, "[i]t is hard to fathom how this language can be read as anything other than Congress telling us, in the form of an amendment to the copyright statute, that the distribution right includes the act of making copies available." David O. Carson, Making the Making Available Right Available: 22nd Annual Horace S. Manges Lecture, 33 Colum. J.L. & Arts 135, 160--61 (2010).

[137] See supra note 11 and accompanying text.

[138] See, e.g., Copyright Office Report, supra, at 55-56.

[139] See Mark Sableman, Link Law Revisited: Internet Linking Law at Five Years, 16 Berkeley Tech. L.J. 1273, 1275--76 (2001) (describing the views of Tim Berners-Lee, one of the first software experts to develop the internet protocol, who believed that "[t]he universality [of free linking] is essential to the Web. . . it loses its power if there are certain types of things to which you can't link").

[140] Id. (noting that "most Internet users see links as desirable on all sides and are puzzled by any legal scheme that would penalize or restrict use of such mutually beneficial indexes, roadmaps, and accolades").

One internet user noted that "[t]o ask permission to link to a page borders on the inane. Next, we will have the position that you cannot recommend a book in the local library without the author's permission."[141]

However, the adoption of the "server rule" may have over-applied this principle by holding that even in-line links, which integrate content onto the linker's website in a way that makes that content appear (to the Internet user) as if it originated on the linker's website, cannot constitute direct copyright infringement. This aspect of the holding of *Perfect 10 v. Amazon* allows any website operator freely to incorporate copyrighted elements from other websites (through in-line linking) without incurring any direct copyright liability, and has been hailed as a "major victory for web site operators" who need no longer worry about copyright liability (or seek licenses from copyright holders) when incorporating works found on other websites onto their own websites.[142]

Such a "victory" may make it difficult for copyright owners safely to use the internet to publish their works without losing control of how their works are presented to audiences. If any copyrighted work, published online, can be freely framed on another unaffiliated and unauthorized website, copyright owners may lose the ability to derive advertising revenue from presenting their works on their own websites, as well as the ability to determine the presentational context in which their works appear, and the ability to derive licensing revenue from other websites which seek to use their copyrighted material.[143] Some commentators have argued that legal regimes which allow unrestricted in-line linking to internet works will force copyright owners to implement additional technical restrictions when publishing their works online, thus making them less freely available to the public.[144] Commentators have also noted

[141] Id. (quoting Posting of Owen Cook, at http://dgl.com/msg1/messages/7.html (posted Sept. 14, 1997)).

[142] Lee Burgunder & Barry Floyd, The Future of Inline Web Designing After Perfect 10, 17 Tex. Intell. Prop. L.J. 1 (2008) ("[As a result of *Perfect 10*] a website that posts its own copyrighted materials cannot complain that other sites are displaying those same works as part of their offerings as long as those displays are made through inline web designing.").

[143] PACA, Digital Media Licensing Ass'n Inc., Nat'l Press Photographers Ass'n, Am. Soc'y of Media Photographers, and Graphics Artists Guild, Comments Submitted in Response to U.S. Copyright Office's July 15, 2014 Notice of Inquiry at 4. The court in *Perfect 10* did suggest that trademark law, rather than copyright law, should protect publishers from "acts that cause customer confusion," indicating that the problem of "in-line linking and framing [which may] cause some computer users to believe they are viewing a single . . . webpage" is not addressed by the Copyright Act. See Perfect 10 v. Amazon, 508 F.3d 1146, 1161 (9th Cir. 2007). The court also suggested that in-line linking or framing could "raise[] contributory liability issues." Id. Secondary liability (a doctrine of which contributory liability is a subset) will be discussed further below, but because claims of secondary liability must rest on an act of direct liability, See A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (2001), secondary liability may not protect copyright holders from websites which in-line link to authorized display of performances of their works.

[144] Matthew C. Staples, *Kelly v. Arriba Soft Corp.*, 18 Berkeley Tech. L.J. 69, 82 (2003) ("Rather than acquiring a license for copyrighted images, Web authors could freely code their webpages to inline link to images residing on others' servers. Servers hosting popular images, particularly those of broad or general relevance, would be linked to by several webpages and would have to employ technological controls to prevent such linking."). Similar critiques were voiced in the EU after the CJEU extended the *Svensson* doctrine to in-line linking in the *BestWater* case. See Case C-348/13, BestWater Int'l GmBH v. Michael Mebes (21 Oct. 2014), http://curia.europa.eu/juris/liste.jsf?num=C-348/13; supra notes 22--24 (discussing *Svensson*); Dr. Matthias Leistner, Closing the Book on the Hyperlinks: A Brief Outline of the CJEU's Case Law and Proposal for European Legislative Reform, 39 European Intellectual Property Review 327, 330 (2017) (noting that the CJEU's *BestWater* case, in applying the *Svensson* doctrine to "framed" or in-line links, may "allow[] the author's work to be placed in contexts which he or she may not agree [to]" and thus forces an "all-or-nothing" decision on the original publisher,

that a regime which forces copyright owners to rely on technical restrictions to publish their works online without fear of unauthorized in-line linking may be unfair to "the unseasoned Internet publisher," who, unlike large, commercial websites, may "not have the time, resources, training, or experience to thwart unwanted links."[145]

III.A.iii.c: The server rule and the international obligation to implement the making available right

The server rule adopted in *Perfect 10 v. Amazon* may also put the United States at risk of falling short of its obligation to protect copyright owners' "making available" right under the WIPO Copyright Treaty ("WCT") and the WIPO Performance and Phonograms Treaty ("WPPT").[146] Some commentators have put forward the argument that the server rule "eviscerates" the making available right by allowing other websites to in-line or frame their copyrighted content without permission, thus divesting the copyright holders of the ability to control how their works are disseminated online.[147] The server rule's exclusion of deep and in-line linking is also at odds with our interpretation of the WIPO Treaties' designation of the "place" from which members of the public choose to access works.[148]

The United States Copyright Office ("Copyright Office") noted many of these arguments in a recent report on the "making available" right, but simply concluded that there remained doubt about whether "a court might deem certain forms of inline linking or framing distinguishable from the technology in *Perfect 10* for purposes of the server test" and that "[c]onclusive resolution of these issues will require further guidance from courts."[149] However, only one case from 2007 (decided nine years before publication of the Copyright Office's report, and 6 months before the Ninth Circuit's decision in *Perfect 10 v. Amazon*) has held that a direct infringement claim based solely on hyperlinking can succeed.[150] It therefore seems unlikely that U.S. courts will limit application of the server rule in a way that will bring U.S. copyright law in line with the WCT and the WPPT's provisions, assuming that the "making available" right reaches at least some forms of linking.

On the other hand, the US exclusion of direct liability for hyperlinking would not preclude US compliance with its international obligations, so long as US law furnished an alternative basis for

---

who must choose "whether he or she will prevent or permit corresponding linking in principle by deploying technical protective measures," and further arguing in support of a recognition that all "frame links misappropriating third-party material fall under the [communication to the public] right" notwithstanding the "new public" criterion).

[145] Matthew Staples, *Kelly v. Arriba Soft Corp.*, 18 Berkeley Tech. L.J. 69, 89 (2003).

[146] See supra Part I.

[147] PACA, Digital Media Licensing Ass'n Inc., Nat'l Press Photographers Ass'n, Am. Soc'y of Media Photographers, and Graphics Artists Guild, Comments Submitted in Response to U.S. Copyright Office's July 15, 2014 Notice of Inquiry at 4. See also United States Copyright Office, Report on The Making Available Right in the United States 49 (February 2016) (noting these arguments).

[148] See supra notes 16--21 and accompanying text.

[149] United States Copyright Office, Report on The Making Available Right in the United States 50--51 (February 2016).

[150] See Live Nation Motor Spots, Inc. v. Davis, 2007 WL 79311 (N.D. Tex. 2007) (holding that a defendant which framed an authorized stream of a copyrighted work committed a direct act of public performance and display and was unauthorized to do so). The *Live Nation* opinion was filed in January 2007, and the Ninth Circuit's *Perfect 10 v. Amazon* decision was filed in May 2007. See Perfect 10 v. Amazon, 508 F.3d 1146 (9th Cir. 2007).

effective enforcement of the exclusive rights of public performance and display.[151] We next consider whether the US doctrine of secondary liability, as applied to hyperlinking, sufficiently fills the gap.

III.B. Secondary Liability for Hyperlinking in the United States

III.B.i: Implications of Treating Hyperlinking under Secondary Liability

Current U.S. doctrine bars claims of direct copyright infringement for hyperlinking and instead addresses hyperlinking through secondary infringement analysis. In the EU, the lack of harmonization of secondary liability standards across EU member states provided the impetus for characterizing direct violations of the right of communication to the public to encompass at least some kinds of facilitation of infringement by means of hyperlinking.[152] In the US, by contrast, copyright doctrine is effectively "harmonized" across jurisdictions with respect to both direct and secondary liability. Albeit based in the common law, secondary liability for copyright infringement is a matter of federal law rather than of the laws of the 50 states. Treating hyperlinking as a matter of secondary liability thus does not present the problem of multiple inconsistent national standards that confronted the CJEU.

This is not to say that the US standards for direct and secondary liability for copyright infringement are identical. While direct infringement in the U.S. is a strict liability offense,[153] the secondary liability doctrine of contributory infringement requires that the secondary infringer "know[s] or [has] reason to know" of direct infringement.[154] The server rule thus makes a hyperlinking defendant's liability turn on its actual or constructive knowledge of the infringing nature of the infringed work.[155]

III.B.ii: Secondary Liability Doctrines in the United States

Copyright actions in the U.S. concerning secondary liability for hyperlinking typically allege that the defendant linked to an *unauthorized* source of a work protected by copyright. Because U.S. courts have reiterated that there can be no secondary liability absent a primary infringement of copyright,[156] plaintiffs therefore will not succeed on secondary infringement claims based on

---

[151] Cf. Copyright Board of Canada, CB-CDA 2017-085 (August 25, 2017) at ¶ 162 (regarding national implementation of the WCT art. 8 making available right) ("What name a right is given in domestic legislation does not make it any more or any less compliant. What is important is that all the acts contemplated by the treaties are covered through one or more exclusive rights.").

[152] See supra section II.A. See also Lyubomira Midelieva, Rethinking Hyperlinking: Addressing Hyperlinks to Unauthorised Content in Copyright Law and Policy, 39 European Intellectual Property Review 479, 487 (2017).

[153] EMI Christian Music Group, Inc. v. MP3Tunes, LLC, 844 F.3d 79, 89 (2d Cir. 2016).

[154] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001) (citing Cable/Home Communication Corp. v. Network Prods., Inc, 902 F.3d 829, 845 & 846 n. 29 (11th Cir. 1990)).

[155] This aspect of the secondary infringement analysis under U.S. law parallels the knowledge-based standard which the CJEU imposed in the *GS Media* case. See Part II, supra.

[156] Id. See, e.g., La Resolana Architects, PA v. Reno, Inc., 555 F.3d 1171, 1181 (10th Cir. 2009) ("[B]oth contributory and vicarious infringements require someone to have directly infringed the copyright."); Perfect 10, Inc. v. Amazon.com, Inc., 608 F.3d 1146, 1169 (9th Cir. 2007). Additionally, a claim of secondary infringement requires that the facilitated act of direct infringement occurs within the United States. See Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088, 1091--95 (9th Cir. 1994); but see Paul Goldstein, International

links to authorized sources because the access which the link enables is not itself an act of direct infringement.[157]

U.S. copyright law recognizes three forms of secondary liability: vicarious infringement,[158] contributory infringement,[159] and inducement of infringement.[160] Vicarious infringement lies when a defendant "profit[s] from direct infringement while declining to exercise the right to stop or limit it."[161] In order to prove a claim of contributory infringement, the copyright holder must

---

Copyright: Principles, Law, and Practice § 3.1, at 71--72 (2001) (criticizing the "overly rigid conception of territoriality" reflected in Subafilms and arguing that such a conception "may result in the conclusion that no infringement has occurred anywhere," especially in the context of suits regarding "[t]he use of digital networks to transmit copyrighted works to individual recipients on demand, and proposing an "effects-based test of territoriality").

[157] In support of secondary infringement claims, some plaintiffs have advanced the theory that when a defendant causes (by way of hyperlink or HTML code) the plaintiff's copyrighted work to be downloaded onto a user's RAM memory, that defendant causes an act of direct infringement on behalf of the *user*, which qualifies as an act of direct infringement on which a claim of secondary liability can be predicated. See, e.g. Live Face on Web, LLC v. The Control Group Media Company, Inc., 150 F.Supp.3d 489, 498 (2015) ("A visitor to one of Defendant's web pages . . . download[s] a copy [of plantiff's software] into his computer's RAM, thereby infringing the [plaintiff's] copyright."). Such an argument rests on the assumption that any user who visits any webpage commits an act of direct infringement by automatically downloading copyrighted works contained on the website to RAM memory, even if the user does not save the image to her hard drive in a more permanent form. Not all courts accept this theory --- in *Perfect 10 v. Amazon*, the Ninth Circuit considered whether "[l]ocal caching [of copyrighted images] by the browsers of individual users" that occurs when a user's browser automatically stores the images to RAM for the purposes of displaying those images on a computer screen constituted a violation of the reproduction right. The court held that "even assuming such automatic copying could constitute direct infringement, it is a fair use" because "it is designed to enhance an individual's computer use, not to supersede the copyright holders' exploitation of their works." See Perfect 10 v. Amazon, 508 F.3d 1146, 1169 (2007).

[158] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 914 (2005) ("[O]ne may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.").

[159] See Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (1971) ("[O]ne who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer.").

[160] Grokster, 545 U.S. 913 (holding that "[e]vidence of active steps . . . taken to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe" which may support a claim of secondary liability under an inducement-of-infringement theory) (internal quotation marks and citations omitted).

[161] Id. at 914. The doctrine of vicarious infringement developed to account for situations in which a defendant exercises some supervisory role over infringing actors, and benefits from that activity without exercising its right to stop the infringement. Thus, the doctrine of vicarious liability is a poor fit for the hyperlinking context, in which the linker rarely has control over the infringing activity to which it links. While it may be argued that a linker may "control" a linked-to source by simply removing the link, courts have held that the "control" element in vicarious infringement analysis requires the actual ability to stop the direct infringement. See Perfect 10 v. Amazon, 508 F.3d 1146, at 1173--74 (2007) (holding that Google's right to terminate a particular website's advertising contract "does not give Google the right to stop direct infringement" because "an infringing third-party website can continue to reproduce, display, and distribute its infringing copies of [plaintiff's] copyrighted works after its" contract with Google ended, and thus Google could not be found liable as a vicarious infringer). Nevertheless, some plaintiffs have brought vicarious infringement claims in in the hyperlinking context based on the theory that the defendant's website *users* committed an act of direct infringement (by visiting defendant's website and automatically downloading the plaintiff's copyrighted works which were framed on that website to RAM memory), and that the defendant, as the operator of the website, had the right and ability to stop these acts of user-infringement by altering the website. See, e.g. Live Face on Web, LLC v. Howard Stern Productions, Civil Action No. 08-2579, 2009 WL 723481, at *2--4 (E.D. Pa. Mar. 17, 2009). These cases are rare, and such a theory of vicarious liability may

show that the defendant "induce[d], cause[d], or materially contribute[d] to the infringing conduct of another" "with knowledge of the infringing activity."[162] Lastly, inducement of infringement may lie if the defendant takes "active steps . . . to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use," builds a business model which "confirm[s] that [the defendant's] principal object" is to facilitate infringement of copyright, and takes no effort to limit the infringing activity resulting from its acts.[163]

III.B.ii.a. Contributory Infringement

The contributory infringement analysis poses dual criteria: (i) "personal conduct that encourages or assists" an act of direct infringement (also framed as "material contribution" to an act of direct infringement) and (ii) actual or constructive knowledge of the specific direct infringement.[164]

Under contributory liability doctrine, even the provision of a "simple link" could constitute an act of secondary infringement if that link "encourages or assists" an ultimate act of infringement.[165] In most of the reported cases concerning secondary liability for hyperlinking, courts have found that providing a hyperlink to an unauthorized source, in addition to some "encouraging" activity, satisfied the "personal conduct that encourages or assists" or "material contribution" requirement. For example, in *Pearson Educ., Inc. v. Ishayev*, the court found that a defendant who sold unauthorized versions of educational materials online and provided the materials to its customers by providing links to file sharing sites through which the infringing materials could be downloaded "plainly" carried out "conduct that encourages or assists in copyright infringement" and could thus be found contributorily liable.[166] In *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry,* a defendant who had posted hyperlinks to third-party websites which offered infringing copies of the plaintiff's copyrighted material on blog posts which encouraged readers to download the materials was held to have "materially contributed" to the acts of direct infringement carried out by the third-party websites.[167]

---

ultimately fail because courts have held that the automatic downloading to RAM of a work by an internet user simply for the purposes of browsing the internet is fair use. See Perfect 10 v. Amazon, 508 F.3d 1146, 1169 (2007) (holding that "even assuming such automatic copying could constitute direct infringement, it is a fair use" because "it is designed to enhance an individual's computer use, not to supersede the copyright holders' exploitation of their works").

[162] Gershwin Publishing Corp., 443 F.2d at 1159.

[163] Grokster, 545 U.S. at 926. See also Perfect 10 v. Amazon, 508 F.3d 1146, 1171 ("[U]nder *Grokster*, an actor may be contributorily liable for intentionally encouraging direct infringement if the actor knowingly takes steps that are substantially certain to result in such direct infringement.").

[164] Matthew Bender & Co. v. West Publishing Co., 158 F.3d 693, 706 (2d Cir. 1998).

[165] For example, if the provided simple link takes the user to the homepage of a website aggregating links to unauthorized sources which the user must then navigate to access the infringing content on the third party sites,, the link provider's act could constitute an act of contributory infringement (or inducement of infringement) if her act "induce[d], cause[d], or materially contribute[d] to the infringing conduct of another" "with knowledge of the infringing activity." Gershwin Publishing Corp., 443 F.2d at 1159.

[166] Pearson Educ., Inc. v. Ishayev, 9 F.Supp.3d 328, 339 (2014) ("[S]ending hyperlinks that permit others to download protected materials would plainly amount to conduct that encourages or assists in copyright infringement.").

[167] 75 F.Supp.2d 1290, 1295 (D. Utah, 1999) (granting an injunction after finding that defendants "actively encouraged the infringement of plaintiff's copyright" by posting three download links and by providing further instructions to a user on how to browse the material after one of the links didn't work).

It may be true that the reported cases do not concern "pure" acts of hyperlinking (i.e. the mere provision of a link, without any encouragement to use the link). Because most of the U.S. precedent on contributory liability for linking concerns some additional "encouraging" activity (i.e. encouraging users to click a link on a blog post, as in *Utah Lighthouse,* or selling a customer access to a link, as in *Ishayev*), it is theoretically possible for a defendant who merely provided a link to argue successfully that the provision of a link alone does not rise to the level of "material contribution" to an act of direct infringement. However, some courts have noted that acts which "facilitate access to websites throughout the world can significantly magnify the effects of otherwise immaterial infringing activities," which supports the assumption that the mere provision of a link to an unauthorized source (which necessarily facilitates and expands access to that source) itself can constitute a material contribution to the underlying act of direct infringement.[168]

The second element, actual or constructive knowledge, is more complex. The knowledge standard for contributory infringement analysis is "an objective one; contributory infringement liability is imposed on persons who 'know or *have reason to know*" of the direct infringement.[169] Generally, the analysis of the knowledge standard will consist of two inquiries: First, can the plaintiff prove that the defendant has specific knowledge of the particular works to which it is alleged to have facilitated access (in contrast to a defendant who may not be aware of the particular acts of infringement which it is facilitating)?[170] Second, can the plaintiff prove that the defendant had knowledge that the acts it facilitated were infringements of copyright? In most notable contributory liability cases, these two inquiries collapse into one --- for example, in *A&M Records, Inc. v. Napster, Inc.*[171] the court assumed that Napster was aware that the files it was helping its users distribute were infringing versions of copyrighted songs, and focused instead on whether Napster had "specific information which identifie[d] infringing activity."[172] Because the Napster organization maintained a central index of all the files shared on its system, the court was able to conclude that Napster had reason to know of the specific instances of infringement which were occurring on its platform (and thus "fail[ed] to remove the material and thereby stop [infringing copies] from being distributed," which satisfied the actual knowledge element).[173]

Therefore, inquiry into whether the defendant had actual or constructive knowledge of the particular works to which its offending hyperlink facilitated access will supply the first step in the analysis of knowledge for claims of contributory liability by hyperlink. Because the provision of a deep or in-line link is, in most cases, an act that relates specifically to one particular source and one particular copyrighted work (and not an act that facilitates large number of potential infringements through the provision of a platform, as in the *Napster* case), the linker will necessarily know which works it is targeting.

---

[168] Perfect 10 v. Amazon, 508 F.3d 1146, 1172 (2007).
[169] Arista Records, LLC v. Doe, 604 F.3d 110, 118 (2010).
[170] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (2001) ("[I]f a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement.")
[171] Id.
[172] Id. at 1021.
[173] Id. (internal quotation marks and citations omitted).

In cases which involve linking to websites which aggregate infringing content (e.g. sites which aggregate online sources of infringing works of films and television content), defendants may be able to argue that they lack the particularized knowledge of the specific works available through the linked-to website. In such cases, the defendant's generalized knowledge that some infringement occurs on the linked-to website may not suffice to meet the actual or constructive knowledge predicate to liability for contributory infringement. However, even if plaintiffs fail to prove that the defendant had particularized knowledge of the specific works available through the linked-to site, plaintiffs still may proceed under the doctrine of inducement of infringement, which furnishes a way to impose liability on defendants who lack particularized knowledge but who take "active steps" to encourage infringement.[174]

Nonetheless, in most hyperlinking cases (aside from cases involving links to aggregators, which we address further below), the "knowledge" analysis will most likely focus on whether the defendant had knowledge that the source to which it linked was unauthorized. Because, in most instances, the actor's knowledge of the infringing nature of the linked-to source has been obvious from the factual record, courts so far have not needed to grapple with this criterion.[175]

In cases in which the defendant's knowledge of the infringing nature of the source is not so clear, litigants may argue that a court should presume knowledge of the infringing nature of the linked-to source.[176] In several cases, plaintiffs have argued that identifying characteristics of a website or the nature and format of the copyrighted work itself should form the basis of a presumption that the defendant knew or should have known that facilitating access to that website constituted the facilitation of copyright infringement. For example, in *EMI Christian Music Group, Inc. v. MP3tunes, LLC*, a copyright owner argued that defendant knew, or should have known, that the songs shared on its online music service were infringing and unauthorized.[177] In that case, the Second Circuit held that the jury could reasonably conclude that the evidence presented at trial proved that the defendant "knew that major music labels generally had not even authorized their music to be distributed in the format most widely available" on defendant's platform, and that this supported a finding that the defendant had "knowledge of, or was willfully blind to, the

[174] See supra section III.B.ii.b (addressing inducement of infringement).

[175] For example, in Pearson Educ., Inc. v. Ishayev, 9 F.Supp.3d 328 (2014), the court could safely assume that the defendant knew that the hyperlink in question linked to an infringing source because the defendant was in the business of selling unauthorized copies of educational materials; and in Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, 75 F.Supp.2d 1290 (D. Utah, 1999), the defendants clearly knew that the linked to materials were infringing because they had previously posted the materials to their own website and were ordered to remove them on the basis of copyright infringement. See id. at 1294--95.

[176] In the U.S., presumptions of knowledge of the infringing nature of the work are typically based on the nature of and circumstances surrounding the allegedly infringing act --- U.S. courts have not adopted a presumption of knowledge of the infringing nature of the work based solely on the commercial nature of the defendant's acts. Compare Case C-160/15, GS Media BV v. Sanoma Media Netherlands BV, at pt. 51 (8 Sept. 2016), http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141 ("[W]hen the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead, so that it must be presumed that that posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder.").

[177] EMI Christian Music Group, Inc. v. MP3tunes, LLC, 844 F.3d 79 (2d Cir. 2016).

infringing nature of" certain well-known songs shared on its platform.[178] However, in *Perfect 10 v. CCBill LLC*, a copyright owner made a similar argument, and asked the court to presume that a web-hosting provider knew that it was facilitating infringing activity by providing services to websites with domain names which hinted that the sites' infringing nature (e.g. "illegal.net" and "stolencelebritypics.com").[179] The court disagreed, holding that the incriminating names "may [have been] an attempt to increase their salacious appeal" and reasoned that the defendant may have been justified to assume that the incriminating names were not "an admission that the photographs [contained on the websites were] actually illegal or stolen."[180]

However, in the context of hyperlinking, it may be easier for a court to presume that a linker knew of the infringing nature of the linked-to work. First, in some cases, one may presume the infringing character of the linked-to site from the nature of the copyrighted work contained on the site.[181] For example, a site offering a stream of a newly released film for free may be presumed to be unauthorized simply because, as a matter of public knowledge, such works are not offered to the public for free by their copyright owners. Second, the copyright owner could notify the defendant of the infringing nature of the work to which the defendant links with a notice, which may suffice to meet the knowledge requirement under the contributory liability analysis.[182]

---

[178] Id. at 92--93. Note that this reasoning was a part of an analysis of whether the defendant qualified for safe harbor under section 512 of the Digital Millennium Copyright Act (DMCA), and did not concern whether the defendant was liable as a contributory infringer. However, the analysis of §512 safe harbor liability is closely related to the analysis of secondary liability. See section V.b, infra.

[179] 488 F.3d 1102, 1114 (2007).

[180] Id. Similarly, in *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F.Supp.2d 627 (2011), the copyright holder argued that the defendant, the provider of an online website that aggregated links to websites through which users could download mp3 files of songs, should be presumed to have known about the infringing nature of the sites which its website linked to simply because some of the linked-to websites used the terms "free," "mp3," or "file-sharing" in their domain names. See Id. at 644.[180] The court rejected this argument, finding that "those terms are ubiquitous among legitimate sites offering legitimate services." Id. Note that the courts' analysis in both *Perfect 10 v. CCBill LLC* and *Capitol Records, Inc. v. MP3tunes, LLC*, like the court's analysis in *EMI Christian Music Group, Inc. v. MP3tunes, LLC*, concerned the defendant's eligibility for DMCA safe harbor, and did not concern the knowledge requirement under contributory liability doctrine.

[181] See, e.g., EMI Christian Music Group, Inc. v. MP3tunes, LLC, 844 F.3d 79, 92--93 (2016) (concluding that evidence that the defendant "knew that major music labels generally had not even authorized their music to be distributed in the format" through which defendant's file sharing platform helped to distribute songs was sufficient to conclude that the defendants had "knowledge of, or was willfully blind to, the infringing nature of the" the songs on its servers); Capitol Records, LLC v. Vimeo, 972 F.Supp.2d 537, 546--549 (2013) (holding that "a reasonable juror could---but need not---find that the infringing [nature of videos uploaded to a video hosting site containing well known songs] was 'objectively' obvious to a reasonable person").

[182] See, e.g., Flava Works, Inc. v. Gunter, No. 10 C 6517, 2011 WL 3205399 at *7 (N.D. Ill. July 27, 2011) (holding that "we . . . have no doubt that defendants knew or should have known" of the infringing nature of the works which the defendants facilitated access to because the copyright owner "sent at least seven DMCA notices that identified specific infringing files" and sent several emails informing the defendant of the infringing nature of the files). The sending of these "take-down" notices implicates the issue of whether the defendant can claim safe harbor under the Digital Millennium Copyright Act, which is addressed below. See 17 U.S.C. § 512(d) (holding that a "service provider shall not be liable [for copyright infringement] by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using . . . hyperlink text . . . if the service provider . . . (1)(C) upon obtaining [knowledge that the material or activity is infringing], acts expeditiously to remove, or disable access to, the material"). Therefore, by sending a notice to the linker, the copyright owner may be able to (i) ensure that the defendant must either take the link down or face disqualification from the DMCA's safe

III.B.ii.b. Inducement of Infringement

Liability for inducement of infringement is a variant of contributory infringement, whose elements the U.S. Supreme Court detailed in a case involving the liability of operators of P2P platforms: (i) "[e]vidence of active steps taken to encourage direct infringement, such as advertising an infringing use or instructing how to engage in an infringing use" e.g. "aiming to satisfy a known source of demand for copyright infringement," (ii) failing to attempt to "diminish the infringing activity," and (iii) building a business model that is structured around infringing use.[183] In a case concerning inducement liability of the operator of a BitTorrent "tracker" platform, the Ninth Circuit Court of Appeals ruled that the defendant had "active[ly] encourag[ed] the uploading of [infringing] torrent files," "acted with a purpose to cause copyright violations by the use of" its service, "took no steps to . . . diminish the infringing activity," and ran a business model based on benefitting from infringing activity.[184] One significant difference between liability for supplying the means to infringe (through traditional contributory or vicarious liability) and liability for inducement concerns the level of required knowledge. While U.S. courts have demanded a showing of specific knowledge regarding the works whose infringement the defendant facilitated,[185] in the case of inducement, by contrast, U.S. courts have ruled that proof of intent to promote infringement sufficed to make out the violation, without requiring that the defendant knew precisely which works would be infringed.

The inducement of infringement doctrine is likely to prove most useful when the link at issue leads to a site on which multiple works are accessible (i.e. a website which aggregates links to online sources of infringing copies of film or television content). Plaintiffs who fail to prove that the defendant-linker had particularized knowledge of the specific works accessible on that site may still succeed if they can show that the defendant-linker "active[ly] encourage[d]" the infringement, "acted with a purpose to cause copyright violations" through the provision if the link, "took no steps to . . . diminish the infringing activity" by removing the link, and ran a business model based on benefitting from the infringing activity which was facilitated by the link at issue.[186]

In many instances, then, doctrines of secondary liability will cover much of the ground left open by US copyright law's exclusion of direct liability for hyperlinking. But, in the online context, both direct and secondary liability claims now encounter assertions of service provider immunity under the 1998 Online Copyright Infringement Liability Limitations Act. To determine what secondary liability claims for hyperlinking might survive the act's liability preclusions, we now address the terms and implementation of the statutory "safe harbors."

III.C. The Digital Millennium Copyright Act and Safe Harbor Under U.S. Law

harbor provisions, and (ii) ensure that she will be able to prove that the defendant had knowledge of the infringing nature of the linked-to source for purposes of proving affirmative liability.

[183] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[184] Columbia Pictures Indus. v. Fung, 710 F.3d 1020 (9th Cir. 2013).

[185] See, e.g., Sony Corp. Of America v. Universal City Studios, Inc., 464 U.S. 417 (1984); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2004).

[186] Columbia Pictures Indus. v. Fung, 710 F.3d 1020 (9th Cir. 2013).

Remedies in the United States for copyright infringement by means of hyperlinking may also depend on the applicability of several safe harbor provisions which, like the EU eCommerce Directive,[187] provide immunity from copyright infringement under certain circumstances. The United States enacted the Digital Millennium Copyright Act (DMCA) in 1998, which includes several provisions designed to "create a series of 'safe harbors[]' for certain common activities of service providers."[188] Through these safe harbor provisions, titled "Limitations on liability relating to material online," Congress sought to provide "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[189] As the Senate report indicates, in acknowledging the occurrence of infringements and the resulting "legal exposure," the DMCA safe harbor provisions do not in fact exclude *liability* for copyright infringement but instead *limit the remedies* available against defendants for both direct and secondary copyright infringement..[190]

The law creates four safe harbors which allow qualifying "service providers" immunity from claims of copyright infringement: subsection 512(a) establishes a safe harbor for "transitory digital network communications" (which applies to providers of internet access), subsection 512(b) establishes a safe harbor for "system caching" (or temporary storage of material), subsection 512(c) establishes a safe harbor for "information residing on systems or networks at [the] direction of users" (which generally applies to websites that store information provided by users); and subsection 512(d) establishes a safe harbor for "information location tools" (such as links to content on other sites, typically applied to search engines).[191]

Subsections 512(a) and (b) will not apply to hyperlinking liability cases because these provisions limit remedies only with respect to infringements occurring "by reason of the provider's transmitting, routing, or providing connections for, material through a system or network," (§ 512(a)) "by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections," (§ 512(a)) or "by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider" (§ 512(b)). Additionally, because section 512(c) applies only to service providers who may be liable for infringement of copyright "by reason of the *storage . . . of material that resides on a system or network controlled or operated by or for the service provider,*" this provision may be equally unhelpful to defendants who are facing liability for linking to material stored on a third-party server.[192]

---

[187] Directive 2000/31, supra note 73.

[188] 17 U.S.C. § 512(a)--(d); S.Rep. No. 105-190 at 2 (1998). The safe harbor provisions passed with the DMCA are separately referred to as The Online Copyright Infringement Liability Limitation Act (OCILLA).

[189] S. Rep. 105-190, at 20 (1998).

[190] Id. at 40 ("The limitations in [§ 512] subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement.")

[191] See 17 U.S.C. § 512(a)--(d); Edward Lee, Decoding the DMCA Safe Harbors, 32 Colum. J.L. & Arts 233, 235 (2009).

[192] 17 U.S.C. § 512(c) (emphasis supplied). However, a defendant who both hyperlinks and engages in other functions which could fall under the other DMCA safe harbor provisions may claim the protection of multiple safe harbor provisions. 17 U.S.C. § 512(n); See also S. Rep. 105-90, at 55 ("Consider, for example, a service provider that provides a hyperlink to a site containing infringing material which it then caches on its system in order to facilitate access to it by its users. This service provider is engaging in at least three functions that may be subject to

Subsection 512(d), however, shields the service provider from awards of damages for copyright infringement "by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or *hyperlink text*."[193] When passing this provision, Congress noted that "information location tools are essential to the operation of the internet" because they enable users to "find the information they need."[194] The legislative history specifically refers to search engines and online directories like Yahoo! as examples of information location tools covered by the act, and noted that the "human judgment and editorial discretion exercised by [directory-based information location tools]" makes these services valuable.[195]

Very few cases in the U.S. have dealt with the applicability of the DMCA's safe harbor provisions to claims for copyright infringement based on hyperlinks, posted by the defendant, to copyrighted material. The majority of cases involving the § 512(d) safe harbor provision involve defendants who provide online platforms on which *users* post hyperlinks.[196] Most § 512(d) cases concerning defendants who themselves provided the links at issue involved defendants who operate search engines and online directories, similar to the actors contemplated in the DMCA's legislative history.[197] However, in a few instances, courts have applied § 512(d) to defendants who do not provide search engines or directories, but who instead simply provide a handful of hyperlinks to websites, some of which may have contained infringing material.[198]

---

the limitation on liability: transitory digital network communications under subsection (a), system caching under subsection (b), and information location tools under subsection (d).").

[193] 17 U.S.C. § 512(d).

[194] H.R. Rep. 105-551, at 58 (1998).

[195] Id. Some commentators have noted that this legislative history may support the argument that the application of § 512(d) is limited to providers of search engines or directories. Anjali Dalal, Protecting Hyperlinks and Preserving First Amendment Values on the Internet, 13 U. Pa. J. Const. L. 1017, 1072--73 (2011) (noting that the definition of "service provider" and the scope of § 512(d) is expansive, but the legislative history's specific discussion of online directories may be "somewhat more limiting"). But see Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1097--98 (C.D. Cal. 2004) (rejecting plaintiff's argument that § 512(d) is limited to websites "which provide links to millions of websites with whom it has no relationship," and acknowledging that § 512(d) could apply to a website which "merely links to a relatively small universe of websites with whom it has in place contractual relationships and established review procedures"), aff'd in part, rev'd in part and remanded, 481 F.3d 751 (9th Cir. 2007); Amy Blom, Search Engines and S 512(d) of the D.M.C.A., 1 Case W. Reserve J.L. Tech. & Internet 36, 44–45 (2009) ("Although large search engines and directories like Google or Yahoo! seem to be what Congress had in mind when it passed the law, this safe-harbor might apply even if a search engine hosts a small number of links and has some form of contractual relationship with linked third-party sites.").

[196] See, e.g. Totally Her Media, LLC v. BWP Media USA, Inc., No. CV1308379ABPLAX, 2015 WL 12659912 (C.D. Cal. Mar. 24, 2015) (holding that a defendant which provides a "web-based social media and community discussion forum" which "contains substantial amounts of user-generated content, including user-generated links to outside content" was protected from copyright liability under § 512(d)); Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1046--47 (9th Cir. 2013) (discussing and ultimately rejecting the § 512(d) safe harbor claim brought by the defendant who operated a torrent-based file sharing platform).

[197] See, e.g. Perfect 10, Inc. v. Google, Inc., No. CV 04–9484 AHM (SHx), 2010 WL 9479059, at *13 (C.D. Cal. July 26, 2010) (holding that Google was entitled to safe harbor under § 512(d) for a subset of the claims at issue, and was therefore partially shielded from liability for providing hyperlinks through its search engine to websites which hosted unauthorized copies of plaintiff's copyrighted works).

[198] See Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1083, 1097--98 (C.D. Cal. 2004) (applying § 512(d) safe harbor to a website that provides age verification services to adult websites by asking users who wish to visit

III.C.i. Basic Requirements for Qualification for DMCA Safe Harbor under § 512

Because the DMCA safe harbors provide affirmative defenses, the burden of proof is on the defendant to establish compliance with the statutory requirements for safe harbor qualification.[199] Several requirements apply to any party seeking to claim safe harbor under the DMCA.

First, the party must establish that it is a "service provider" as defined by the statute.[200] The statute defines the term "service provider" (for the purposes of § 512(b)--(d)) as "a provider of online services or network access, or the operator of facilities therefor."[201] This definition is "intended to encompass a broad set of Internet entities"[202] and most likely covers any website on the internet.[203]

Second, the party must have "adopted and reasonably implemented, and inform[ed] subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[204] This provision has three basic requirements: first, a service provider must "adopt a policy that provides for the termination of service access for repeat infringers," second, a service provider must "inform users of the service policy," and third, the service provider must "implement the policy in a reasonable manner."[205] The application of this "repeat infringer policy" requirement to hyperlinking cases is not clear. The statute protects service providers who offer platforms which other parties may use to infringe copyrighted works (i.e. video hosting platforms, to use a commonly litigated example). The repeat infringer policy seems designed specifically to ensure that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others" are informed by service providers that their access may be revoked if the infringing activity continues.[206]

The framework of the DMCA's "repeat offender policy" requirement seems inapplicable to a case in which a website seeks DMCA safe harbor to immunize itself from copyright liability for

---

those websites to verify their age and then providing those users with a link to websites which allegedly contained infringing material), aff'd in part, rev'd in part and remanded, 481 F.3d 751 (9th Cir. 2007); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1179--83 (C.D. Cal. 2002) (applying § 512(d) in a similar case, but denying safe harbor because of deficiencies in the defendant's compliance with the qualification requirements).

[199] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1039 (9th Cir. 2013); WPIX, Inc. v. ivi, Inc., 691 F.3d 275, 278 (2d Cir. 2012).

[200] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 500, 509 (S.D.N.Y. 2013).

[201] 17 U.S.C. § 512(k)(1)(B).

[202] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 39 (2d Cir. 2012).

[203] One court commented that the definition of "service provider" is so broad that the court "[had] trouble imagining the existence of an online service that would *not* fall under the definitions." In re Aimster Copyright Litig., 252 F.Supp.2d 634, 658 (N.D.Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003) (emphasis in original); also see Sam Bayard, Embedded Video and Copyright Infringement, Digital Media Law Project (Jul. 10, 2007), available at http://www.dmlp.org/blog/2007/sam-bayard/embedded-video-and-copyright-infringement ("The plain language of § 512(d) seems to provide bloggers and website operators who embed infringing video content with a means for avoiding liability.").

[204] 17 U.S.C. § 512(i)(1)(A).

[205] Wolk v. Kodak Imaging Network, Inc., 840 F.Supp.2d 724, 744 (S.D.N.Y. 2012).

[206] S. Rep. 105-190, at 52 (1998)

its provision of a link to a website with which the defendant does not have a pre-existing relationship. In such cases, there are no "subscribers or account holders" to "inform . . . of the service policy."[207] Courts have held that when a defendant is claiming DMCA safe harbor for a service which lacks "account holders or subscribers," simply providing proof that the defendant has a "system for receiving and processing notifications" is sufficient to meet the "repeat offender policy" requirement.[208] Thus, this requirement may not apply in full force to hyperlinking cases, as long as the defendant complies with the notice-and-takedown procedures for dealing with DMCA notifications.[209]

Third, the party must "not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works."[210] The statute defines "standard technical measures" as "technical measures" that "(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks."[211] However, as of 2017, this provision has not been used to disqualify a service provider from DMCA safe harbor because of the lack of a "broad consensus" regarding the definition of "standard technical measures."[212]

III.C.ii. Specific Requirements for Qualification for Safe Harbor under § 512(d)

Sections 512(c) and (d) of the DMCA impose additional qualification requirements on host and search engine service providers who seek safe harbor under those provisions. These provisions require that the service providers do not have actual or "red flag" knowledge of the infringing nature of the material to which the service provider facilitates or provides access, that the service providers do not "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity,"[213] and that

[207] 17 U.S.C. § 512(i)(1)(A), Wolk, 840 F.Supp.2d at 744.

[208] Perfect 10, Inc. v. Google, Inc., No. CV 04-9484 AHM (SHx), 2010 WL 9479059, at *4 (C.D. Cal. July 26, 2010) ("Google has provided evidence that it has a system for receiving and processing notifications . . . Moreover, Google points out . . . that [its] Web Search [and] Image Search [products] do not have account holders or subscribers, . . . and [plaintiff] does not content that Google must, or even can, have a repeat infringer policy for these services.").

[209] See supra discussion of 17 U.S.C. § 512(c)(3). Also see Miquel Peguera, When the Cached Link Is the Weakest Link: Search Engine Caches Under the Digital Millennium Copyright Act, 56 J. Copyright Soc'y U.S.A. 589, 614 (2009) (arguing that the § 512(d) "repeat offender policy" requirement may not apply to search engines which "lack . . . subscribers or account holders").

[210] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 500, 509 (S.D.N.Y. 2013); also see UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F.Supp.2d 1099, 1117 (C.D.Cal. 2009).

[211] 17 U.S.C. § 512(i)(2).

[212] See U.S. Copyright Office, Section 512 Study: Request for Additional Comments, 81 Fed. Reg. 78636, 78641 (Nov. 8, 2016) ("[S]ince passage of the DMCA, no standard technical measures have been adopted pursuant to section 512(i)."); Capitol Records LLC v. Vimeo, LLC, 972 F.Supp.2d 500, 517 (S.D.N.Y. 2013) (rejecting plaintiffs' argument that the defendant's privacy settings "prevent copyright owners from collecting information needed to issue a takedown notice" constitutes the failure to implement a 'standard technical measure' because privacy settings are not a "standard technical measure," and while privacy settings "may be relevant to other provisions of the DMCA . . . privacy settings do not constitute interference with standard technical measures").

[213] In the linking context, defendants will rarely have the "right and ability" to control the infringing activity of the unauthorized sites they link to. See Perfect 10 v. Amazon, 508 F.3d 1146, at 1173--74 (2007) (holding that Google's

the service provider complies with the notice-and-takedown procedures laid out in § 512(c) by "responding expeditiously to remove, or disable access to" material once that material is identified in a "notification of claimed infringement" provided to the service provider.[214]

Actual or "Red Flag" Knowledge Requirement --- Sections 512(c)(1)(A) and 512(d)(1) require that the defendant seeking safe harbor under § 512(c) or (d) prove the absence of actual or "red flag" knowledge of the infringing nature of the activity at issue.[215] The defendant "(A) [must] not have actual knowledge that the material or activity is infringing; (B) in the absence of such actual knowledge, [must not be] aware of facts or circumstances from which infringing activity is apparent [i.e. "red flag" knowledge]; or (C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material."[216] This provision parallels the analysis of affirmative liability under contributory liability analysis; at first blush, a defendant who possesses actual or constructive knowledge of the infringing nature of the facilitated activity would under contributory liability doctrine accordingly fail to qualify for the § 512(c)(1)(A) or § 512(d)(1) safe harbor.[217]

Courts construing the DMCA, however, have underscored a difference between common law standards of contributory liability and the statutory regime under the DMCA.[218] Importantly, the statutory language of the DMCA includes both "a subjective and an objective element" --- the defendant can be disqualified from the safe harbor if the plaintiff can show that the defendant had either "actual knowledge that the material or activity is infringing" (the subjective element) or "aware[ness] of facts or circumstances from which infringing activity is apparent" (the objective element).[219] The Second Circuit has clarified that "the actual knowledge provision

---

right to terminate a particular website's advertising contract "does not give Google the right to stop direct infringement" because "an infringing third-party website can continue to reproduce, display, and distribute its infringing copies of [plaintiff's] copyrighted works after its" contract with Google ended, and thus Google could not be found liable as a vicarious infringer). Therefore, this provision is not immediately relevant to our analysis.

[214] 17 U.S.C. § 512(c); Id. at § 512(d).

[215] 17 U.S.C. § 512(c)(1)(A); Id. at § 512(d)(1).

[216] Id.

[217] Some commentators have noted that "the threshold requirements for [DMCA] immunity closely track the traditional elements of secondary liability." Jane C. Ginsburg, Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs, 50 Ariz. L. Rev. 577, 591 (2008). See also Mark A. Lemley & R. Anthony Reese, Reducing Digital Copyright Infringement Without Restricting Innovation, 56 Stan. L. Rev. 1345, 1371--72 (2004) (noting that the DMCA's safe harbor provisions "essentially mirror[]" the tests for contributory and vicarious liability and therefore offer "little protection to innovators against secondary liability claims"). But see Amy Blom, Search Engines and S 512(d) of the D.M.C.A., 1 Case W. Reserve J.L. Tech. & Internet 36, 48–49 (2009) ("[F]or contributory infringement purposes, the 'fatal' knowledge imputed by courts might be a somewhat less stringent standard than the actual or constructive knowledge required for a search engine to lose its safe-harbor treatment under §§ 512(d)(1)(A-B).").

[218] See, e.g. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001) (rejecting the lower court's argument that the defendant's potential "liability for contributory and vicarious infringement renders the [safe harbor provisions of the] Digital Millennium Copyright Act inapplicable per se"); Lemley & Reese, supra, at 1372 n.102 ("The standard of knowledge that a provider must have to fall outside the protections of the safe harbor may be somewhat higher than the standard required in an ordinary action for contributory infringement, so the safe harbor may offer some incremental protection even against claims of contributory infringement.").

[219] 17 U.S.C. § 512(d); S. Rep. 105-190 at 44 (1998) ("The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag," the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those

turns on whether the provider actually 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was *subjectively aware* of facts that would have made specific infringement "objectively" obvious to a reasonable person."[220] However, under either standard, the plaintiff must prove that the defendant had subjective or objective knowledge of *specific* instances of infringement, rather than a mere "general awareness that there are infringements" --- courts have labeled this as the "specificity requirement."[221] Therefore, the DMCA standard may require plaintiffs to prove *more* than they would otherwise have to prove to meet the knowledge standard under contributory liability analysis. Rather than proving that defendant knew, *or should have known* of the facts and circumstances making infringement obvious, the plaintiff must prove actual, subjective knowledge of those facts and circumstances to disqualify a defendant from safe harbor under the DMCA's "red flag" knowledge standard. One commentator noted that, absent proof of subjective "actual" knowledge of infringing material, "[red flag] knowledge can never be found unless a plaintiff produces evidence which can demonstrate both the specificity of infringing material as well as a clear indication of the content's illicit nature."[222]

Courts also point to § 512(m), which bars courts from requiring that a service provider "monitor[] its service or affirmatively seek[] facts indicating infringing activity,"[223] to limit the grounds on which a defendant can be disqualified from § 512(c) safe harbor on the basis of "red flag" knowledge. Because of the explicit "no monitoring obligation" language in the DMCA, the protections of the DMCA safe harbor may be *broader* than the affirmative liability standard under contributory liability doctrine --- in other words, it may be possible for a defendant to qualify for safe harbor under § 512(c) or (d) even when that defendant might otherwise have been found liable for contributory infringement.

A comparison between the cases *A&M Records, Inc. v. Napster, Inc.*[224] and *Capitol Records, LLC v. Vimeo, LLC*[225] illustrates the differences between the contributory liability "knowledge" analysis and the § 512(c)/(d) "knowledge" analysis. In *A&M Records, Inc. v. Napster*, record companies and music publishers sued Napster, an internet service that allowed the peer-to-peer transmission of digital audio files. The court ruled that Napster had "both actual and

---

facts or circumstances constitute a "red flag"–in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances–an objective standard should be used.")

[220] Viacom Intern., Inc. v. Youtube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (emphasis supplied).

[221] Id. (quoting Viacom Intern. Inc. v. YouTube, 718 F.Supp.2d 514, 519 (S.D.N.Y. 2010). See also id. at 31 ("The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard."). Courts have noted that this "specificity requirement" can be implied from the removal provisions of the DMCA, which require providers to "act[] expeditiously to remove, or disable access to, the material" once learning of its infringing nature. See 17 U.S.C. § 512(c)(1)(A)(ii), § 512(d)(1)(C); Viacom Intern. Inc. v. YouTube, 676 F.3d 19, 30 (2d Cir. 2012) ("[T]he nature of the removal obligation itself contemplated knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove.").

[222] Methaya Sirichit, Catching the Conscience: An Analysis of the Knowledge Theory Under S 512(c)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags, 23 Alb. L.J. Sci. & Tech. 85, 141 (2013).

[223] 17 U.S.C. § 512(m)(1); see also Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 41 (2d Cir. 2012) ("[T]he safe harbor expressly disclaims any affirmative monitoring requirement --- except to the extent that such monitoring comprises a 'standard technical measure' within the meaning of § 512(i).").

[224] 239 F.3d 1004 (9th Cir. 2001).

[225] 826 F.3d 78 (2d Cir. 2016).

constructive" knowledge of the direct infringements that its platform enabled. The Ninth Circuit found that Napster had *actual* knowledge of direct infringement because (i) Napster maintained a directory of all the files shared on its system which gave it the ability to "learn of specific infringing material available on [its] system,"[226] and (ii) because several documents introduced to the record conclusively showed that Napster executives had been informed of some specific infringing files which were available on its system, and had full knowledge that its users were "exchanging pirated music."[227] The court further agreed with the lower court's finding that Napster had *constructive* knowledge of direct infringement, based on its observations that "(a) Napster executives have recording industry experience; (b) they have enforced intellectual property rights in other instances; (c) Napster executives have downloaded copyrighted songs from the system; and (d) they have promoted the site with 'screen shots listing infringing files.'"[228] In other words, knowledge that Napster executives were *generally* aware that mass infringement occurred on their platform, combined with Napster's clear ability to identify infringing activity through its central directory, was sufficient to support a claim of contributory liability.

In *Capitol Records, LLC v. Vimeo, LLC,* [229] a group of record companies and music publishers sued Vimeo, an online video sharing platform, asserting that Vimeo was hosting infringing content on its platform. Vimeo claimed safe harbor under § 512(c).[230] The plaintiffs had presented evidence that some of Vimeo's employees had watched and interacted with some videos which contained "all or substantially all" of recognizable copyrighted songs, and argued that this should disqualify Vimeo from § 512(c) safe harbor because the evidence established Vimeo's possession of "red flag" knowledge of the infringing content. The plaintiffs also presented evidence that Vimeo employees knew that many of the videos on the platform contained infringing content (this evidence was very similar to the evidence presented in the Napster case), and that Vimeo employees had, "in order to expand its business, actively encouraged users to post videos containing infringing material."[231] Lastly, the plaintiffs argued that Vimeo had monitored videos for infringement of visual content, but had declined to monitor its videos for infringement of audio content, which proved that Vimeo at least had the technical ability to identify specific infringing material.[232] The court rejected these arguments, and found that the evidence presented was insufficient to show that Vimeo was disqualified from claiming § 512(c) safe harbor. The court reasoned that § 512(m) "relieves the service provider of [the] obligation to monitor for infringement posted by users on its website," and thus Vimeo's "awareness of facts suggesting a likelihood of infringement" did not "requir[e] investigation merely because [Vimeo had] learn[ed] facts raising a *suspicion* of infringement."[233] The court's

[226] Napster, 239 F.3d at 1021.
[227] Id. at 1020 n.5 (quoting A&M Records, Inc. v. Napster, Inc. 114 F.Supp.2d 896, 918 (N.D. Cal. 2000)).
[228] Id.
[229] 826 F.3d 78 (2d Cir. 2016)
[230] Id. at 81.
[231] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 500, 524 (S.D.N.Y. 2013) (noting evidence that Vimeo employees had sent emails internally indicating that the company "[i]gnor[es]" the fact that many videos on the platform use copyrighted material, and noting that another employee had responded to a question regarding Vimeo's copyright policy by telling a user "[d]on't ask, don't tell ;)").
[232] Capitol Records, LLC v. Vimeo, 826 F.3d at 98.
[233] Id. at 98. Also see UMG Recordings, Inc. v. Veoh Networks, Inc. 665 F.Supp.2d 1099, 1108 (C.D. Cal. 2009) ("[I]f investigation of 'facts and circumstances' is required to identify material as infringing, then those facts and circumstances are not 'red flags.'").

decision was primarily motivated by a concern that, when designing the DMCA safe harbor provisions, Congress had intended to "[p]rotect[] service providers from the expense of monitoring" for infringing content."[234]

Therefore, evidence that may be sufficient to support an argument of "actual or constructive knowledge" for contributory infringement purposes may be *insufficient* to disqualify a defendant from claiming the protections of DMCA safe harbor on the basis of actual or "red flag" knowledge. In both *Napster* and *Vimeo*, the plaintiffs had presented evidence which established (i) that the defendant had at least some *general* knowledge that infringement occurred on its platform,[235] and (ii) that the defendant had the ability to identify infringing content and remove it. However, while this evidence was sufficient to support a finding of affirmative liability in *Napster*, the evidence was insufficient to support a finding that the defendant was disqualified from seeking the protections of DMCA safe harbor in *Vimeo*. Thus, at least with respect to the knowledge requirement, the protections provided to service providers under the DMCA seem to be broader than the defenses to allegations of liability for contributory copyright infringement.

Two recent developments in DMCA case law may, however, signal that courts are retreating from this broad reading of the safe harbor provisions. First, in *Viacom v. Youtube*, the Second Circuit recognized that plaintiffs may meet the disqualifying "knowledge" standard under the DMCA through arguments based on the doctrine of willful blindness.[236] Despite the absence of any mention of willful blindness in the DMCA's statutory language, the court ruled that a defendant who becomes "aware of a high probability of [its facilitation of infringement] and consciously avoided confirming that fact" may be disqualified from DMCA safe harbor under the actual or red flag knowledge provisions.[237] Because willful blindness is a "proxy for knowledge," willful blindness must too relate to "specific infringements" --- in other words, willful blindness of facts that would lead a reasonable observer to have a generalized knowledge of infringement will not suffice to disqualify a party from DMCA safe harbor.[238]

Plaintiffs may thus be able to "avoid difficulties in proving apparent knowledge" by simply proving that the defendants were aware of the high probability of the infringing nature of a *specific* facilitated act, and deliberately avoided learning additional facts which could have

[234] Id.

[235] In another case, plaintiff's evidence that showed that 75-80% of all videos on defendant's platform contained copyrighted material, and that "defendants were conscious that significant quantities of material on [their] website were infringing" did not suffice, standing alone, to prove that the defendant "actually knew, or was aware of facts or circumstances that would indicate, the existence of particular instances of infringement" for the purposes of § 512(c) eligibility analysis. See Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 33 (2d Cir. 2012).

[236] Viacom Intern., Inc. v. Youtube, Inc., 676 F.3d 19, 35 (2d Cir. 2012).

[237] Id. See also UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F.Supp.2d 1099 at *7. The doctrine of willful blindness may have roots in the DMCA's legislative history. See H.R. Rep. 105--551(II) at 57 (1998) (noting that a service provider would not qualify for safe harbor "if it had turned a blind eye to 'red flags' of obvious infringement"); Columbia Pictures Inds. V. Fund, 2009 WL 6355911, at *17 (quoting this language in order to find that the defendant was disqualified from DMCA safe harbor because he had overlooked facts which would have made specific instances of infringement apparent).

[238] Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 78, 99 (2d Cir. 2016) (quoting Viacom Intern., Inc. v. Youtube, Inc., 676 F.3d 19, 34--35 (2d Cir. 2012).

confirmed the infringing nature of that act.[239] Notably, the concept underlying willful blindness may cut against a broad application of the principle that the service provider should *never* be under any obligation to investigate specific acts of infringement, based on § 512(m) of the DMCA.[240] Accordingly, courts have applied the willful blindness doctrine conservatively. For example, in *Capitol Records, LLC v. Vimeo, LLC,* the Second Circuit refused to apply the doctrine of willful blindness to a defendant who had shown the ability to monitor its platform for infringing content, but declined to monitor in a way which would reveal infringements of plaintiff's copyrights, even though the plaintiffs had presented evidence that proved that the defendant was generally aware that its acts facilitated copyright infringement.[241]

Second, recent case law suggests that in some circumstances, service providers may in fact have affirmative obligations to monitor for infringing activity --- and that the "no monitoring obligations" language in § 512(m) of the DMCA forbids the imposition only of *general* duties to monitor."[242] In *EMI Christian Music Group, Inc. v. MP3tunes, LLC,* a copyright holder had produced evidence which showed that defendants, who operated an online music service on which users posted links to mp3 files, knew (i) that their service allowed users to share mp3 versions of Beatles songs, and (ii) that "there had been no *legal* online distribution of Beatles tracks before 2010."[243] The Second Circuit concluded that the jury below was "permitted to conclude that [defendants had] a time-limited, targeting duty --- even if encompassing a large number of songs," and implied that only an "amorphous" duty to monitor constituted a "contravention of the DMCA['s § 512(m) provision]."[244] Notably, the Second Circuit also paid particular attention to the observation that implementing this "time-limited, targeted duty" would be relatively easy for the defendant: the "design of the service's indexing feature, coupled with the readily ascertainable and searchable nature of certain categories of infringing material" meant that the imposition of a limited monitoring duty would not be overly burdensome.[245]

While these recent developments may imply that courts are reconsidering their initially broad interpretations of the DMCA safe harbor provisions, the "no monitoring obligation" provision (§ 512(m)) may stunt the reach of the novel approaches based on "willful blindness" and "time-limited, targeted dut[ies]". Therefore, while there is significant doctrinal uncertainty surrounding

[239] Methaya Sirichit, Catching the Conscience: An Analysis of the Knowledge Theory Under S 512(c)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags, 23 Alb. L.J. Sci. & Tech. 85, 154 (2013).

[240] See, e.g. Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012) (noting the tension between willful blindness doctrine and § 512(m), and stating that while § 512(m) is "incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring," willful blindness doctrine does not necessarily impose "an affirmative duty to monitor" and thus § 512(m) does not prevent a narrow application of the willful blindness doctrine to DMCA cases).

[241] Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 78, 98 (2d Cir. 2016).

[242] EMI Christian Music Group, Inc. v. MP3tunes, LLC, 844 F.3d 79, 93 (2d Cir. 2016) (emphasis supplied).

[243] Id.

[244] Id. This logic has been used to find that a service provider who ran a platform which enabled users to upload photographs, after receiving take down notices identifying specific infringing photographs, had a targeted duty to monitor for other "substantially similar or readily identifiable" copies of those photographs uploaded by other users after the initial infringing images were taken down. Venus Fashions, Inc. v. ContextLogic, Inc.No. 3:16-cv-907-J-39MCR, 2017 WL 2901695, at *27 (M.D. Fla. Jan. 18 2017) (citing EMI Christian Music Group, 844 F.2d at 93).

[245] Randi W. Singer & Jonathan Bloom, Second Circuit Examines Limits of DMCA Safe-Harbor Protection, 29 Intell. Prop. & Tech. L.J. 3, 7 (2017); EMI Christian Music Group, Inc. v. MP3tunes, LLC, 844 F.3d 79, at 93 ("[T]here was evidence at trial that MP3tunes could disable access. Indeed, an expert testified that searching through libraries of MP3 songs was a common function of MP3tunes's business.").

this issue, when a defendant is not actually aware of the infringing nature of the facilitated activity, is not aware of "facts making [a *specific* instance of] infringement *obvious*,"[246] and does not consciously avoid acquiring knowledge of these facts, a plaintiff will most likely fail to disqualify the defendant from DMCA safe harbor based on the knowledge provisions. In other words, a defendant who has only *general* knowledge that its actions facilitate infringement, and who declines to implement its ability to identify and remove specific infringing content may still qualify for DMCA safe harbor, even though that defendant may have otherwise been found liable under affirmative contributory liability doctrine.[247]

Thus, in the hyperlinking context, the analysis of a defendant's knowledge of the infringing nature of the linked-to source may be more defendant-friendly under the DMCA safe harbor analysis than under general principles of contributory liability. Because the DMCA case law establishes that the defendant is required to investigate whether a particular facilitated act is illicit only when it learns of "facts making infringement *obvious*" (rather than when it learns of facts that "rais[e] a *suspicion* of infringement"), it may be relatively easy for a defendant-linker to claim the benefits of the § 512(d) safe harbor as long as the defendant does not know of the infringing nature of the linked-to source, and does not possess knowledge of (nor is willfully blind to) facts or circumstances which would make the infringing nature of the linked-to source obvious to a "reasonable person."

Moreover, the legislative history of § 512(d) indicates that courts should be particularly careful when assuming the existence of "red flag" knowledge for the purposes of determining whether a defendant qualifies for the "information location tools" safe harbor under the DMCA. The House Report which accompanied the DMCA clarified that "[t]he knowledge or awareness standard [contained in § 512(d)] should not be applied in a manner which would create a disincentive to the development of directories which involve human intervention" and that "[a]bsent actual knowledge, awareness of infringement as provided in [§ 512(d)] should typically be imputed to a directory provider only with respect to pirate sites or in similarly obvious and conspicuous circumstances, and not simply because the provider viewed an infringing site during the course of assembling the directory."[248]

Compliance with Notice-and-Takedown Procedures --- To qualify for § 512(d) safe harbor, a party must also comply with the notice-and-takedown procedures laid out in § 512(c)(3).[249] After receiving a proper notice from a copyright holder, the party seeking safe harbor must "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[250] In order for a notice to be proper, the notice must meet the detailed statutory requirements of § 512(c)(3)(A)(i), (iv)-(vi),[251] "identif[y] . . . the reference

[246] Capitol Records, LLC v. Vimeo, LLC, 826 F.3d 78, 98 (2d Cir. 2016).
[247] See, e.g. supra discussion of Capitol Records, LLC v. Vimeo, LL, 826 F.3d 78 (2d Cir. 2016) and A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).
[248] H.R. Rep. 105--551, at 58 (1998).
[249] 17 U.S.C. § 512(d)(3) (requiring compliance with the notice-and-takedown procedures laid out in § 512(c)(3)).
[250] Id. The statute does not define "expeditiously" and Congress noted in the DMCA legislative history that "[b]ecause the factual circumstances and technical parameters may vary from case to case, it is not possible to identify a uniform time limit for expeditious action." See S. Rep. No. 105–190, at 44 (1998).
[251] Id. at § 512(c)(3)(A)(i), (iv)-(vi) (requiring the notice to include a signature, contact information of the copyright holder or its agent, a statement of "good faith belief that use of the material in the manner complained of is not

or link" at issue, and provide "information reasonably sufficient to permit the service provider to locate that reference or link."[252] A notice that complies "substantially" with these requirements may suffice to give the defendant "knowledge" of the work, thus disqualifying it from the safe harbor if it does not remove the material at issue.[253] While the § 512(c) safe harbor provision requires the party seeking safe harbor to designate an agent "to receive notifications of claimed infringement," § 512(d) does not require designation of an agent.[254]

After the service provider receives the notice and "remove[s], or disable[s] access to" the identified link, § 512(g) sets out a procedure through which the service provider may be required to replace the removed or disabled link.[255] While § 512(g) refers to § 512(c) and not § 512(d), courts have held that § 512(g) applies in equal force to takedown procedures under § 512(d).[256]

However, it is unclear how the replacement procedures set out in § 512(g) apply to § 512(d) defendants who do not have a pre-existing service relationship with a "subscriber[] or account holder[]." § 512(g) requires that the service provider "takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material," and then allows the "subscriber" to send a counter-notification which will require the service provider to restore access to the removed or disabled work within 10-14 days.[257] However, as noted above, a defendant facing a claim for infringement for a link that the defendant itself provided may not have "subscribers or account holders" to notify of the removal of the particular link.[258] For example, search engines and online directories seeking the § 512(d) safe harbor (which, by some measures, elicit the majority of all DMCA takedown notices[259]) may not have a pre-existing service relationship with the sites to which they link, and thus may not have an accessible way to

---

authorized," and a "statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the [copyright holder]").

[252] Id. at § 512(d).

[253] Id. at § 512(c)(3)(B).

[254] Id. at § 512(c)(2). This might not be clear from the statutory language --- § 512(d) incorporates § 512(c)(3), which does refer to a "designated agent." See Id. at § 512(c)(3)(B)(ii) (referring to "the service provider's *designated agent*"). However, the Copyright Office takes the position that only parties seeking safe harbor under § 512(c) need to designate an agent. See U.S. Copyright Office, Section 512 Study: Notice and Request for Public Comment, 80 FR 81862, 81868 (Dec. 31, 2015) ("A service provider seeking to avail itself of the section 512(c) safe harbor for user-posted content is further required to designate an agent to receive notifications of claimed infringement.").

[255] See 17 U.S.C. § 512(g).

[256] See, e.g., Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1179 (C.D.Cal.2002).

[257] 17 U.S.C. § 512(g)(2)--(3).

[258] In some cases, courts have implemented § 512(g) in the context of a hyperlink provider who is in privity with the websites to which the hyperlinks lead. For example Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1180 (C.D. Cal. 2002), the court examined the defendant's compliance with § 512(g) by examining the procedure through which the defendant would restore a removed link. The defendant in that case was an age-verification service for adult websites, and the court considered defendant's client websites as the "subscribers" for the purposes of determining whether the defendant had followed the counter-notification and put-back procedures in § 512(g). However, not all providers of hyperlinks will have a relationship with the linked-to source site, and therefore in some § 512(d) cases there may be no "subscriber" to which the defendant must send a notification that the link has been removed.

[259] Jennifer M. Urban & Laura Quilter, Efficient Process of "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act, 22 Santa Clara Computer & High Tech L.J. 621, 644 (2006) (noting that 59% of the DMCA notices studied from the "Chilling Effects" database were § 512(d) notices sent to search engines, requesting removal of a webpage from search results).

"notify" a website that it has removed a link after receiving a takedown notice.[260] Without a mechanism to notify the affected websites, the DMCA's "counter-notification and put-back" procedure, which was designed as procedural protection for alleged infringers who may be adversely affected by inappropriate or abusive takedown requests, may not operate effectively in the context of many § 512(d) service providers.[261]

Google claims that, after removing content from its search engine due to a takedown notice, it "notif[ies] the administrator of the affected site through Google's Search Console."[262] However, not all website administrators whose websites are included in Google's search results utilize the "Search Console" service, which is an opt-in analytics product.[263] The Lumen removals database, a project of Harvard's Berkman Klein Center for Internet & Society, provides a creative solution to this problem: search engines can forward takedown notices to Lumen, which publishes these notices online and provides a simple way for website owners to file DMCA counter-notifications.[264] Search engines can respond to a takedown notice by breaking the link to the allegedly infringing website, and redirecting that link directly to the page on the Lumen website on which the publication of the relevant take-down notice appears.[265] Through this process, even though a website operator may not be affirmatively notified that her link has been removed due to a takedown notice, the website operator may quickly learn of the removal and have an opportunity to respond after searching for her own site on a search engine.

[260] Id. at 626 ("As search providers likely have no service relationship with the alleged infringer, they rarely have the ability to notify . . . . Links to complained-of material are thus typically removed from the search engine's index based only on the copyright holder's takedown notice, without any notice to the target or other process.").

[261] Id. at 628 (referring to the counter-notification and put-back procedures as an "important procedural protection"); Id. at 684 (noting the "troubling" use of questionable takedown notices by website operators against their competitors, and describing this practice as a "new weapon in the search-rank wars").

[262] Transparency Report: Requests to Remove Content Due to Copyright, Google (last visited Oct. 12, 2017), available at https://transparencyreport.google.com/copyright/overview. ("When we take action in response to a copyright notice, we notify the administrator of the affected site through Google's Search Console. Following DMCA process, a webmaster may issue a counter notification. If they believe the content is not infringing or that a notice has been filed in error, the administrator of an affected site or the provider of affected content may also file a counter notification.").

[263] Search Console Help: What is Search Console?, Google (last visited Oct. 12, 2017), available at https://support.google.com/webmasters/answer/4559176?hl=en ("Google Search Console is a free service offered by Google that helps you monitor and maintain your site's presence in Google Search results. You don't have to sign up for Search Console for your site to be included in Google's search results, but doing so can help you understand how Google views your site and optimize its performance in search results.").

[264] Transparency Report: Requests to Remove Content Due to Copyright, Google (last visited Oct. 12, 2017), available at https://transparencyreport.google.com/copyright/overview ("Lumen is a project of Harvard's Berkman Klein Center for Internet & Society. Lumen works with a variety of international research partners to offer information about the global landscape of Internet takedown requests. Lumen posts and analyzes different kinds of requests to remove material from the Internet, including requests based on copyright claims."); See, e.g. Websearch Infringement Notification via Online Form Complaint, Lumen Database (last visited Oct. 12, 2017), available at https://lumendatabase.org/notices/1151854 (publication of a takedown notice sent to Google requesting removal of several "allegedly infringing URLs" and inviting the owner of those URLs to "[c]reate DMCA Counter Notice").

[265] Id. ("When it is possible to do so legally, Google links from search results to the requests published by Lumen in place of removed content.")

Some commentators have concluded that § 512(d) does not require the service provider to notify targets of the take-down.[266] While this conclusion is not clear from the statutory language, this interpretation seems consistent with the approach some courts have followed when interpreting the § 512(i) "repeat infringer policy" requirement as applied to service providers who could not implement it because of their lack of "subscribers and account holders."[267] Nonetheless, the awkwardness of applying the full notice--takedown--put-back framework to some § 512(d) contexts raises concerns about the adequacy and effectiveness of the DMCA's procedural protections for the spectrum of online participants who may be adversely affected by abuse of the takedown procedures. The counter-notification and put-back procedures may work appropriately for § 512(d) service providers who crowd-source links (i.e. sites which invite users to post links) or search engines who have a service relationship with the websites to which they link (i.e. Google and its means of communicating with linked websites through the Google Search Console tool). However, to preserve eligibility for the § 512(d) safe harbor, websites which simply post links to content on other websites may be forced to take down links in response to takedown notices, and may not be able to take advantage of the DMCA's put-back procedures because of the lack of a pre-existing service relationship with the sites to which they link.[268]

PART IV: COMPARATIVE AND INTERNATIONAL LAW PERSPECTIVES ON U.S. AND E.U. HYPERLINKING LAW

IV.A. Consistency of notice-and-takedown regimes with international norms

[266] Dena Chen, Musetta Durkee, Jared Friend & Jennifer Urban, Public Knowledge, Updating 17 U.S.C. § 512's Notice and Takedown Procedure for Innovators, Creators, and Consumers (March 31, 2011), available at https://www.law.berkeley.edu/wp-content/uploads/2015/04/cranoticetakedown.pdf ("[S]ervice providers providing information location services, defined in § 512(d) . . . are not required to notify targets that their material is being taken down in order to maintain safe harbor protection."); Urban & Quilter, supra, at 628 ("One important protection for subscribers is receiving notice of the copyright holder's complaint, which is afforded only to Internet subscribers of hosting services under § 512(c), and not to beneficiaries or subscribers of other regulated services, such as § 512(d) search services or § 512(a) Internet access providers."). These commentators apparently base this conclusion on the absence of any requirement in § 512(d) for the service provider to "notify targets that their material is being taken down." It is true that § 512(d) does not include this requirement, but the absence of such a provision may not mean that § 512(d) service providers are entirely exempt from this requirement --- the requirement to "take reasonable steps promptly to notify the subscriber that it has removed disabled access to the material" comes from § 512(g) and similarly does not appear in § 512(c).

[267] Perfect 10, Inc. v. Google, Inc., No. CV 04-9484 AHM (SHx), 2010 WL 9479059, at *4 (C.D. Cal. July 26, 2010) ("Google has provided evidence that it has a system for receiving and processing notifications . . . Moreover, Google points out . . . that [its] Web Search [and] Image Search [products] do not have account holders or subscribers, . . . and [plaintiff] does not content that Google must, or even can, have a repeat infringer policy for these services.").

[268] While it is true that the linking service provider could simply refuse to take down the link after receiving a takedown notice, such a refusal may disqualify the service provider from § 512(d) because that provision requires the service provider to "respond[] expeditiously to remove" the infringing link "upon notification of claimed infringement." 17 U.S.C. § 512(d)(3). Therefore, if the service provider refuses to take down a link and is subsequently sued by the copyright holder, the service provider would have to defend itself against a claim of secondary infringement without the protections of the § 512(d) safe harbor. Because the conditions for qualifying for safe harbor may be more defendant-friendly than the conditions for escaping affirmative liability under contributory infringement doctrine, see supra note 188 and accompanying text, this may disadvantage defendants who refuse to remove allegedly infringing links after receiving a valid takedown notice.

An initial question inquires "which international norms"? Should service provider liability limitation regimes be treated as exceptions whose consistency with international norms would be analyzed under the three-step test on which WCT art. 10 and TRIPS art. 13 condition conformity or national legislation to international norms?[269] Or should they be considered a matter of remedies, whose contours Berne art. 5(2), by providing that "the means of redress afforded to the author to protect his rights, shall be governed exclusively by the laws of the country where protection is claimed," leaves to member state determination? Classifying these regimes as exceptions may condemn them to conflict with international norms because it is difficult to see how a regime that applies to all copyrighted works could be characterized as limited to "certain special cases" (step one of the three-step test).[270] The WTO dispute resolution panel interpreting the first step has stated that "an exception or limitation should be narrow in quantitative as well as a qualitative sense" and "a limitation or exception in national legislation should be clearly defined and should be narrow in its scope and reach."[271] Service provider liability limitations may be "clearly defined" in that they cover all copyrighted works, but by the same token their reach is extremely broad. If, as the WTO Panel held,[272] an exception that does not pass the first step will fail the test as a whole, an exception that exceeds the scope of the first step is fatally flawed.

To avoid this result, one might interpret the first step to accommodate application of an exception to a broad class of works, so long as the purpose of the exception were very constricted, but given the significance of internet communications, a purpose of immunizing service providers from liability does not seem very narrow, either. On the other hand, the specific prerequisites to the immunity might be deemed sufficiently to narrow the uses subject to the exemption. Failing acceptance of that limiting construction, another way to salvage service provider liability limitations would reject the WTO Panel's seriatim approach to the three-step test ("Failure to comply with any one of the three conditions results in the Article 13 exception being disallowed"), and balance all steps into a general inquiry into market harm and social benefit.[273] This approach essentially ignores the tripartite treaty formulation, as well as the treaty

[269] See WCT, supra note 6, art. 10 ("(1) Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author."); Agreement on Trade-Related Aspects of Intellectual Property Rights Apr. 15, 1994, 33 I.L.M. 81, 93 (1994) art. 13 [hereinafter TRIPS] ("Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder.").

[270] See id.

[271] WTO Panel, WT/DS160/R – 15 June 2000 United States – Section 110(5) of the U.S. Copyright Act Report of the Panel, ¶¶ 6.109, 6.112.

[272] Id. para. 6/97: "The three conditions apply on a cumulative basis, each being a separate and independent requirement that must be satisfied. Failure to comply with any one of the three conditions results in the Article 13 exception being disallowed."

[273] Much has been written on competing approaches to the three-step test. See generally, Christophe Geiger et al., Declaration: A Balanced Interpretation of the "Three-Step Test" in Copyright Law, 39 Int'l Rev. Intell. Prop. & Competition L. 707 (2008) (arguing that the three-step test "should be interpreted so as to ensure a proper and balanced application of limitations and exceptions"); Wittem Group, European Copyright Code at Art. 5.5 (proposing an alternate approach based allowing exceptions "provided that the corresponding requirements of the relevant limitation are met and the use does not conflict with the normal exploitation of the work and does not

command that exceptions and limitations should be "confined,"[274] but has the "advantage" of creating a standard so vague that service provider liability limitations of the kind we have seen might conceivably pass muster. Even an approach that melds the three steps into one, or balances them against each other, might nonetheless prove dubious in the case of deep and in-line links because these may well conflict with a normal exploitation of the work by substituting the linker's advertising for a lawful source page's advertisements. Moreover, because the service provider will not be liable in damages, there is no remuneration right to compensate for the use under the third step.

The U.S. approach appears more compatible than the EU's with international norms because section 512 does not contest the existence of direct or indirect liability of service providers for copyright infringement, rather it narrows the remedies available against infringing service providers to injunctive relief. The exclusion of damages against service providers arguably comes within the leeway Berne allows member states. While the Berne Convention specifies minimum remedies only with respect to infringing importation,[275] the TRIPS Accord, art. 45(1), requires member states to provide damages remedies for infringement of intellectual property rights, but only if the infringer knew or "had reasonable grounds to know" of the infringement.[276] Since the section 512 safe harbors apply only to linkers who neither knew nor had "red flag" knowledge of infringement, TRIPS would not require awards of damages in the case of copyright infringement by reason of the acts covered by the limitation on remedies.[277] By contrast, where TRIPS does mandate the availability of a damages remedy, that is, when the defendant had actual or constructive knowledge of the infringement, damages against the service provider remain available under US law.

The US safe harbors thus may well fit within the Berne scheme, while the EU regime, as a system of exceptions from liability rather than limitations on remedies, might not. But since the EU regime largely operates like the US regime, providing for de facto private injunctions through the notice and takedown procedure, and for judicial injunctions by virtue of art. 8(3) of the Information Society Directive, condemning one while upholding the other seems an exercise

---

unreasonably prejudice the legitimate interests of the author or rightholder, taking account of the legitimate interests of third parties"); Martin Senftleben, Copyright, Limitations and the Three-Step Test (2004).

[274] See WCT, supra note 6, art 10, TRIPS art. 13 ("Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder.")

[275] Berne Convention, supra note 2, art. 16.

[276] TRIPS, supra note 269, art. 45(1): "1. The judicial authorities shall have the authority to order the infringer to pay the right holder damages adequate to compensate for the injury the right holder has suffered because of an infringement of that person's intellectual property right by an infringer who knowingly, or with reasonable grounds to know, engaged in infringing activity." Commentators have interpreted this provision to require "[k]nowledge (or reasonable grounds to know) by the infringer *that the activity was infringing . . . ."* Daniel Gervais, The TRIPS Agreement: Drafting History and Analysis 582 (4th ed. 2012) (interpreting TRIPS art. 45(1)) (emphasis supplied); Sascha Vander, Commentary on TRIPS Article 45 at 720, *in* WTO---Trade-Related Aspects of Intellectual Property Rights (Peter-Tobias Stoll, Jan Busche & Katrin Arend, eds. 2009) (interpreting the knowledge provision in TRIPS art. 45 to mean "knowledge or reasonable grounds to know . . . that the activity was infringing" and noting that in most circumstances, knowledge can be "assumed . . . where offences have been committed by the infringer after having received a warning from the right holder").

[277] Arguably "reasonable grounds to know" would encompass a greater range of actors than those with "red flag" knowledge as currently interpreted by US courts, but US courts in the future might interpret that standard harmoniously with the international norm.

in pure formalism. Perhaps the EU provisions, albeit labeled as prerequisites to non-liability, would better be conceptualized as limitations on remedies, and treated functionally as "means of redress" falling under art. 5(2) rather than the three-step test for exceptions.

Alternatively, one might revisit the permissible contours of exceptions and limitations. If the three-step test constrains the scope of exceptions to Berne-WCT-TRIPS minimum rights, it becomes necessary to consider the Berne-WCT-TRIPS minimum remedies accompanying those rights. Putting together the relevant provisions, TRIPS obliges member states to protect the right of communication to the public,[278] and requires availability of injunctive relief,[279] but mandates availability of monetary relief only if the infringer knowingly engaged in the infringing activity. In other words, TRIPS allows, but does not compel, member states to afford a damages remedy to innocent infringers of the right of communication to the public.[280] It is therefore possible to argue that the eCommerce Directive's liability limitation provisions, read together with the Information Society Directive's imposition of injunctive relief against intermediary service providers, are not an exception or limitation at all under TRIPS art 13, because the EU texts do not in fact derogate from an international obligation.

IV.B. Comparison of EU and US rules on liability for hyperlinking

IV.B.i. Lack of liability for linking to an authorized public source

Both the U.S. and the E.U. regimes generally preclude liability for hyperlinking to an *authorized* source on the internet. In *Svensson,* the CJEU held that even though hyperlinks are a "making available" and thus a "communication to the public," a hyperlink that merely offers to *re-*communicate a work from a source authorized by the rightholder which has made the work available to all internet users (i.e. without technical restrictions or paywalls) is not "covered by the concept of 'communication to the public', within the meaning of Article 3(1) of Directive

[278] TRIPS, supra note 269, art. 9 (mandating compliance with Berne Convention arts. 1-21). To the extent the WCT making available right institutes prerogatives that go beyond the Berne communication to the public right, rather than merely clarifying the pre-existing scope of the communication to the public right, TRIPS might not require the provision of monetary or injunctive relief in the event of a violation of a Berne+ right. On the other hand, art. 19 of Berne, which TRIPS does incorporate, requires member States to extend to works from other Berne member States any greater protection the country of protection provides. Arguably, TRIPS minimum remedies could apply to violations of Berne+ rights through the back door of art. 19.

[279] Id. art 44.

[280] TRIPS mandates no remedies for violations of the right of communication to the public beyond the scope of that right as articulated in the 1971 Paris text. The right of making available was introduced in the 1996 WIPO Copyright treaties, which post-date TRIPS. If the making available right is a "new" right, then it falls outside TRIPS. Whether the right is in fact "new," or rather a clarification of the pre-existing Berne right, is a matter of some controversy. See
Reinbothe & Von Lewinski, supra note 7, at 127 (noting that "the making available right was considered to be an aspect of the communication right"); Silke von Lewinski, International Copyright Law & Policy 458 (2008) ("Under the WCT, the right of making available has been made a part of the right of communication to the public."); see generally Jane C. Ginsburg, "The (New?) Right of Making Available", *in* Intellectual Property In The New Millennium: Essays In Honour Of William R. Cornish 234, 246 (Cambridge U. Press, 2004), available at http://lsr.nellco.org/columbia/pllt/papers/0478 (concluding that "[t]he core concept of 'making available,' . . . can fairly be called neither a reaffirmation nor a novelty," because it resolves ambiguities surrounding the Berne communication to the public right).

2001/29,"[281] because it does not make the work available to a public the rightholder did not take into account in the initial authorized communication. The CJEU expanded this "new public" principle to in-line links in *BestWater Int'l GmBH v. Michael Mebes*.[282] Therefore, any hyperlink to a site on which a copyrighted work has been published with proper authorization cannot constitute an actionable "communication to the public" because such a hyperlink does not communicate the work to a "new public."

Similarly, after *Perfect 10 v. Amazon* and the widespread adoption of the "server rule" in the U.S., courts are likely to reject copyright holders' claims that a link to an authorized publication of their work constitutes a violation of her rights under § 106 of the Copyright Act.[283] Under the "server rule," a hyperlink of any type cannot constitute a direct infringement of copyright unless the linker "store[s] and serve[s]" the copyrighted work from its own server --- any liability for linking would be a matter of secondary infringement.[284] But because those claims require an underlying act of direct infringement,[285] a secondary infringement claim based on a hyperlink to an authorized source will fail.[286]

The two regimes reach the result through different reasoning, but the result seems to reflect widespread concerns about the adverse consequences of imposing copyright liability on actors who innocently link to authorized content on the internet, and to reflect a broader recognition of the importance of hyperlinks to the functioning of the internet as a whole.[287] On the other hand, this result raises the concern that copyright holders who make their works available on the internet without technical restrictions may lose control of how their works are presented and disseminated.[288]

IV.B.ii. Liability for providing a link v. Liability for facilitating actual access through a link?

In the E.U., the CJEU's construction of the "making available" right[289] establishes that an actor incurs liability for a "communication to the public" simply by offering the public access to a

[281] Case C-466/12, *Svensson v. Retriever Sverige AB* (13 Feb. 2014) at ¶. 24, http://curia.europa.eu/juris/document/document.jsf?text=&docid=147847&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141.

[282] Case C-348/13, BestWater Int'l GmBH v. Michael Mebes (21 Oct. 2014), http://curia.europa.eu/juris/liste.jsf?num=C-348/13.

[283] Perfect 10 v. Amazon, 508 F.3d 1146, 1159 (9th Cir. 2007).

[284] Perfect 10 v. Google, 416 F.Supp.2d 828, 843--45 (C.D. Cal. 2006).

[285] See, e.g., La Resolana Architects, PA v. Reno, Inc., 555 F.3d 1171, 1181 (10th Cir. 2009) ("[B]oth contributory and vicarious infringements require someone to have directly infringed the copyright."); Perfect 10, Inc. v. Amazon.com, Inc., 608 F.3d 1146, 1169 (9th Cir. 2007).

[286] See supra notes 156--157 and accompanying text (explaining this point, and noting that some U.S. plaintiffs have made the unsuccessful argument that by enabling an automatic download of a copyrighted work to a user's computer from an authorized source website, a link to an authorized source does enable an act of direct infringement).

[287] See supra notes 139--141 and accompanying text (noting the importance of the principle of "universal free linking"); Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016) at ¶ 31, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141 (noting the importance of finding a "a fair balance between, on one hand, the interests of copyright holders . . . and, on the other, the protection of the interests and fundamental rights of users of protected objects, in particular their freedom of expression and of information, . . . and of the general interest.").

[288] See supra notes 143--145 and accompanying text (discussing these concerns).

[289] Directive 2001/29, supra note 21.

work --- a copyright holder need not prove that any member of the public in fact accessed the work. By contrast, while the weight of authority in the U.S. indicates that a violation of the § 106 public performance or display rights may require only an "offer" to perform or display a work,[290] some U.S. case law indicates that a violation of the distribution right might require proof of an actual transfer of a work; a mere "offer" to transfer a copy of the work (that is, making the work available for downloading) may not suffice without additional proof of actual downloads.[291]

The following scenario illustrates the difference between liability for offering downloads and liability for actual downloads. Were it necessary to prove actual downloads, then a U.S. copyright holder who brings a claim of secondary infringement on the basis of a link to an unauthorized source of a work would need to show completed acts at both the primary and secondary levels of infringement. Thus, she would be required to prove (i) that a member of the public in fact clicked on the URL that the defendant-linker supplied, and (ii) that the activation of the URL actually resulted in a distribution of the work. If the plaintiff failed to prove that the defendant-linker's URL was clicked, the defendant would argue that, even though the link it provided had the *potential* to facilitate an act of direct infringement, without proof of the realization of that potential, the link did not in fact "materially contribute" to an act of infringement. Further, if the plaintiff failed to prove that the linked-to source actually delivered a digital copy of the work (rather than a merely offered downloads), the defendant could invoke case law establishing that the "general rule" in the U.S. holds that an "infringement [of the distribution right] requires an *actual dissemination*" and thus no act of direct infringement has been established.[292]

In practice, U.S. courts have grappled with neither of these questions in hyperlinking cases. In the reported hyperlinking cases, U.S. courts typically have not required the copyright holder to prove that the defendant's link enabled an actual distribution of the work to an internet audience.[293] Despite this oversight, those U.S. courts bound by precedent which establishes that an "actual dissemination" is necessary for a violation of the distribution right should in theory not overlook a plaintiff's inability to show that a defendant's link actually caused the

[290] See, e.g., Cmty. Broad. Serv. v. Time Warner Cable, LLC, No. 07-139-B-W, 2008 WL 3200661, 9--10 (D. Me. Aug. 7, 2008) (noting that the plaintiff alleging a performance "to the public" need only allege that the transmission "was capable of being viewed by a substantial number of people," and that the plaintiff "need not prove that a substantial number of people actually viewed the challenged transmission").

[291] See, e.g., Atlantic Recording Corp. v. Howell, 554 F.Supp.2d 976, 985 (D. Ariz. 2008) (holding that "[t]he general rule, supported by the great weight of authority, is that infringement of [the distribution right] requires an actual dissemination of either copies or phonorecords"); Elektra Entertainment Group, Inc. v. Barker, 551 F.Supp.2d 234, 243--45 (S.D.N.Y. 2008) (stating that the distribution right guaranteed by the Copyright Act may be infringed by an offer to distribute, although merely alleging that files were made available, without alleging that they were also distributed, is not enough to state a claim). But see London-Sire Records v. Does, 542 F.Supp.2d 153, 176 (D. Mass. 2008) (holding that "evidence and allegations, taken together, [can be] sufficient to allow a statistically reasonable inference that at least one copyrighted work was downloaded at least once" and that this inference is "sufficient to make out a prima facie case" of infringement). See also supra notes 133--138 and accompanying text.

[292] Atlantic Recording Corp. v. 554 F.Supp.2d at 985.

[293] See, e.g. Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, 75 F.Supp.2d 1290, 1292 (D. Utah, 1999) (noting that "[i]t is undisputed that defendants [provided] three website addresses of websites containing [plaintiff's copyrighted works]" but neglecting to discuss whether any of those websites actually provided the underlying work to internet users, or whether defendant's links were actually used to access any of these source websites).

dissemination of a copyrighted work to a user's computer. That said, this tortuous reasoning applies only to offers to download: US authorities have not required proof of actual communications when plaintiffs allege violations of the rights of public performance or display.[294] As a result, claims involving links to unauthorized streaming sites would appear to forgo the hurdles of proving either that the user clicked on the link or that the site in fact streamed the content to the user.

IV.B.iii. Comparing U.S. standards for secondary liability and E.U. standards for direct liability

Some commentators have observed that the CJEU's imposition of a knowledge-based standard after *GS Media*, albeit providing the basis for direct liability for facilitation of infringement of the right of communication to the public, in fact resembles a secondary or contributory infringement standard.[295] As a result, even though US courts have declined to hold linkers directly liable for infringement that they facilitate, and therefore address claims against linkers as matters of secondary liability, EU standards of direct liability for facilitation of infringement seem to parallel US standards of derivative liability. The legal standard under both regimes focuses on similar questions, and may reach similar results.

Mere Supplier of Means vs. Acts of Communication / Secondary Infringement? --- The standard under both U.S. and E.U. law requires a consideration of the significance of the defendant's action: both regimes seek to distinguish between actors who merely supply the means to commit acts of infringement, and actors who take a more intentional and active role in enabling infringement. In the U.S., contributory liability analysis requires an inquiry into whether the defendant "materially contributed" to an act of direct infringement, which requires more than a "mere quantitative contribution to the primary infringement . . . participation in the infringement must be substantial."[296] The CJEU has distinguished between the mere provision of facilities for making a communication and the performance of a more "active" or "essential role" in the communication.[297] Case law from both jurisdictions confirms that the provision of a hyperlink to

[294] See supra note 134 and accompanying text (citing case law and the opinion of the U.S. Copyright Office establishing that a claim for infringement of the public display or performance rights does not require proof of an actual communication of the work).

[295] Eleonora Rosati, The CJEU Pirate Bay judgment and its impact on the liability of online platforms, European Intellectual Property Review (forthcoming) at 11 ("It has been argued that, by introducing a knowledge requirement within the scope of primary liability, the CJEU has blurred the distinction between what has traditionally regarded as a strict liability tort (primary infringement) and liability informed by the defendant's subjective state of actual or constructive knowledge (secondary infringement)."); Jane C. Ginsburg, The Court of Justice of the European Union Creates an EU Law of Liability for Facilitation of Copyright Infringement: Observations *on Brein v. Filmspeler* [C-527/15] (2017) and *Brein v. Ziggo* [C-610/15] (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024302

[296] Livnat v. Lavi, No. 96 CIV. 4967 (RWS), 1998 WL 43221, at *3 (S.D.N.Y. Feb. 2, 1998).

[297] See Directive 2001/29, supra note 21, at Recital 27 ("The mere provision of physical facilities for enabling or making a communication does not in itself amount to [an act of] communication."). This language derives from the Agreed Statement to Article 8 WCT. See WCT, supra note 6, art. 8 ("It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention."). The CJEU has held that a defendant commits an "act of communication" when that defendant performs an "essential role" in the making available of a particular work, by "interven[ing], in full knowledge of the consequences of his action, to give [users] access to a protected work, particularly where, in the absence of that intervention, those [users] would not be able to enjoy the . . . work, or would be able to do so only with difficulty." Case C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV* (June 14, 2017) at ¶ 26,

a location on the internet is a sufficiently significant act to support the imposition of liability on the link provider, even if the hyperlink merely made it easier for end-users to access a website which would have been available to them without the hyperlink.[298]

Knowledge and Inducement --- Under both U.S. and E.U. law, a defendant may face liability (i) if the defendant knew, or had reason to know, of the specific works to which it facilitated access,[299] or alternatively (ii) if the defendant actively induced users to access infringing works, even if the defendant did not know or have reason to know of the specific works to which it facilitates access.[300] Thus, a defendant-linker who supplies a deep or in-line link could face liability under either regime because such a link necessarily relates to one particular source and one particular copyrighted work, and thus a plaintiff will be able to establish that the defendant knew of the specific work to which it enabled access. And a defendant-linker who supplies a simple link to a website which aggregates infringing content (who may not know, or have reason to know, of the particular works to which it facilitates access through the simple link) may face liability under either regime if the defendant actively induced users to use the link to gain unauthorized access to a copyrighted work.

Liability for hyperlinking in both the U.S. and the E.U. also requires that the defendant have knowledge (actual, constructive, or presumed) of the infringing nature of the work to which it facilitated access. In *GS Media*, the CJEU established a rebuttable presumption that a defendant

---

http://curia.europa.eu/juris/document/document.jsf?text=&docid=191707&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523658.

[298] See supra notes *137--*139 and accompanying text (noting that U.S. courts have typically found that providing a hyperlink to an unauthorized source, in addition to some minimal activity encouraging or prompting users to use the hyperlink, suffices to constitute a "material contribution" to an act of direct infringement); *Ziggo, Case C-610/15, at* ¶ 26 (noting that a defendant commits an act of communication even if, 'in the absence of [the defendant's] intervention, . . . [users] would be able to [access the infringing source of the work] only with difficulty"); Case C-527/15, *Stichting Brein v Jack Frederik Wullems* [Filmspeler] (Apr. 26, 2017) at ¶ 49, http://curia.europa.eu/juris/document/document.jsf?text=&docid=190142&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=523515. ("[W]here it is established that such a person knew or ought to have known that the hyperlink he posted provides access to a work illegally placed on the internet, the provision of that link constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29.").

[299] Under traditional contributory liability analysis in the U.S., the plaintiff must prove that the defendant had actual or constructive knowledge of the specific acts of direct infringement that it facilitated. Arista Records, LLC v. Doe, 604 F.3d 110, 118 (2010). This standard is based on *specific* knowledge: the defendant must have known, or must have had reason to know, of the *specific* works which it has facilitated infringement of. See, e.g. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (2001) ("[I]f a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."). Similarly, the *Ziggo* case confirmed that, as a matter of EU law, a plaintiff must show that the defendant acted in "full knowledge of the consequences of his action," and that a plaintiff can meet this requirement by establishing that the defendant could not have been unaware" of the infringing nature of the conduct it facilitated. *Ziggo*, at ¶¶ 23 & 45. The *Ziggo* decision implies that evidence that the defendant "classif[ies] the works under different categories" and "delete[s] obsolete or faulty torrent files and actively filter[s] some content," which necessarily establishes that the defendant had knowledge of the *specific* works to which it was facilitating access, is relevant to the knowledge analysis. See id. at ¶ 38.

[300] See, e.g., Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 915--16 (2005) (establishing the doctrine of inducement of infringement in the U.S., through which a plaintiff may prevail on a secondary infringement claim even if the plaintiff fails to prove that the defendant knew or had reason to know of the specific works to which it facilitated access); *Filmspeler*, Case C-527/15, at ¶¶ 50--51 (holding the defendant liable without addressing whether the defendant had specific knowledge of the particular works to which it facilitated access).

who provides a hyperlink "for profit" does so "with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder."[301] Thus, many plaintiffs in E.U. hyperlinking cases will be spared the burden of proving that the defendant (with a profit motive) knew of the infringing nature of the work.

U.S. law does not recognize such a "for profit" presumption of knowledge.[302] In most U.S. hyperlinking cases, courts have avoided the question of the defendants' knowledge of the infringing nature of the work because such knowledge was obvious from the factual record.[303] However, in cases in which the defendant's knowledge of the infringing nature of the work is not so clear, plaintiffs may be able to argue that the defendant's knowledge of the infringing nature of the work should be presumed based on identifying characteristics of a website or the nature and format of the copyrighted work.[304]

IV.B.iv. Comparing Safe Harbor regimes in the U.S. and the E.U.

The EU and US safe harbors also appear to operate similarly, although the level of knowledge that will disqualify a US service provider may be somewhat higher, particularly given the textual disparity between US law's preclusion of a duty to monitor, and the EU's rejection of a "*general* duty to monitor"[305] (which, accordingly, leaves room for a specific duty to monitor, for example, to ensure that infringing content, once taken down, stays down).[306] In the EU, the service

[301] Case C-160/15, *GS Media BV v. Sanoma Media Netherlands BV* (8 Sept. 2016) at 51, http://curia.europa.eu/juris/document/document.jsf?text=&docid=183124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=95141 ("[W]hen the posting of hyperlinks is carried out for profit, it can be expected that the person who posted such a link carries out the necessary checks to ensure that the work concerned is not illegally published on the website to which those hyperlinks lead, so that it must be presumed that that posting has occurred with the full knowledge of the protected nature of that work and the possible lack of consent to publication on the internet by the copyright holder. In such circumstances, and in so far as that rebuttable presumption is not rebutted, the act of posting a hyperlink to a work which was illegally placed on the internet constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29."). But see supra note 68 (discussing recent German case law disregarding this rebuttable presumption in cases regarding the liability of search engines). In *Ziggo*, the CJEU did not apply the rebuttable presumption of knowledge announced in *GS Media*, perhaps because it was abundantly clear that the defendant was acting in full knowledge of the illicit nature of the communications that it was facilitating. See *Ziggo*, Case C-610/15, at ¶ 45.

[302] In general, the relevance of the commercial character of a defendant's conduct seems much more significant in E.U. cases than in U.S. cases. See *Filmspeler*, Case C-527/15, at ¶ 34 (noting that the "profit-making nature of a communication, within the meaning of Article 3(1) of Directive 2001/29, is not irrelevant"); *Ziggo*, supra, point 29 (same). In the U.S., the "commercial character" of a defendant's conduct may be relevant only in the context of a claim of inducement of infringement, which requires a plaintiff to prove that the defendant built a business model structured around infringing use. See Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[303] For example, in Pearson Educ., Inc. v. Ishayev, 9 F.Supp.3d 328 (2014), the court could safely assume that the defendant knew that the hyperlink in question linked to an infringing source because the defendant was in the business of selling unauthorized copies of educational materials; and in Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, 75 F.Supp.2d 1290 (D. Utah, 1999), the defendants clearly knew that the linked to materials were infringing because they had previously posted the materials to their own website and were ordered to remove them on the basis of copyright infringement. See id. at 1294--95.

[304] See supra notes 176--180 (discussing case law in which courts have considered such presumptions based on the names and characteristics of the works shared).

[305] 17 U.S.C. sec c. 512(m); Directive 2000/31, supra note 73, art. 15 (emphasis supplied).

[306] See, e.g., *Rapidshare I*, Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, I ZR 18/11, 2012, ¶¶ 19 & 31 (Ger.) (holding that in "specific cases" once a right-holder informs a service provider of infringement, the service provider must do "everything that is . . . technically and economically reasonable to prevent further

provider may be obliged to take down of its own accord recurring user-posted links to infringing sources, while it is less clear that a US copyright owner may impose such an obligation on a US service provider. On the other hand, while US law includes a safe harbor specifically for the benefit of search engines and providers of links, the eCommerce directive requires creative judicial exposition to reach these actors.[307] Nonetheless, the knowledge standard the CJEU has now engrafted onto a prima facie case of infringement of the communication to the public right by facilitation of infringement may well fill the gap between the activities shielded on the back end by US law, and activities excluded on the front end by the knowledge requirement in the EU.

infringements"); *GEMA v. RapidShare AG*, Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, I ZR 80/12, 2013, ¶. 39 (Ger.) (holding that a service provider who was notified of claimed infringement was required to monitor content uploaded by its users to prevent further infringement). But see Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 (holding that a general, preventative, time-unlimited duty to monitor a system for infringements would violate the prohibition of general monitoring obligations under art. 15 eCommerce Directive).

[307] See supra notes 78--77 and accompanying text (noting EU cases in which courts have implied that search engines may be able to claim safe harbor under art. 14 eCommerce Directive).