2010

User-Generated Content Sites and Section 512 of the US Copyright Act

Jane C. Ginsburg
Columbia Law School, jane.ginsburg@law.columbia.edu

Columbia Law School

Public Law & Legal Theory Working Paper Group

Paper Number 10-255

User-Generated Content Sites and Section 512 of the US Copyright Act

Jane C. Ginsburg
Columbia Law School

From Irini A. Stamtoudi, ed. Copyright Enforcement and the Internet (Kluwer Law International 2010)

November 2010

From Irini A. Stamatoudi, ed., Copyright Enforcement and the Internet (Kluwer Law International 2010)

Part II

User-Generated Content Sites and Section 512 of the US Copyright Act

*Jane C. Ginsburg**

I. INTRODUCTION

With the evolution of digital communications, the means of reproducing and disseminating copyrighted works increasingly leave the control of copyright owners and commercial distribution intermediaries. Websites and peer-to-peer and other technologies allow members of the public to originate the public communication of works of authorship. This does not mean that dissemination intermediaries have vanished from the copyright landscape, but rather that we have new kinds of intermediaries who do not themselves

* Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia University School of Law. This article is updated and adapted from Jane C. Ginsburg 'Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs', *Arizona Law Review* 50 (2008): 577. Thanks to Professors Graeme Austin, Hal Edgar, Doug Lichtman, Jessica Litman, Clarisa Long, Miquel Peguera, Sam Ricketson, and Pierre Sirinelli, and to June Besek, Esq. and Jeffrey Cunard, Esq., and the participants in the intellectual property workshops at Columbia Law School, the University of Michigan, and the University of Arizona. Thanks for research assistance to Jeff Vernon and Jennifer Maul, Columbia Law School class of 2008 and Nikhil Bodade, Columbia Law School LLM class of 2007.

Irini A. Stamatoudi, *Copyright Enforcement and the Internet*, pp. 183–198.

distribute copyrighted content but give their customers the means to make works available to the public.

When the works thus offered are neither of the distributor's own creation, nor distributed with the creator's permission, the person making the works available is a copyright infringer – assuming no exception, such as fair use, applies.[1] But the principal economic actor in this scenario is not likely to be the member of the public effecting the distribution. Rather, it is the entrepreneur who intentionally facilitated the distribution, for example, by operating a website to which members of the public could post the works, by targeting search services to locations where the works can be found, or by distributing file-sharing software designed to enable unauthorized copying and communication of works. Meaningful copyright enforcement will seek to establish the liability of the entrepreneurs.[2]

But all the technologies just evoked are 'dual purpose'. That is, they are not inherently pernicious; on the contrary, they can in fact be, and often are, put to perfectly lawful and socially desirable uses. If the technology itself is at least in theory neutral, does this pose an insoluble quandary: either enforce copyright at the expense of technological evolution, or promote technology at the cost of copyright? Or does the question so framed enmesh us in a false

1. Disseminating or offering works online for end-user access via streaming or downloading comes within the author's exclusive right of 'making available', set out at Art. 8 of the World Intellectual Property Organization Copyright Treaty, 20 Dec. 1996, S. Treaty Doc. No. 105-17, which defines the right in terms similar to the US right of public performance by transmission, but is not limited to performances of works. 17 U.S.C. § 101 (2000). Although the US's membership in this treaty requires implementation of the 'making available' right, the exclusive rights listed in the US Copyright Act, 17 U.S.C. § 106 (2000), do not explicitly include a 'making available' right. While a streaming digital delivery is a public performance, a file transfer consisting of a download that does not also render a performance, may not be. See *United States v. ASCAP*, 485 F. Supp. 2d 438, 443–444 (SDNY 2007). The § 106(3) distribution right covers those digital deliveries, see *id.* and authorities cited therein, but it is less clear whether offering a file for download, without a concomitant delivery to another's digital receiving device, also comes within § 106(3). See generally, D.O. Carson, 'Making the Making Available Right Available', *Columbia Journal of Law and the Arts* 33 (2010): 135 (discussing statute and cases); J.C. Ginsburg, 'Recent Developments in US Copyright Law – Part II: Exclusive Rights on the Ebb?', *Revue Internationale du Droit d'Auteur* 218 (October 2008): 167 and 239 (discussing cases).
2. As Judge Posner bluntly stated in In re *Aimster Copyright Litigation*: 'The [digital file] swappers, who are ignorant or more commonly disdainful of copyright and in any event discount the likelihood of being sued or prosecuted for copyright infringement, are the direct infringers. But firms that facilitate their infringement, even if they are not themselves infringers because they are not making copies of the music that is shared, may be liable to the copyright owners as contributory infringers. Recognizing the impracticability or futility of a copyright owner's suing a multitude of individual infringers (''chasing individual consumers is time consuming and is a teaspoon solution to an ocean problem,''), the law allows a copyright holder to sue a contributor to the infringement instead, in effect as an aider and abettor.' 334 F.3d 643, 645 (7th Cir. 2003) (citation omitted).

dichotomy? The legal rules should enable us to have it both ways, fostering both authorship and technological innovation, by ensuring the 'neutrality' of the technology as applied in a given business setting. 'Neutrality', however, is not the same thing as non-intervention. An entrepreneur who adopts what I'll call a passive-aggressive approach to user conduct that the entrepreneur reasonably should anticipate (and indeed may intend) will collectively be infringing on a large scale may in fact be building its business at the expense of authors and right owners. In that event, it should not matter how anodyne in the abstract the technology may be; by failing to take steps to forestall 'massive' infringement, the entrepreneur may in fact be encouraging unlawful user conduct, and may thereby be exposing itself to liability, at least under common law principles of secondary liability.[3]

The recent District Court decision in *Viacom v. YouTube*, however, indicates that the statutory safe harbour established by section 512 of the US copyright act may shield the entrepreneur who anticipates – and even 'welcome(s)' – infringements so long as the entrepreneur lacks 'actual or constructive knowledge of specific and identifiable infringements of individual items'.[4] While the statute makes clear that the entrepreneur should not be pressed into service as the investigative arm of the copyright owner,[5] the *Viacom* decision does not simply decline to impose an obligation to seek out the infringers who may lurk within the user base. Rather, the decision arguably rejects neutrality to read into the statute a high degree of solicitude not only for online entrepreneurs whose businesses occasionally may accommodate infringing users, but also for those who effectively solicit infringers. If, by contrast the neutrality principle does animate the statute, a court could appropriately apply that principle through a duty to take reasonable precautions to avoid apparent and repeat infringements.

This article considers the liability of entrepreneurs of 'user-generated content' (UGC) sites. These immensely popular fora, such as YouTube and My Space, enable their participants to post and view a great variety of content, not all of it in fact generated by the posting user. (It might be more accurate to label these sites as 'User-posted content' sites.) The legislative compromise worked out between telecommunications providers and content owners in the 1998 'Digital Millennium Copyright Act' provides the statutory framework for determining the extent to which the liability limitations enacted into section 512 of the Copyright Act can be interpreted to realize the neutrality objective, at once insulating the operators of UGC sites from debilitating copyright sanctions, while still affording meaningful relief to copyright owners.

3. See *MGM v. Grokster*, 545 U.S. 913 (2005).
4. 2010 U.S. Dist. LEXIS 62829 at *14 and *15–*16 (SDNY 2010).
5. 17 U.S.C. § 512(m)(1) (2000).

II. THE STATUTORY NOTICE-AND-TAKE-DOWN SAFE HARBOUR

In section 512 of the Digital Millennium Copyright Act,[6] Internet Service Providers (telecoms) obtained a large measure of impunity: if the service provider meets the threshold requirements, it will incur no liability (direct or derivative) for monetary damages if it responds expeditiously to a proper notice from the copyright holder, and blocks access to the offending material.[7] The statutory criteria are designed to ensure that the beneficiaries of the section 512(c) safe harbour remain copyright-neutral. Courts interpreting section 512(c) have recognized the neutrality prerequisite:

> This immunity, however, is not presumptive, but granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three [threshold requirements] of 17 U.S.C. Section 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe.[8]

Under section 512, the qualifying 'innocent' service provider incurs no general burden of anticipating or preventing infringement;[9] it need only react to notices of infringement that the copyright holders uncover. But because one may anticipate that at least some of the content the notified service provider takes down will promptly reappear, hydra-like, the question arises at what point, if any, the service provider becomes disqualifyingly 'aware' that the contested content is making repeat appearances, so that some obligation to forestall specific infringements may arise.

---

6. *Id*., § 512(c).
7. See § 512(c).
8. *ALS Scan, Inc. v. RemarQ Cmtys., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001).
9. *Id.*, § 512(m)(1) (stating that availability of the safe harbour is not conditioned on 'a service provider monitoring its service or affirmatively seeking facts indicating infringing activity'). Section 512(i)(1)(B) does make 'accommodat[ion of] . . . standard technical measures' a prerequisite to qualifying for the statutory safe harbours. Arguably, filtering technology might be such a measure. The definition of 'standard technical measures', however, suggests that the present state of filtering technologies may not suffice, principally because there is not yet an inter-industry consensus regarding the design and implementation of filtering measures. See § 512(i)(2). Section 512(i)(2) states:

> (2) Definition – As used in this subsection, the term 'standard technical measures' means technical measures that are used by copyright owners to identify or protect copyrighted works and –
>
> (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.
>
> *Id.*

The following discussion will analyse the specific statutory prerequisites to qualifying for a limitation on liability. To aid in that discussion, consider a hypothetical website, culture-for-me.com. It offers its users the opportunity to post video clips to its website. Culture-for-me.com neither promotes infringement, nor filters infringements out; its business plan aspires to a high volume of traffic to the site. In its early days, the website attracted amateur videos, but more recently users have also been posting copies of commercial film and television programming. Culture-for-me.com's popularity has risen substantially since professionally-produced (unauthorized) content began to be found on the site; the traffic to the unauthorized user postings is very heavy; indeed, those postings generally (but not always) receive more 'hits' than the amateur content.

A. 'Service Provider'

Culture-for-me.com operates a website; is it therefore a 'service provider' within the ambit of the statutory immunity? Section 512s definition of 'service provider' is exceedingly vague; the term 'means a provider of online services or network access or the operator of facilities therefore'.[10] 'Online services' are not defined. In the abstract, the term could mean any services offered online, including the service of making copyrighted works available to the public. Or the term could mean services specific to being online (other than network access, for which the definition specifically provides). Under the first interpretation, anyone who operates a website is a 'service provider'. Under the second, an entrepreneur who hosts a website is a 'service provider', as is one who provides online search services; the entrepreneur who makes content available, however, would not be a 'service provider' because the services provided are not Internet-specific. One can provide content from a variety of platforms (e.g., print, broadcast), but one can host or link to a website only via the Internet.[11]

The case law nonetheless has generally interpreted 'service provider' extremely broadly, to cover not only Internet-specific businesses, but a variety of traditional businesses' Internet operations, such as online auctions,[12]

10. § 512(k)(1)(B).
11. Section 512(i)(1)(A), which requires qualifying service providers to implement a policy for terminating the accounts of repeat infringers, may not cover operators of websites to which users post content if the users do not need to subscribe to or have an account with the website in order to post material to it. This could suggest that such websites do not qualify for the statutory safe harbour. On the other hand, making ability to terminate the accounts of repeat infringers a prerequisite to any 'service provider's' ability to qualify for a safe harbour might clash with the § 512(d) safe harbour for search engines, because most, if not all users of search engines access the service without becoming subscribers or account holders of the service.
12. *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (but parties did not dispute whether eBay was a 'service provider' within the meaning of the statute).

online real estate listings,[13] and an online pornography age verification service.[14]

The statute's legislative history indicates that a 'service provider' was not intended to embrace every kind of business found on the Internet. The examples of service providers given in the House Report consist entirely of enterprises who provide 'space' for third-party websites and fora, not the operators of the websites themselves.[15] This makes sense in the context of *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[16] the case law that section 512(c) substantially codified.[17] In *Netcom*, the service provider defendant was an Internet access provider that hosted third-party newsgroups, to which another defendant had posted documents without the authorization of the Church of Scientology. Nonetheless, even if Congress may not have had website operators in mind (much less the emerging Web 2.0 businesses), the language it chose to define 'service providers' is broad enough to encompass more Internet entities than Congress specifically contemplated in 1998.

B. 'Storage at the Direction of a User'

Assuming, then, that a website operator can be a service provider within the meaning of section 512, which of its activities does the statute immunize, and subject to what conditions? Section 512(c) absolves a service provider from liability 'for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider . . .'.[18] Is a website, as opposed to a server which hosts websites, 'a system or network controlled or operated by or for the service provider'? If not, the provision would not apply. But a website might be part of a system operated by the service provider, so this element does not screen out many actors. More importantly, section 512 exculpates '*storage* at

13. *Costar Group Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688, 701 (D. Md. 2001) (''Online services'' is surely broad enough to encompass the type of service provided by LoopNet that is at issue here.').
14. *Perfect 10, Inc. v. Cybernet Ventures*, Inc., 213 F. Supp. 2d 1146, 1175 (C.D. Cal. 2002) (assuming defendant qualified as a service provider, but admitting that it 'has found no discussion [in prior case law] of this definition's limits').
15. H.R. Rep. No. 105-551, pt. 2, at 64 (1998) ('This definition includes, for example, services such as providing Internet access, e-mail, chat room and web page hosting services.'); see also *ibid.*, at 53 (describing services covered by § 512(c): 'Examples of such storage include providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users').
16. 923 F. Supp. 1231 (N.D. Cal. 1995).
17. See, for example, David Nimmer, *Nimmer on Copyright* (San Francisco: Matthew Bender, 2009)§ 12B.06[B][2][a] (2006) (s. 512 essentially codifies Netcom).
18. 17 U.S.C. § 512(c)(1) (2000).

the direction of a user';[19] it does not suspend liability for other acts in which the service provider might engage with respect to the user-posted content.[20] Additional unrelated acts may fall outside the scope of mere 'storage'. The Ninth Circuit in *Perfect 10 v. CCBill* came to a similar conclusion regarding section 512(d)'s safe harbour for search engines:

> Even if the hyperlink provided by CCBill could be viewed as an 'information location tool', the majority of CCBill's functions would remain outside of the safe harbor of Section 512(d). Section 512(d) provides safe harbor only for 'infringement of copyright *by reason of* the provider referring or linking users to an online location containing infringing material or infringing activity'. (Emphasis added). Perfect 10 does not claim that CCBill infringed its copyrights by providing a hyperlink; rather, Perfect 10 alleges infringement through CCBill's performance of other business services for these websites. Even if CCBill's provision of a hyperlink is immune under § 512(n), CCBill does not receive blanket immunity for its other services.[21]

More recently, however, federal district courts ruled that section 512(c) does not require the host service provider to restrict its activities to the mere storage of user-posted content.[22] As one of the district courts stressed, section 512 assumes that users will be able to access content posted to host websites; thus, the websites must be permitted to transmit the stored content to the requesting user. The court did not address whether a storage-plus activity that is not 'closely related to, and follows from, the storage itself' would disqualify the host from the section 512(c) safe harbour.[23] The district court in *Viacom v. YouTube* agreed that:

> To the extent defendants' activities go beyond what can fairly be characterized as meeting the above-described collateral scope of 'storage' and allied functions, and present the elements of infringements under existing principles of copyright law, they are not facially protected by § 512(c). Such activities simply fall beyond the bounds of the safe harbor and liability for conducting them must be judged according to the general law of copyright infringement.[24]

---

19. *Id.* (emphasis added).
20. Cf. *Costar Group Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688 (D. Md. 2001) ('The legislative history indicates that [the actions protected by § 512(c) do] not include [the action of uploading] material ''that resides on the system or network operated by or for the service provider through its own acts or decisions and not at the direction of a user''.' (quoting H.R. Rep. No. 105-551, at 53 (1998)).
21. 481 F.3d 751, 766 (9th Cir. 2007).
22. See *UMG v. Veoh*, 2008 U.S. Dist. LEXIS 104980; 89 U.S.P.Q.2D (BNA) 1449 (C.D. Cal. 2008); *Io v. Veoh*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).
23. See *UMG v. Veoh*, above, at *31.
24. 2010 U.S. Dist. LEXIS 62829 at *40.

Nonetheless, the court continued, *YouTube* would lose the safe harbour only with respect to the activities that exceeded the bounds of '"storage" and allied functions'; any excess would not disqualify those activities that came within those bounds.

To return to culture-for-me.com, let us assume it is not contributing substantial value-added to the user-posted content, so that its liability would be based simply on its provision of a site from which users may upload and others may download content. This conduct comes squarely within the zone of the statutory exception. But the exception will not apply unless the entrepreneur meets the statutory conditions. A review of these conditions shows their common law ancestry: the criteria are very close to the elements of contributory and vicarious liability.[25]

C. Statutory Conditions for Limitation on Liability: Knowledge or Awareness

First, while the service provider has no obligation to monitor the site,[26] it must neither have actual knowledge that the postings are infringing,[27] nor be 'aware of facts or circumstances from which infringing activity is apparent'.[28] Once the service provider becomes aware of apparent infringements, it must 'act[] expeditiously to remove, or disable access to, the material'.[29] Such awareness triggers a proactive obligation to block access in order to qualify for the statutory immunity. What constitutes 'apparent' infringing activity, then, is key to determining whether the safe harbour applies.

The case law interpreting the statutory 'red flag'[30] standard suggests the flag may need to be an immense crimson banner before the service provider's obligation to intervene comes into play:

> Although efforts to pin down exactly what amounts to knowledge of blatant copyright infringement may be difficult, it requires, at a minimum, that a service provider who receives notice of a copyright violation be

25. See, for example, P. Goldstein, *Goldstein on Copyright*, 3rd edn (New York: Aspen Publishers, 2009) (Looseleaf), 2, § 8.3.2 ('The first of the three concurrent conditions for the safe harbor is patterned after the knowledge requirement for contributory infringement. . . . The second condition for this safe harbor effectively embodies the rules on vicarious liability. . . . ').
26. 17 U.S.C. § 512(m) (2000). Section 512(m) states that '[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i) . . . .' *Id.*
27. § 512(c)(1)(A)(i).
28. § 512(c)(1)(A)(ii).
29. § 512(c)(1)(A).
30. See *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751, 763 (9th Cir. 2007).

> able to tell merely from looking at the user's activities, statements, or conduct that copyright infringement is occurring.[31]

Examples of conduct sufficiently blatant to warrant the service provider's vigilance might include abnormally and disproportionately high traffic to the area of the site where the alleged infringement is located, or the appearance of terms like 'pirated' or 'bootleg' in the name of the file.[32] But the context of the website might blur the meaning even of file names like 'stolen'. In *Perfect 10 v. CCBill*, the Ninth Circuit declined to hold that the titles of pornographic websites that defendant hosted, 'illegal.net' and 'stolencelebritypics.com', should have alerted the defendant host server to the copyright-infringing nature of the websites' content.[33] The court observed:

> When a website traffics in pictures that are titillating by nature, describing photographs as 'illegal' or 'stolen' may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.[34]

Similarly, the district court in *Viacom v. YouTube* stressed that 'General knowledge that infringement is ''ubiquitous'' does not impose a duty on the service provider to monitor or search its service for infringements':[35]

> the phrases 'actual knowledge that the material or an activity' is infringing, and 'facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough. That is consistent with an area of the law devoted to protection of distinctive individual works, not of libraries. To let knowledge of a generalized practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA.[36]

---

31. *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1104–1105 (W.D. Wash. 2004).
32. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc*., 351 F.3d 1229, 1233 (D.C. Cir. 2003) (offering large volume of audio or audiovisual files); *In re Aimster Copyright Litig*., 334 F.3d 643 (7th Cir. 2003) (chat groups offering instructions on how to engage in illegal downloading); *Corbis*, 351 F. Supp. 2d at 1100 (citing *Hendrickson v. eBay*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001)) (suspicious file names); cf. *Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc*., 256 F. Supp. 399, 404 (S.D.N.Y. 1966) (noting that suspiciously low price of records might have made it obvious to defendant that they were pirated).
33. *CCBill*, 481 F.3d at 763.
34. *Ibid.*
35. 2010 U.S. Dist. LEXIS 62829 at *35.
36. *Id*., at *29–*30.

On the other hand, one might contend that if the file title includes the name of a motion picture, television programme, or sound recording of which the person or entity posting the content is obviously not the copyright owner, this may be sufficiently specific to raise a red flag.[37] Of course, not every file name's incorporation of a film's title inevitably means the file infringes. Some files may in fact be parodies of, or other kinds of pastiche or commentary on, the copyrighted work, and therefore could well be fair use. The question is whether the presence of the title under circumstances in which it would be obvious that the rightholder did not authorize the posting should trigger a pro-active obligation on the part of the service provider to take a look. Any such obligation might be reinforced if the titles were the subject of repeated section 512(c) 'take down' notices sent by the rights holders. In those circumstances, the film's title might make infringement 'apparent', and minimal investigation on the service provider's part could indicate whether in a particular case, appearances deceive.[38]

But the *Viacom* court applied a much more bright-line approach to the 'red flag' standard: if the posting on its face does not clearly reveal infringement, then

37. Cf. *Corbis*, 351 F. Supp. 2d at 1105 ('Without some evidence from the site raising a red flag, Amazon would not know enough about the photograph, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement.').

38. Repeated take down notices are likely to result from an automated search of the website (or of the Internet as a whole): the search 'bot' identifies a file bearing or including the name of the copyrighted work, and automatically generates a take-down notice sent to the host service provider. See generally Public Knowledge, 'Transcript of Verizon-RIAA Subpoena Discussion at National Press Club', <www.publicknowledge.org/?node/730>, 20 Mar. 2008. Mechanisms of this sort may reduce some of the enforcement costs that the § 512(c) regime imposes on copyright owners, although it is not clear that individual authors and small independent producers have the means to avail themselves of these automated resources. See 17 U.S.C. § 512(c) (2000). The clearance burden that § 512 displaces to copyright owners thus would fall disproportionately on those least equipped to assume the greater enforcement costs. See *id.* § 512. Automated take-down notices, however, may be problematic if they are triggered by nothing more than a file name correlation, for some notices may demand removal of postings which could be fair uses; such notices might subject the sender to liability under § 512(f) for 'knowingly materially misrepresents under this section (1) that the material or activity is infringing'. See *Lenz v. Universal Music Group*, 572 F.Supp.2d 1150 (N.D. Cal. 2008).

In addition, if the film's title correlates to the subscriber information or IP address of an uploader who previously posted infringing files, the combination of claimed content and suspect source should deepen the red flag's hue. Section 512(i) requires that service provider adopt and implement a policy for terminating subscribers who are 'repeat infringers', but it does not so far appear that the prospect of cutting users' access to the websites to which they post infringing content offers a meaningful remedy, perhaps because terminated subscribers can re-subscribe under other names or identifying information, and/or because the statutory standard is unclear: for example, must the repeat infringements have been adjudicated? See Ronald J. Mann & Seth R. Belzley, 'The Promise of Internet Intermediary Liability', *William & Mary Law Review* 47 (2005): 239, 301 (raising these points with respect to an analogous provision in § 512(a) regarding access providers).

infringing activity is not sufficiently 'apparent'; no further investigation should be required.

> '. . . if investigation of ''facts and circumstances'' is required to identify material as infringing, then those facts and circumstances are not ''red flags'' '. That observation captures the reason why awareness of pervasive copyright-infringing, however flagrant and blatant, does not impose liability on the service provider. It furnishes at most a statistical estimate of the chance any particular posting is infringing – and that is not a 'red flag' marking any particular work.[39]

Viacom v. YouTube and the cases on which it relies, however, may apply too stringent a test. 'Apparent' does not mean 'in fact illegal', nor does it mean 'conclusively exists'. The statute articulates two circumstances that hoist the red flag: 'actual knowledge' of infringement and 'facts and circumstances from which infringing activity is apparent'. *Viacom* and some of its predecessors appear to conflate the two. Infringement may be 'apparent' yet subject to verification (or contradiction). If the file name coincides with a work the right owner has notified the user generated content site has not been licensed for third party dissemination, and if the user has previously posted infringing files, a 'red flag' standard that demands greater certainty from the outset risks allowing the service provider to 'turn a blind eye' to infringements because the provider could claim that the possibility that some files might not be infringing means that infringement can never be 'apparent' as to any file.[40] By the same token, section 512(m)'s dispensation of service providers from 'affirmatively seeking facts indicating infringing activity', should not entitle the service provider to passive-aggressive ignorance.

D. Statutory Conditions for Limitation on Liability: Direct Financial Benefit

Second, the service provider must not 'receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider

---

39. 2010 Dist. LEXIS 62829 at *31–*32, *quoting UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009).

40. Cf. *Perfect 10, Inc. v. Cybernet Ventures, Inc*., 213 F. Supp. 2d 1146, 1177 (C.D. Cal. 2002). In *Cybernet*, the district court stated that:

> [t]he Court does not read section 512 to endorse business practices that would encourage content providers to turn a blind eye to the *source* of massive copyright infringement while continuing to knowingly profit, indirectly or not, from every single one of these same sources until a court orders the provider to terminate each individual account.

Id.

has the right and ability to control such activity'.[41] This standard adopts the common law test for vicarious liability enunciated in copyright cases involving both traditional[42] and digital infringement.[43] As applied to culture-for-me.com, the analysis would focus on how 'direct' the benefit of storing user-posted infringing content must be to disqualify the website operator, and on the level of control the website operator can exercise over the users who post material to the site.

With respect to the nexus between the infringement and the benefit to the website, if the website accepted advertising targeted to the infringing content, the benefit would surely be 'direct'. Moreover, if the website knew the content was infringing, it would be obliged to remove the material even without notification by the rightholder. Assume, however, that the relationship between infringement and the benefit is more attenuated. For example, the website accepts advertising; the rates charged are a function of the popularity of the material alongside which the ads appear. Or, the website accepts advertising, but the advertisements appear randomly; the rates are the same whatever the content in connection with which the ads appear. The overall popularity of the website will, however, influence the amount of money the website operator can charge for ads. If it is true that free (unauthorized) copyrighted content is a 'draw',[44] then making ad rates turn on the popularity of portions of the website may foster too close a relationship between the infringements and the financial benefit.

By contrast, in the second scenario the financial benefit may be too attenuated;[45] it might be necessary to show that the presence of free unauthorized content makes the site as a whole more attractive than it would be without

---

41. § 512(c)(1)(B).
42. See, for example, *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996) (liability of landlord of flea market at which vendors sold pirated sound recordings).
43. See, for example, *Perfect 10, Inc. v. CCBill LLC*, 481 F.3d 751, 766–767 (9th Cir. 2007) (common law standards and § 512(c)(1)(B) standards are the same); *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1022–1023 (9th Cir. 2001); *Costar Group Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001), *aff'd* 373 F.3d 544 (4th Cir. 2004) ('Basically, the DMCA provides no safe harbor for vicarious infringement because it codifies both elements of vicarious liability.'). But some courts have applied one of the elements of the common law standard for vicarious liability more narrowly in the context of § 512(c)(1)(B). See n. 55 below and accompanying text.
44. See, for example, *Fonovisa*, 76 F.3d at 263 (reversing the district court's decision to dismiss plaintiff's vicarious copyright infringement claim where defendant flea market operator received admissions fees, concession stand sales, and parking fees that were tied to number of people at flea market); *UMG Recordings, Inc. v. Sinnott*, 300 F. Supp. 2d 993, 1002–1003 (E.D. Cal. 2004) (finding defendant received a benefit from increased revenue at concession stands and on-site go-kart track); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 Civ. 4660 (SHS), 2002 WL 1997918, at *11 (S.D.N.Y. 29 Aug. 2002) ('direct financial interest' prong satisfied when infringing works acted as draw and defendant received substantial amount of advertising tied to number of users).
45. Cf. *Aitken, Hazen, Hoffman, Miller, P.C. v. Empire Constr. Co.*, 542 F. Supp. 252, 262 (D. Neb. 1982) (building company built building based on plaintiff's architectural works

that content. Put another way, the copyright owner may need to show that the free unauthorized content is in fact 'drawing' users to the site.[46] Such a showing may imply a significant volume of infringing material,[47] although one court has declared that what matters 'is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of *how substantial* the benefit is in proportion to a defendant's overall profits'.[48] Comparisons of 'before and after' visitor rates to websites formerly hosting infringing material can supply some indication of the effect of that material on a website's popularity,[49] but it may not be appropriate to generalize from one website to another.[50] The parties thus may be locked in a vicious circle: if proving causation requires a 'before and after' showing with respect to the defendant website, but the 'after' data cannot be acquired without ordering the website to filter out infringing material, then either the copyright owner in effect obtains the requested relief (compelling proactive steps on the part of

---

without permission, but lumber company and engineer employed by building company who received fixed fees for constructing building held not vicariously liable).

46. See *Costar Group*, 164 F. Supp. 2d at 704–705 (stating that an *in*direct benefit that infringements may provide to a website 'does not fit within the plain language of the statute').
47. *Compare Polygram Int'l Publ'g v. Nevada/TIG, Inc.*, 855 F. Supp. 1314, 1333 (D. Mass. 1994) (stating that '[t]he crucial question for establishing the benefit prong of the test for vicarious liability is not the exact amount of the benefit, but only whether the defendant derived a benefit from the infringement that was substantial enough to be considered significant' and finding that the benefit was significant even though only 4 of 2,000 exhibitors committed infringing acts), *with Artists Music, Inc. v. Reed Publ'g (USA), Inc.*, Nos 93 CIV. 3428(JFK), 73163, 1994 WL 191643, at *6 (S.D.N.Y. 19 May 2004) ('This Court does not believe that alleged infringements by four of 134 exhibitors in any way affected gate receipts at the Show. Plaintiffs offer no evidence that so much as a single attendee came to the Show for sake of the music played by four out of 134 exhibitors.').
48. *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004).
49. See Brad Stone & Miguel Helft, 'New Weapon in Web War over Piracy', *New York Times*, 19 Feb. 2007, C1 (explaining that when videosharing site 'Guba' implemented filters to screen out infringing material, the site's popularity 'took a huge hit').
50. Several services provide information regarding web sites' traffic over a period of time. See, for example, <www.comscore.com>, 26 May 2009; <http://siteanalytics.compete.com>, 26 May 2009. But it is unclear whether such data can help courts draw reliable conclusions about whether infringing works on a website acted as a draw. For example, Compete has a measure – 'people count' – which purports to track how many people visit a website each day. Many of the filtering service Audible Magic's most notable clients did not report a drop in traffic (according to this ranking) after announcing a plan to implement its filtering technologies, although other entrepreneurs did experience loss of traffic to their sites. The lesson to draw from this information is unclear. Perhaps those websites who did not lose audience did not depend on infringing materials in the first place. Or perhaps the filtering technology has not been effective. Or, even if the technology works as intended, perhaps the websites that saw an increase in traffic might have seen an even greater increase had they not implemented the filtering technology. Attempts to draw conclusions by comparing sites that do filter with those that do not are not likely to be very probative because different levels of traffic may result from characteristics of the websites that have nothing to do with filtering.

the website) before it has made the required showing, or the relief is denied for lack of a showing which cannot be made without ordering the website to take the very action it resists.

E. Statutory Conditions for Limitation on Liability: Right and Ability to Control Infringing Activity

Even if the 'direct financial benefit' standard is met, the service provider will not be disqualified from the safe harbour unless it also had the 'right and ability to control' the infringing activity. Some courts appear to interpret the control element differently depending on whether they are applying common law principles of vicarious liability, or the section 512(c) criteria. In the common law context, courts will rule that a defendant online service provider has the 'right and ability to control' an infringing activity if it can block attempts to use its online service for infringing activities.[51] By contrast, some courts have found that the ability to block access to infringing uses of a website does not of itself mean that an online service provider has the 'right and ability to control' for the purposes of section 512.[52] The rationale for this departure from the common law case law appears to derive from other aspects of section 512. Section 512(c)(1)(C) conditions qualification for the safe harbour on expeditious removal of the infringing content once the service provider is properly notified of its existence. To qualify for the statutory exemption, then, the service provider must have the ability to block access, at least once the material has been posted. But if the ability to block access also meets part of the standard for disqualification from the exemption, then the statute would be incoherent.[53]

Thus, in this view, 'right and ability to control' under section 512(c)(1)(B) must mean something more than a subsequent ability to block access. Section 512(c)(1)(B) already sets out an additional element: receipt of a direct financial benefit, so perhaps it is not necessary to devise what one might call a 'common law plus' interpretation of 'right and ability to control'. Alternatively, 'something more' might mean an ability to intervene before the infringing content is placed on the website.[54] But this plus factor presents its own

---

51. See, for example, *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023–1024 (9th Cir. 2001); *Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc.*, 907 F. Supp. 1361, 1375–1376 (N.D. Cal. 1995).
52. See, for example, *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093–1094 (C.D. Cal. 2001); *Costar Group Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688, 704–705 (D. Md. 2001).
53. See *Hendrickson*, 165 F. Supp. 2d at 1093–1094; *Costar Group*, 164 F. Supp. 2d at 704 n.9.
54. See *Tur v. YouTube, Inc.*, No. CV064436 FMC AJWX, 2007 WL 1893635, at *3 (C.D. Cal. 20 Jun. 2007) ('[T]he requirement [of ''something more''] presupposes some antecedent ability to limit or filter copyrighted material.' (citations omitted)); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1181–1182 (C.D. Cal. 2002) ('Here Cybernet prescreens sites, gives them extensive advice, prohibits the proliferation of

anomalies: if the service provider must be more closely implicated in the user's activities in order to have the requisite control, then this condition on the safe harbour would be redundant: the service provider would already be disqualified on the section 512(c)(1)(A) ground that the service thereby acquires forbidden knowledge of the user's activities,[55] or on the section 512(c) threshold ground that the services it provides exceed the mere storage and communication of user-posted content.

Moreover, it is not clear why recognizing post-hoc ability to block access as satisfying the 'right and ability to control' prong would in fact make the statute incoherent (or, at least, any more incoherent than it arguably already is). It seems clear that a section 512(c) service provider cannot benefit from the safe harbour if it sets up a system that disables it from exercising any control over user postings: while absence of control would meet the section 512(c)(1)(B) criterion, the service provider would then fail to qualify under section 512(c)(1)(C) because it would not be able to block access to the infringing content. Thus, the inconsistencies of the statutory scheme are readily apparent when one considers that the level of control requisite to qualifying under (C) might also cause disqualification under (B), and that the inability to block access qualifies the service provide under (B), but disqualifies it under (C).

III. CONCLUSION

It appears, despite the complexities of section 512, that the statutory prerequisites for application of the safe harbour should exclude a website that is not economically viable without its users' infringements, or which significantly benefits from infringement. Most importantly, the statutory constraints on qualifying for the section 512 safe harbour would preclude a UGC site from correlating advertising to infringing material, thus preventing the website operator from realizing the full value of the posted material. Under section 512, the operator must charge the same advertising rates for the popular professionally-produced content that its users post (in theory without the website's knowledge or invitation) as for genuinely user-created content. But one might expect that advertisers would pay more to run their ads alongside a successful television show than abutting my home video of my

---

identical sites, and in the variety of ways mentioned earlier exhibits precisely this slightly difficult to define ''something more''.').

55. The *Viacom* court appears to have committed this solecism: in holding that 'The ''right and ability to control'' the activity requires knowledge of it, which must be item-specific.' 2010 US Dist. LEXIS 62829 at *41, the court conflated the s. 512(c)(1)(A)(ii) 'red flag' criteria with the s. 512(c)(1)(B) financial benefit criteria. Because the safe harbor claimant must satisfy *both* standards, the standards should be interpreted to have independent meaning.

hamster's summer vacation. Once the site seeks to monetize the actual value of the posted material, however, it leaves the shelter of section 512. Thus, notwithstanding the outcome of judicial analysis of section 512 in the *Viacom v. YouTube* and other cases, one may anticipate that business imperatives will in the long run counsel an accord between copyright owners and UGC sites.[56]

56. See, for example, Alan N. Braverman & Terri Southwick, 'The User-Generated Content Principles: The Motivation, Process, Results and Lessons Learned', *Columbia Journal of Law & Arts* 32 (2009): 471 (describing multi-party development of ''Copyright Principles for UGC Services'''); Claire Cain Miller, 'YouTube Ads Turn Videos Into Revenue', New York Times (Sept. 2, 2010), <www.nytimes.com/2010/09/03/technology/03youtube.html?_r=1&scp=9&sq=youtube%20friday%20September%203&st=cse> (describing licensing of user-posted third-party copyrighted content for revenue-sharing advertisements).