European Intellectual Property Review

2002

Article

THE DMCA AND THE ECOMMERCE DIRECTIVE

Victoria McEvedy.

Case: A&M Records Inc v Napster Inc 239 F.3d 1004 (2001) (9th Cir (US))

Legislation: Digital Millennium Copyright Act 1998 (United States) s.512

Council Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the internal market

Subject: INTELLECTUAL PROPERTY. Other related subjects: Information technology

Keywords: Copyright; Digital technology; EC law; Electronic commerce; Service providers; United States

Abstract: Provisions in 1998 Act on safe harbours to shelter ISPs from liability for copyright infringement, conditions and notice and takedown procedure, comparison with provisions in Directive 2000/31 and impact of 1998 Act in Napster case.

***65** The United States has unquestionably taken the lead in the regulation of the internet and its efforts have been closely observed by the international community, which has largely been prepared to await the results in the United States before adopting its models. In this article, the author examines the Digital Millennium Copyright Act ("DMCA") [FN1] on which the new Directive on E-Commerce [FN2] is closely based. In marked contrast to other statutes, [FN3] the early showing of the DMCA is disappointing--the clearest example to date being the Court of Appeals for the Ninth Circuit's refusal to apply it in the Napster case. [FN4]

The Digital Millennium Copyright Act ("DMCA") 1998

Title II of the DMCA adds a single section to the Copyright Act--section 512-- which provides four safe harbours [FN5] to shelter ISPs [FN6] from liability for copyright infringement. [FN7] However, in order to benefit ISPs must be "good citizens" who err in favour of removal of the material complained of. [FN8] In return, ISPs can avoid monetary penalties and disabling injunctions if they can bring themselves within the "safe harbours". If they ***66** can, the only penalty that they face is a narrow injunction to block access to individual infringing users. [FN9]

The DMCA Safe Harbours

There are four safe harbours [FN10]:

(1) mere conduit [FN11]--for ISPs transmitting, routing or providing connections for information (s.512 (a)) [FN12];

(2) caching [FN13]--where ISPs temporarily and automatically store material made available by others online (s.512 (b)) [FN14];

(3) user storage [FN15]--where ISPs store material at the direction of a user (s.512 (c)) [FN16];

(4) information location tools [FN17]--for ISPs referring or linking users to online locations by directory, ***67** index, reference, pointer or hypertext (s.512 (d)). [FN18]

Conditions

The objective of the DMCA was to provide ISPs with certain protection from liability without requiring them to determine the merits of rightholders' claims. Unfortunately, in order to take advantage of a safe harbour, ISPs must comply with a "myriad of minute circumstances". [FN19] The conditions for the mere conduit and caching safe harbours are largely unsurprising, while the user storage and information location tools harbours share common conditions, applying where a service provider:

> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit [FN20] directly attributable to the infringing activity ... [where] the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity .... [FN21]

This is almost a codification of the common law tests for secondary liability, being actual (or constructive) knowledge and financial benefit directly attributable to the infringing activity when combined with a right and ability to control the activity. [FN22] Alfred Yen observes:

> The foregoing shows that the DMCA clearly offers ISPs safe harbor from vicarious or contributory liability for subscriber infringement. However, that assurance of non-liability applies largely in situations where ISPs face no liability in the first place. The statute appears to state that ISPs are not liable if they remove alleged infringements upon receipt of a formal complaint and are not otherwise vicariously or contributorily liable. [FN23]

However, the "red flag" standard in A (ii) has been distinguished from common law constructive knowledge [FN24] and described as not "what a reasonable person would have deduced given all of the circumstances" but rather "whether the service provider deliberately proceeded in the face of blatant factors of which it was aware". [FN25] Thus, while an ISP is expressly relieved of any obligation to monitor [FN26] or affirmatively seek facts indicating infringing activity, it cannot bury its head in the sand--if it becomes aware of a red flag, it will lose the benefit of the safe harbour by failing to react and remove the material. [FN27] The issue is likely to be most complicated in relation to the information location tools safe harbour as the question arises whether an ISP might be deemed to have turned a blind eye to a red flag solely because its human agents had visited an infringing site. If so, then the benefit of this safe harbour might prove illusory. While the matter has yet to be sufficiently tested, this was not the legislative intention. [FN28]

***68** Thus ISPs must remove material from the internet or lose the safe harbour:

> (1) on gaining actual knowledge of infringing activity [FN29] or becoming aware that the criteria for the "red flag" test are met [FN30]; or
>
> (2) receiving notice of a claimed infringement. [FN31]

Meanwhile rightholders have a strong incentive to monitor and notify infringements to ISPs in order to avoid later bearing the onus of establishing that the ISP had actual knowledge or had ignored a "red flag". [FN32]

Notice and Takedown

The DMCA introduces a detailed "notice and takedown" procedure. This procedure is scarcely relevant to the mere conduit harbour (notification being unlikely given the transitory nature of the communication [FN33]) and is unlikely to have significant application to the caching and information location tools as in both cases, the rightholder is likely to be more concerned to disable the material at source by attacking the site itself, so that it will be primarily significant in relation to the user storage harbour. [FN34] On notification by a rightholder of infringing material or activity, an ISP must expeditiously remove or disable access to the infringing material or activity. [FN35]

The DMCA provides that only complaints filed with the ISP's designated agent, in accordance with the statutory form, create knowledge or raise a red flag for purposes of the safe harbours. [FN36] This means that ISPs that take advantage of the DMCA have a single controlled avenue for receiving complaints. Detailed requirements for notification are prescribed. [FN37] However, even a non-conforming notice is likely to lead to

the removal of material, [FN38] as it requires the ISPs to contact the sender of the non-conforming notice in order to facilitate receipt of a conforming one. [FN39]

Subsection 512 (g) immunises the ISP from liability for the removal or disabling in the event that the claim of infringement turns out to be unsustainable, [FN40] providing ***69** a "Good Samaritan" defence. [FN41] However, in order to benefit, the ISP must also:

(1) notify the subscriber that it has removed or disabled access to the material;

(2) on receipt of a counter-notice [FN42] from the subscriber provide the notifier with a copy thereof and inform the notifier that it will replace the removed material or cease disabling it in 10 business days; and

(3) replace the removed material or cease disabling access [FN43] to it not less than 10, nor more than 14, business days following receipt of the counter-notice, unless it (by its designated agent) first receives notice from the notifier that he has issued suit seeking a court order to restrain the subscriber from infringement, [FN44] in which case the material will remain disabled until the court seised orders otherwise.

Rightholders and subscribers who knowingly make misrepresentations by notifications or counter-notifications face liability [FN45] and in the case of the later, do so on pain of perjury. [FN46] Yet as recent cases indicate, particularly where the subscriber relies on the defence of fair use, it may not be apparent which party is wrong and both may be acting in good faith.

The notice and takedown procedure allows an ISP to deal with complaints according to the letter of the procedure without exercising human judgment as to the merits of an alleged infringement--and still avoid liability.

The E-Commerce Directive

The European Union has taken a "horizontal" approach to ISP liability in the framework Directive on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (2000/31) ("the E-Commerce Directive"), [FN47] which applies to "copyright piracy, unfair competition practices, misleading advertising, etc.". [FN48] In addition, particular protection is provided for copyright infringement in the draft Directive on Copyright and Related Rights in the Information Society ("Copyright Directive"). [FN49]

The E-Commerce Directive closely resembles the DMCA in that it provides "limitations of liability" [FN50] ***70** while leaving the underlying law unaffected; that is, the nature and scope of an ISP's liability remains the subject of the underlying applicable law of the relevant Member States. [FN51]

The two key differences are that the E-Commerce Directive does not protect information location tools and there is no notice and takedown procedure and therefore little guidance or protection for ISPs in the removal or restoration of material. However, the E-Commerce Directive was intended to remove primary barriers to cross-border commerce on the internet and not to regulate comprehensively.

The E-Commerce Limitations of Liability

The exceptions from liability for "intermediary service providers" [FN52] are:

(1) Mere conduit--where the service provided is "the transmission in a communication network of information provided by a recipient of the service" [FN53] or "the provision of access to a communication network", the service provider is not liable for the information transmitted (Art. 12) [FN54];

(2) Caching--where the service provided is "the transmission in a communication network of information provided by a recipient of the service", the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service on their request (Art. 13) [FN55];

(3) Hosting--where the service provided "consists of the storage of information provided by a recipient of the service", the service provider is not liable for the information stored (Art. 14).

There is no explanation in the travaux préparatoires for the absence of protection for information location tools. Although this is surprising in the light of the number of controversial cases involving search engines, the

likelihood of a consensus on the issue is remote owing to the diverging national approaches the cases demonstrate. [FN56]

Conditions

In relation to hosting, the conditions mirror the DMCA in that they require:

1(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; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider. [FN57]

Just as in the DMCA, Member States are expressly ***71** prohibited from imposing any general obligation on ISPs to monitor information that they transmit and store or to actively seek facts or circumstances indicating illegal activity. [FN58] However, this does not prevent Member States from monitoring specific cases or orders made by national authorities under national legislation. [FN59] Nor does it prevent Member States from imposing obligations on hosting ISPs to apply duties of care specified under national law, to detect and prevent certain types of illegal activities. [FN60] As with the DMCA however, the limitations on liability do not preclude the development of "technical systems of protection and identification and of technical surveillance instruments made possible by digital technology". [FN61]

Removal

In the absence of a notice and takedown procedure, Member States remain free to establish "specific requirements" for "expeditious fulfilment prior" to removal [FN62] consistent with their own legal cultures.

The result is that ISPs will have to determine whether rightholders or other complainants have a prima facie claim, and whether users have a prima facie defence, an exercise involving expertise and judgment, and then take a view on removal and restoration.

The intention is that voluntary codes of conduct should be developed by industry. [FN63] ISPs are directed to observe the principle of freedom of expression in removing or disabling access to information but no other guidance is provided. [FN64] A number of industryled initiatives for establishing codes of conduct have commenced. [FN65]

Napster and the DMCA

The DMCA has yet to be tested to any real extent; however, in the few cases where it has been invoked, the promised protection for ISPs has been elusive. The best example to date is the Napster case. [FN66]

In May 2000 Napster brought a motion [FN67] for summary judgment relying on the "mere conduit" safe harbour in section 512 (a) of the DMCA. [FN68] The plaintiffs argued that Napster's directory and search facilities disqualified it from the mere conduit safe harbour and that these services fell within the more stringent safe harbour for information location tools in subsection 512 (d). Even if section 512 (a) did apply, the plaintiffs relied on the fact that the infringing material was not transmitted or routed through Napster, but directly between its users over the internet. [FN69] Napster countered that the information location tools it provided were incidental to its core function of transmitting or routing MP3 files for users and that even if they fell within 512 (d), the safe harbour in 512 (a) covered the other aspects of its service. Napster failed on its motion. The court found that it performed some information location tool functions as it had a searchable directory and index and (while a host's file names could only be searched while the host was logged on) it operated a "hot list" that enabled notification of users that a relevant host had logged on. It did not accept that these functions were peripheral or that they should be separately analysed under 512 (d). As to the application of 512 (a), it found that the MP3 files were not transmitted through Napster's system but directly between ***72** users over the internet. [FN70] The court also considered that Napster had failed to comply with the general eligibility requirement applicable to all safe harbours, in section 512 (i) which required that an ISP must have adopted, implemented and informed its users of a policy [FN71] for terminating repeat infringers. [FN72]

In July 2000, in its defence to a plaintiff's motion for a preliminary injunction, [FN73] Napster relied on the information location tool safe harbour in section 512 (d) of the DMCA. The court dismissed this in a footnote

[FN74] on the basis that its finding that Napster had constructive knowledge of the direct infringements put an end to what it described as Napster's "persistent attempts" to invoke section 512. It is also observed that it was not persuaded that 512 (d) sheltered contributory infringers. Based on findings that the plaintiffs had shown a reasonable likelihood of success on the merits of their claims against Napster for contributory and vicarious copyright infringement, [FN75] Napster was enjoined from "engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of the rights owner". [FN76] The court also stipulated that the injunction applied to all such works owned by the plaintiffs and not merely those specified in the complaint and that Napster bore the burden of developing a means to comply with the injunction so as to ensure that no work owned by the plaintiffs which neither Napster or its users had permission to use or distribute be uploaded or downloaded on Napster. The plaintiffs were also ordered to co-operate with Napster in identifying their works. [FN77]

Napster appealed to the Court of Appeals for the Ninth Circuit [FN78] on grounds which included its defence under the safe harbour in section 512 (d) of the DMCA. The court stated that it did not accept that the section would never apply to secondary infringers but that the issue would be more fully dealt with at trial. However, it recorded that the plaintiffs raised significant questions as to the applicability of the statute, including:

(1) whether Napster is a service provider as defined in § 512 (d);

(2) whether copyright holders had to provide "official" notice of infringing activity in order that it would have the requisite knowledge of infringement;

(3) whether Napster had complied with § 512 (i) in relation to its compliance policy.

The Court of Appeals agreed that the balance of hardships tipped in favour of the plaintiffs but found that the scope of the injunction required modification. The court found that contributory liability could potentially be imposed only to the extent that Napster

(1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings;

(2) knows or should know that such files are available on the Napster system; and

(3) fails to act to prevent "viral" distribution of the works

...

The mere existence of the Napster system, absent actual notice and Napster's failure to remove the offending material is insufficient to impose contributory liability.

Napster could be vicariously liable when it "fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed on its search index".

The result was that the injunction was overbroad, as

> it places on Napster the entire burden of ensuring that no "copying, downloading, uploading, transmitting, or distributing" of plaintiffs' works occur on the system. As stated we place the burden on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content. Napster however also bears the burden of policing the system within the limits of the system. Here, we recognize that this is not an exact science in that the files are user named. In crafting the injunction on remand, the district court should recognize that Napster's system does not currently appear to allow Napster access to users' MP3 files.

The injunction was therefore affirmed in part, reversed in part and remanded. It was to remain stayed until modified by the District Court to conform to the appellate opinion.

***73** In June 2001, a Federal Appeals panel rejected Napster's request for en banc review by a full eleven-judge panel of the Court of Appeal's decision. Napster argued, inter alia, that the Court of Appeal had fundamentally undermined the DMCA by failing to address the applicability of the safe harbour in section 512 (d) and by ordering injunctive relief that required Napster to monitor its service, contrary to the express provisions of the DMCA. [FN79] No decision has been announced at the time of writing as to whether Napster will petition the Supreme Court.

Conclusion

The DMCA then failed Napster. The matter is still at an interlocutory stage, although the likelihood of the case continuing to proceed to trial is uncertain. If it does not, then the Court of Appeal's opinion creates a dangerous precedent, imposing an obligation to monitor where Congress had intended the opposite. The

polarisation of the community over the case may have influenced the outcome; however, it does not bode well for the DMCA. Indeed the case has prompted extended hearings by the Senate Judiciary Committee to consider whether the DMCA ought to be amended, all of which makes one wonder how the E-Commerce Directive will fare, given that it is an import which is not consistent with the legal cultures of many of the Member States.

FN Victoria McEvedy is a New York attorney and a solicitor of England and Wales, New South Wales, Australia and New Zealand. She follows internet and intellectual property law. You may contact her on vmcevedy@aol.com.

FN1. In fact the relevant statute is the Online Copyright Infringement Liability Limitation Act, which was incorporated as Title II of the DMCA, Pub. L. No. 105-304. It amends Chapter 5 of Title 17 U.S.C. It was signed into law on October 28, 1998. The DMCA was enacted to bring U.S. law into compliance with private international law and in particular with the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty of 1996 which also introduced the "black box" measures to protect authors against the circumvention of technology used in protecting copyright management information. These measures were enacted in Title I of the DMCA.

FN2. Directive on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internet Market (2000/31) [2000] O.J. L178/1.

FN3. For example, the Communications Decency Act 1996, 47 U.S.C. § 223. Pub. L. No. 104-104 509 enacted a federal "Good Samaritan" defence for ISPs against state law causes of action for defamation. See § 230 (c) (1), (2) (A) and (d) (3). Although parts of that statute related to its indecency provisions were struck down in Reno v. ACLU 521 U.S. 844 (1997) the relevant provisions were unaffected and have proved highly effective. See Zeran v. America Online Inc. 129 F. 3d 327 (4th Cir. 1997), cert. denied 118 S. Ct 2341 (1998) and Blumenthal v. Drudge. 992 F. Supp. 44 (D.D.C. 1998) and Ben Ezra, Weinstein & Co. Inc. v. America Online, Inc. 4 I.L.R. (P. & F.) 620 [10th Cir, 2000]. It has also proved applicable to non-defamation cases, see Aquino v. Electriciti, Inc. 26 Media L. Rep. (BNA) 1032 (Cal. Super. Ct 1997) (negligence, intentional infliction of emotional distress, breach of contract).

FN4. See A&M Records, Inc. v. Napster, Inc., No. 99-05183, 2000 WL 573136 (N.D. Cal. May 12, 2000) (motion for summary judgment); A&M Records, Inc. v. Napster Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000) (motion for preliminary injunction) A&M Records, Inc. v. Napster, Inc., 7 I.L.R. (P. & F.) 3004 (appeal against preliminary injunction).

FN5. Nimmer on Copyright, Lexis Publishing at § 12B.01[C][2] p. 12B-18 explains that these are something less than complete exemptions in that the party qualifying for one, may still be subject to an injunction, albeit a severely limited one. The safe harbours constitute affirmative defences. See Nimmer, ibid., at § 12B.06[A] p. 12B-53 n. 2. See Alfred C. Yen, "Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment" (2000) 88 Geo. L.J. 1883, who describes the Act as an "odd" solution to the problem of ISP liability, as while ISPs do not know if they are liable--owing to the confused state of the law on liability--they do know how to escape liability. Note that the DMCA clearly saves other grounds of defence. See 17 U.S.C. § 512 (1).

FN6. s.512 of the DMCA uses the term "service provider". Three of the four safe harbours share the definition of service provider in s.512 (k) (B): "as used in this section ... the term 'service provider' means a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A)." The remaining "mere conduit" exception uses the definition in s.512 (k) (1) (A): "As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Nimmer, ibid., at § 12B.03[B][2] p. 12B-34 notes that the definition is sufficiently broad to include all types of entities affording access including schools and universities and, it appears, corporations and firms providing intranets and other facilities--even if only to their own employees.

FN7. There are three theories for potential liability for copyright infringement: direct liability, and the two categories of secondary liability; namely vicarious liability and contributory liability. However, for secondary liability, direct infringement must first be established. Only direct liability is statutory, see

17 U.S.C. § 501 (a). Vicarious liability for copyright infringement was developed by the Second Circuit as an extension of the doctrine of respondeat superior. Contributory liability for copyright infringement originated from the rule in tort that one who knowingly participates in or furthers a tortious act is jointly and severally liable with the primary tortfeasor. The DMCA's safe harbours offer protection from direct and to a limited extent, secondary, liability and was essentially intended to codify the result in Religious Technology Center v. Netcom Online Communications Services Inc. 907 F. Supp. 1361 (N.D. Cal. 1995) (rejecting direct liability for owners of machinery or systems used to make copies by third parties as some element of volition or causation must be present despite statute's strict liability). See H. Rep. No. 105-551 (I), p. 11: "The bill distinguishes between direct infringement and secondary liability, treating each separately ... As to direct infringement, liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another. Thus the bill essentially codifies the result in [Netcom]."

FN8. To take advantage of any of the four safe harbours, an ISP must show it (1) has "adopted and reasonably implemented, and informs subscribers and account holders of [its] system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of [its] system or network who are repeat infringers"; and (2) "accommodates and does not interfere with standard technical measures" (§ 512 (i) (1) (A) and (B)). The technical measures are defined in § 512 (i) (2) as "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, multiindustry 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". Nimmer, n. 5 above, at § 12B.02[B][3]-12B-28 criticises Congress for legislating a "blank page" into law, given that there is currently no such consensus and no guarantee that one will emerge and points out a possible conflict with § 512 (i) (1) (A) if any eventual consensus requires monitoring.

FN9. See 17 U.S.C. § 512 (j) (1) (B).

FN10. Whether an ISP qualifies for one of the four safe harbours will not assist it in qualifying for any of the others. Each of them are separate and distinct with their own exclusive criteria. See Nimmer, n. 5 above, § 12B.06[A] p. 12B-53.

FN11. Note that the word conduit is not used in the section, but only in the legislative history. See Commerce Rep. (DMCA) H.R. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998), p. 63; S. Rep. (DMCA) No. 105-190, 105th Cong., 2d Sess. (May 11, 1998) p. 54.

FN12. s.512 (a) has the following conditions:
"(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
(2) the transmitting, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing; or provision of connections; and
(5) the material is transmitted through the system or network without modification of its content."

FN13. See Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 52 describes caching, "which is used on some networks to increase network performance and to reduce network congestion generally, as well as to reduce congestion and delays to popular sites ... the material in question is stored on the service provider's system or network for some period of time to facilitate access by users subsequent to the one who previously sought access to it ...".

FN14. s.512 (b). The conditions are
"(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in paragraph (A) at the direction of that other person;

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

(2) Conditions--the conditions in paragraph (1) are:

(A) the material ... is transmitted to the subsequent user ... without modification to its content ... ;

(B) the service provider ... complies with rules concerning the refreshing, reloading, or other updating of the material when specified ... in accordance with a generally accepted industry standard ... only if those rules are not used ... to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return ... the information that would have been available to that person if the material had been obtained by the subsequent users ... directly ... only if that technology--(i) does not significantly interfere with the performance of the provider's system or network or with intermediate storage of the material; (ii) is consistent with generally accepted industry standard communications protocols; and (iii) does not extract information from the provider's system or network ... ;

(D) if the person described in paragraph (1) (A) has in effect a condition that a person must meet prior to having access to the material, such as ... payment of a fee or provision of a password or other information, the service provider permits access to the stored material ... only to users of its system or network that have met those conditions and

(E) if the ... material [is] available online without the authorisation of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement ... only if--(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled ... ".

FN15. See Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 53 which lists the following examples of user storage--"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" but not including 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".

FN16. See main text above for conditions.

FN17. See Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 56 which gives as examples "a search engine that identifies pages by a specified criteria; a reference to other on-line material, such as a list of recommended sites; a pointer that stands for an Internet location or address; and a hypertext link which allows users to access material without entering its address". See also Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 58 and S. Rep. (DMCA) No. 105-190, 105th Cong., 2d Sess. (May 11, 1998) p. 49 where this safe harbour is explained as follows: "Information location tools are essential to the operation of the Internet; without them, users would not be able to find the information they need. Directories are particularly helpful in conducting effective searches by filtering out irrelevant and offensive material. The Yahoo! directory, for example, currently categorises over 800,000 on-line locations and serves as a 'card catalogue' to the World Wide Web, which over 35,000,000 different users visit each month. Directories such as Yahoo!'s usually are created by people visiting sites to categorize them. It is precisely the human judgment and editorial discretion exercised by these cataloguers which make directories valuable." This safe harbour is therefore included to "promote the development of information location tools generally, and Internet directories such as Yahoo!'s in particular." The exemption therefore protects an ISP that links to sites that, unbeknown to it, are infringing. As Nimmer, n. 5 above, § 12B.05 [A][1] p. 12B-48 points out, this leaves the copyright owner with a remedy against the site itself. What the ISP is protected from is indirect infringement.

FN18. s.512 (d). "Information Location Tools--A service provider shall not be liable for monetary relief, or except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright 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 hypertext link, if the service provider-- ... [See (A)-(C) as set out in the main text above]". Condition (C) continuing in this case "except that, for purposes of this paragraph, the information described in subsection (c) (3) (A) (iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link."

FN19. Nimmer n. 5 above, § 12B.01[C][4] p. 12B-20.

FN20. The legislative history further indicates that "a common sense, fact based approach" should be taken to financial benefit, so that a financial benefit should not be regarded as "directly attributable to the infringing activity" where the infringer makes the same kind of payment as non-infringing users of the provider's service--for example a one-time set-up fee and flat, periodic payments for service, fees based on the length of the message or by connect time--unless the fee's value is plainly tied to providing access to infringing material. See Nimmer, n. 5 above, § 12B.04[A][2] p. 12B-38. Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 54., H. Rep. (DMCA) No. 105-551, Part 1, 105th Cong., 2d Sess. (May 22, 1998) p. 25, S. Rep. (DMCA) No. 105-190, 105th Cong., 2d Sess. (May 11, 1998) pp. 44-45. This is the standard applied in Religious Technology Center v. Netcom Online Communications, n. 7 above.

FN21. § § 512 (c) and (d) (emphasis added).

FN22. See Gershwin Publ'g Corp. v. Columbia Artists Management, Inc. 443 F. 2d 1159 (2d Cir. 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."). See also Shapiro, Bernstein and Co. v. H.L. Green Co., 316 F. 2d 304 (2d Cir. 1963) (For vicarious liability plaintiffs must show defendant has (1) right and ability to supervise the infringing activity; and (2) a direct financial interest in such activity). See also Fonovisa v. Cherry Auction Inc. 76 F. 3d at 259 (9th Cir. 1996).

FN23. n. 5 above.

FN24. Nimmer distinguishes the common law standard for constructive notice-- knows or should have known--for contributory liability from the statutory red flag standard while agreeing that the preclusion of financial benefit from an ISP with the right and ability to control is a codification of both elements of vicarious liability. See Nimmer, n. 5 above, § 12B.04[A][1] p. 12B-36 n. 18 and [A][2] p. 12B-38 n. 30.

FN25. Nimmer, n. 5 above, § 12B.04[A][2] p. 12B-36. See Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 44: "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 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."

FN26. § 512 (m) (1)--subject to any technical measures that may in future become standard. See n. 8 above.

FN27. Nimmer, n. 5 above, § 12B.04[A][2] p. 12B-38. Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 53.

FN28. See Nimmer, n. 5 above, § 12B.05[B][2] p. 12B-46 and 47. Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 57: the red flag would only wave if "the location was clearly, at the time the directory provider viewed it, a 'pirate' site ... where sound recordings, software, movies or books were available for unauthorized downloading, public performances, or public display". As Nimmer notes, this begs the question as to what renders a site plainly piratical? Furthermore, in a situation where a site may contain some questionable material, how is the cataloguer to make the legal determinations required for the complex evaluation of infringement

including whether the work is now in the public domain or is licensed or the use is fair?

FN29. § 512 (c) (1) (A) (i), (d) (1) (A).

FN30. § 512 (c) (1) (A) (ii), (d) (1) (B).

FN31. § 512 (b) (2) (E), (c) (1) (C), (d) (3).

FN32. See Nimmer, n. 5 above, at § 12B.04[A][3] p. 12B-39. The safe harbours being affirmative defences--once an ISP proves its eligibility and this would include some kind of assertion or evidence that it lacked knowledge--the burden shifts to the plaintiff to prove the contrary, a significant hurdle.

FN33. But not inconceivable--see Nimmer, n. 5 above, at § 12B.07[D][2] p. 12B-66.

FN34. See Nimmer, n. 5 above, at § 12B.07[C] p. 12B-64.

FN35. See § § 512 (b) (2) (E), (c) (1) (C), (d) (3). In relation to the information location tool safe harbour, on notification, rather than removing the material in question, the ISP must remove the link to such material and the notification must identify the reference or link. Note also that s.512 (h) provides for the issuing of subpoena to an ISP for the identification of an alleged infringer.

FN36. See Commerce Rep. (DMCA) H.R. Rep. No. 105-551, Part 2, 105th Cong., 2d Sess. (July 22, 1998) p. 54, "[N]either actual knowledge nor awareness of a 'red flag' may be imputed to a service provider based on information from a copyright owner or its agent that does not comply with the notification provisions ... ". By virtue of the reference in § § 512 (b) (2) (E), (c) (1) (C), (d) (3) to the notification procedures in § 512 (c) (3), which refer to the requirement in § 512 (c) (2), ISPs must appoint a designated agent. See § 512 (c) (2): "Designated Agent--the limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing the Copyright Office, substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent. (B) other contact information which the Register of Copyrights may deem appropriate ... "

FN37. "§ 512 (c) (3) Elements of notification--

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent or the law.

(vi) 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 owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent."

Nimmer, n. 5 above, at § 12B.04[B][2] p. 12B-40 points out the notable omission of the

requirement that the copyright be registered--surprising, given the formality. Registration would of course raise the presumption that the claim to copyright was valid.

FN38. See § 512 (c) (3) (B) (ii). However, that result follows only if clauses (A) (ii) identification of the work, (iii) identification of the infringing material and (iv) contact details of the complainer, are substantially met. However, the notification must be in writing and must be to a designated agent. Informal notice received from a rightholder does not of itself create knowledge or awareness, however: § 512 (c) (3) (B) (i). See ALScan Inc. v. RemarQ Communities Inc., 7 I.L.R. (P. & F.) 3003 [4th Cir. 2001] where failure to comply with a "substantially conforming" notice lost RemarQ its DMCA safe harbour.

FN39. Yen, n. 5 above.

FN40. § 512 (g) (1)-(2) (A) provides that an ISP "shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing".

FN41. As described in the legislative history. See H. Rep. (DMCA) No. 105-551, Part I, 105th Cong., 2d Sess. (May 22, 1998) p. 26.

FN42. The contents of the counter-notification are also prescribed--see § 512 (g) (3): "(A) a physical or electronic signature of the subscriber. (B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled. (C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled. (D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c) (1) (C) or an agent of such person."

FN43. The ISP is also immunised from liability for the restoration by § 512 (g) (4).

FN44. "512 (g) (2) ... (A) ... promptly ... notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification [from the subscriber] ... promptly provide the person who provided the notification ... with a copy of the counter notification, and inform the[m] that it will replace the removed material or cease disabling it in 10 business days; and

(C) replace the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c) (1) (C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network."

FN45. § 512 (f).

FN46. § 512 (g) (3) (C).

FN47. [2000] O.J. L178/1.

FN48. See the Explanatory Memorandum to the Commission's original proposal COM (1998) 586 final. See also Copyright Directive, Recital 16 which explains that liability in a "network environment" concerns not only copyright and related rights but also "defamation, misleading advertising, or infringement of trademarks" which are dealt with "horizontally" in the E-Commerce Directive (Art. 14 of the E-Commerce Directive uses the term "illegal activity").

FN49. On April 9, 2001, the Council of Europe and the European Parliament adopted a Directive on

the Harmonization of Copyright and Related Rights in the Information Society. Pending publication in the Official Journal, for text see Common Position of Council adopted on September 28, 2000 [2000] O.J. C344/1 as amended by the European Parliament legislative resolution of February 14, 2001 (A5-0043/2001). See Recital 16 to the Copyright Directive. The Copyright Directive harmonises key exclusive rights and exhaustively provides for both mandatory and optional exceptions thereto. It also expressly protects ISPs for temporary reproductions made by a technical process during the transmission of works which have no independent purpose. See Art. 5(1): "Temporary acts of reproduction referred to in Article 2, which are transient or incidental, which are an integral and essential part of a technological process whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance shall be exempted from the reproduction right provided for in Article 2." Recital 33 explains that this exception "should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of information". It also provides that Member States shall ensure that rightholders can apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. See Art. 8 (3) and Recital 58, which explains that in many cases "intermediaries are best placed to bring such infringing activities to an end" and thus--without prejudice to additional sanctions and remedies--rightholders should be able to seek injunctions against intermediaries. It further explains that this should be so "even where the acts carried out by the intermediary are exempted under Art. 5" and that the "conditions and modalities relating to such injunctions should be left to the national law of the Member States".

FN50. They may--like the DMCA's safe harbours--be considered less than full exemptions as each is subject to its own proviso: "This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems of requiring the service provider to terminate or prevent an infringement ... [and in the case of hosting] nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information." See Arts 12 (3), 13 (2) and 14 (3). The service provider may then still be compelled or enjoined by the courts despite the immunity. Further in relation to hosting sites in disregard of red flags, reference is made to claims for damages. See also Recital 45: "The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it."

FN51. See the Explanatory Memorandum to the Commission's original proposal COM (1998) 586 final.

FN52. The relevant section being s.4 of the E-Commerce Directive, entitled "Liability of intermediary service providers." Service providers are defined in Art. 2 as "any natural or legal person providing an information society service". The term "information society service" is defined in Art. 2 by reference to the definition in Directive 98/34 of the European Parliament and of the Council of June 22, 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services, Article 1 (2) [1998] O.J. L204/37. As amended by Directive 98/48 of the European Parliament and of the Council of July 20, 1998 amending Directive 98/34 laying down a procedure for the provision of information in the field of technical standards and regulations [1998] O.J. L217/18. Broadly, the definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. See Recital 17 of the E-Commerce Directive.

FN53. "Recipient of a service" is defined in Art. 2 of the E-Commerce Directive as "any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible". See also Recital 20 of the same.

FN54. Member States are to ensure that the service provider is not liable for the information transmitted, on condition that it "(a) does not initiate the transmission; (b) does not select the receiver

of the transmission; and (c) does not select or modify the information contained in the transmission." 12 (2) provides that "the acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission". See also Recital 43 which explains this exemption and that for caching.

FN55. The conditions are: "(a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, in a manner widely recognized and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."

FN56. For example La Ligue Contre le Racsime et l'Antisémitisme v. La Société Yahoo! Inc., Tribunal de Grande Instance de Paris No. RG 00/05308 No. 1/kl, Ordonnance de Référé rendue le 20 Novembre 2000, Jean-Jacques Gomez. Although that case concerned Yahoo!'s own sites, presumably the ruling applied to other sites selling Nazi memorabilia, including sites accessible through Yahoo!'s search functions.

FN57. This is consistent with the guiding principle that the exemptions only cover cases where the activity of the ISP is limited to the technical process of operating and giving access to a communication network over which third party information is transmitted or temporarily stored, solely for efficiency, where the activity is of a "mere technical, automatic and passive nature which implies that the [ISP] has neither knowledge of nor control over the information which is transmitted or stored". Recital 42.

FN58. Although Member States may require that ISPs inform authorities of such activity: Art. 15

FN59. See for example the United Kingdom's Regulation of Investigatory Powers Act which was given Royal Assent in July 2000.

FN60. See Recitals 47 & 48.

FN61. Recital 40.

FN62. Recital 46.

FN63. The Directive is to "constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information". These it suggests could be "developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States". Recital 40.

FN64. Recital 46. For example in France takedown is at present required only on judicial order by law 2000-719, August 2, 2000, p. 11903 modifying law 86-1067. Although a new Bill implementing the E-Commerce Directive will likely require take down on notice only, judicial involvement in take down is likely to be retained in certain circumstances at least. See http://www.assemblee-nationale.fr/projects/pl3134.asp.

FN65. For example that of the Global Business Dialogue on Electronic Commerce which is working towards a voluntary self-regulatory model IPR--specific notice and takedown procedure--which appears to be based closely on the procedure in the DMCA.

FN66. On December 6, 1999 record companies and music publishers, assisted by the RIAA (Recording Industry Association of America) issued suit against Napster for contributory and vicarious copyright infringement, violation of California Civil Code s.980 (a) (2), and unfair competition. See complaint, A&M Records v. Napster, Inc., No. 99-5183 (N.D. Cal.), 5 I.L.R. (P. & F.) 2088.

FN67. The motion was heard by Marilyn Hall Patel, chief judge of the U.S. District Court for the Northern District of California. See A&M Records, Inc. v. Napster, Inc., No. 99-05183, 2000 WL 573136 (N.D. Cal. May 12, 2000).

FN68. The following facts were agreed by the parties for the purposes of the motion. Once a Napster user logs on using Napster's MusicShare software or browser, they become connected to one of Napster's servers. MusicShare then reads the list of the MP3 files on the user's hard drive that the user has elected to make available for sharing. That list is uploaded (the song is not uploaded, only its file name) to the directory and index on the server for the period that the user is logged on. A user searching for a song will highlight and thereby select a file from the list generated in response to the search. Napster's servers will then communicate with requesting and host (to the song) computers and facilitate a connection between them for the downloading of the song.

FN69. See s.512 (a) (5). The plaintiffs also relied on the words in subsection 512 (k) (1) (A)--the relevant definition of "service provider"--which requires that the transmitting or routing must take place "between or among points specified by a user". Napster said that the server got the necessary I.P. address information from the host user so that the requester could connect to the host directly with the actual transfer of the song taking place over the internet and not through Napster's servers. Apparently, at the time of the suit Napster stayed involved in the entire download process to ensure successful transmission, but this feature was disabled in January 2000. See Ariel Berschadsky, "RIAA v. Napster: A Window onto the future of Copyright law in the Internet Age" (from (2000) 18 J. Marshall J. Computer & Infor. L. 755, at n. 17. Alternatively, the plaintiffs argued that if the requesting user's and the host user's computers were considered to be part of the Napster "system" then Napster would fall foul of the requirement that the material should not be stored longer than necessary.

FN70. The court reasoned that even assuming that the users' computers formed part of the system, the transmission of an actual file still bypassed the Napster server and if the browsers were considered part of the system, the transmission went from one part of the system to another or between parts of the system--and not through the system. As to whether Napster was "providing connections", it found that it was not as though the server delivered the host's address to the requester; the actual connection between them was made through the internet, so that even on the most favourable view, Napster was not a conduit for the connection itself but only for the address information. Noting that neither party had made adequate submissions on "routing", the court also found that this did not occur through the Napster system.

FN71. It was alleged that Napster only adopted a policy after suit had been issued and that it failed to enforce it in a meaningful way.

FN72. It placed weight on the fact that Napster did not require the real name and other identifying information of subscribers and while it blocked repeat infringers' passwords, it did not block their I.P. addresses, enabling them to re-subscribe with new identities.

FN73. A&M Records, Inc. v. Napster Inc. 114 F. Supp. 2d 896 (N.D. Cal. 2000) heard July 26, 2000 by Chief Judge Patel.

FN74. See opinion of the court, Napster, ibid., at 919, fn. 24.

FN75. Napster also argued that its users had not committed direct infringement relying on the defences of fair use and the staple article of commerce doctrine.

FN76. Napster was ordered to comply with the injunction by midnight on July 28, 2000, but obtained an emergency stay of pending appeal.

FN77. By filing a written plan by September 5, 2000 with a method for identifying works for which they owned the rights and to post a $5 million bond against Napster's losses on the reversal or vacation of the injunction.

FN78. See opinion of February 12, 2001, A&M Records, Inc. v. Napster, Inc. 7 I.L.R. (P. & F.) 3004. Heard on October 2, 2000 by the three-member Court of Appeals for the 9th Circuit comprising Chief

Justice Schroeder and circuit judges Beezer and Paez.

FN79. s.512 (m) DMCA. See Napster's Petition for Rehearing and Rehearing En Banc, Appeal Nos 00-16401 and 00-16403, a copy of which can be found at http:// www.napster.com.

END OF DOCUMENT