5-1-2014

Internet File Sharing: The Liability of the Host and The Users

Tat Chi Chio

Internet File Sharing:

The Liability of the Host and The Users

Tat Chi Chio

1. Introduction

The Internet is one of the most important innovations in the Twentieth Century. It facilitates communication between people around the world by rapid, accurate, and inexpensive distribution of information. A person with a personal computer and Internet connection can communicate with people from around the world anytime and anywhere. With this capability, the person can disseminate and/or receive information instantly.

In the mid-1960's, the Advanced Research Project Agency (ARPA) began developing data networks that would connect computers together so that scientists could share computers. Leonard Kleinrock was instrumental in the development of the government-supported data network called the ARPANET that would use the technology that is known as "packet switching" today. On October 29, 1969, the first Host-to-Host message was sent on the Internet from UCLA to Stanford Research Institute.[1]

[1] www.lk.cs.ucla.edu/Personal_history.html

Based on the Internet's structure, several powerful and efficient information exchange technology have been developed: Peer-to-Peer network, File-Hosting service, and Video-Sharing websites. Because these technologies are cutting-edge, the legal responsibility of the providers of these technologies and their users is still an unknown area for each of the parties. In this paper, we are going to explore the legal responsibility of each of the parties.

2. Background

File sharing between individuals within a computer network was developed by Sun Microsystems for their UNIX system.[2] The advantage of sharing digital copies of files over distribution of physical copies of the same files is that the information can be distributed more rapidly and easily.[3] The advent of the Internet and file transfer protocol ("FTP") system allows sharing of information between individuals separated by great distance.[4] A person with a valid password to the FTP website can download and copy files onto their computer for later use.[5]

1. Peer-to-Peer File Sharing Technology

In 1999, Shawn Fanning created peer to peer (P2P) file sharing software called "Napster" that allowed computer users to share music over the Internet.[6] Napster enabled users to exchange songs through centralized computer servers. After Napster was shut

---

[2] *See* Howard P. Goldberg, Note, *A Proposal for an International Licensing Body to Combat File Sharing and Digital Copyright Infringement,* 8 B.U. J. SCI. & TECH. L. 272 (2002).
[3] *See id.*
[4] *See id.*
[5] *See id.*
[6] *See* Hayward, J., *Grokster Unplugged: It's Time to Legalize P2P File Sharing*, Selected Works, 2007, located at http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=john_hayward.

down, other P2P file sharing programs emerged such as Kazaa, Grokster, Morpheus, and Streamcast. They allowed users to exchange songs directly from one computer to another without employing a central server.[7]

P2P file sharing programs allow a user's computer to connect to a network, in which the computer initiates communication and responds to queries from other computers in the same network without going through an intermediate server.[8] In a P2P network, users download files by querying the other users on the same network for a file of interest and requesting a copy of the file when the file is located.[9] At the same time, users can respond to queries for files from other users on the same network. If the queried user has the requested file on his/her computer, the computer can directly send a copy of the file to the querying user's computer.[10] On the other hand, a client-server communications architecture is employed in a non-P2P network. A user computer connected to the network can only communicate with other user computers via the server.[11]

Since computers connected to P2P networks can communicate with each other without a central server, they provide several advantages over the server-client architecture. First, a breakdown of any peer in a P2P network would not seriously affect the operation of the network. The contents are shared and stored between users without a central server. Each computer in the network can act as a client or server for the other computers in the network. Thus, there are numerous servers for a given peer requesting

---

[7] *See id.*
[8] *See* Richard Swope, Comment, *Peer-to-Peer File Sharing and Copyright Infringement: Danger Ahead for Individuals Sharing Files on the Internet*, 44 Santa Clara L. Rev. 861 (2004).
[9] *See id.*
[10] *See id.*
[11] *See id.*

files. However, since the server in the server-client architecture controls all the contents, a breakdown of the server may result in the damage and loss of the contents. Second, P2P networks provide a consumer-centered medium for users: every user can determine which content to share and control the schedule of operation. Finally, P2P networks can handle a large number of users and offers a reliable, flexible, and inexpensive multimedia communications platform.[12]

With the flexibility and convenience offered by P2P networks, copyright infringements are more likely to occur in P2P networks. Since every computer connected to the network can act both as a client and a server, every user in the network can receive and distribute both copyrighted and un-copyrighted contents. When users share copyrighted contents without permission, they are committing copyright infringements. In addition, because there is no central server, the ability to control access to copyrighted contents is limited. Thus, P2P networks are easily used to commit copyright infringements.[13]

BitTorrent is a P2P application that operates to share a huge file by dividing the file into small pieces. When a peer downloads a file, it connects to BitTorrent's centralized software called the tracker, which will return a list of peers that have the file. The download will establish connection with other peers simultaneously and downloads the pieces of the file from the peers who have them. There are two types of peers in

[12] *See* Chunhsien Sung and Po-Hsian Huang, *Copyright Infringement and Users of P2P Networks in Multimedia Applications: The Case of the U.S. Copyright Regime*, Peer-to-Peer Networking and Application, Springer Science + Business Media, LLC 2012.
[13] *See id.*

BitTorrent: seeds and downloaders. The seeds are peers who have all the pieces of the file and the downloaders are peers who do not have all the pieces of the file.[14]

2. One-Click Hosting Services

In 2005, a new type of file sharing service has been developed such as MegaUpload and RapidShare. They are commonly known as One-Click Hosting (OCH).[15] These sites allowed users to share files through dedicated centralized servers without relying on an underlying P2P infrastructure. A user is able to share large files with other users in the following steps: (1) upload the file on an OCH server through an upload website interface; (2) share the URL for the file provided by the OCH service with other users either publicly (e.g. post the URL on personal webpages or blogs) or privately (e.g. share the URL through email); (3) users can download the file through a download website interface by clicking on the URL.[16]

OCH services provide several advantages over P2P networks. First, files uploaded on OCH services are always available, whereas the files are available only when peers carrying the files are connected to the network. Second, in OCH services, the IP addresses of the downloaders and uploaders are known only to the OCH services, whereas in P2P networks, peers have to disclose their IP addresses when they are uploading or downloading a file. Third, less popular contents can be found more often on OCH services than in P2P networks. Fourth, the performance of OCH services are higher than P2P networks. Experiments show that a Premium RapidShare user receives higher

---

[14] *See* Dongyu Qiu and R. Srikant. *Modeling and Performance Analysis of BitTorrent-Like Peer-to-Peer Networks,* SIGCOMM'04 Aug. 30-Sept. 3, 2004.
[15] *See* Demetris Antoniades, Evangelos P. Markatos, and Constantine Dovrolis. *One-click Hosting Services: a File-sharing Hideout*, In Proc. of ACM IMC '09.
[16] *See id.*

throughput than a BitTorrent user downloading the same file. Finally, OCH services encourage users to upload more files by providing higher download throughput to frequent uploaders. This results in more contents available in OCH services.[17]

3. Video-sharing website: YouTube

Like P2P networks and OCH services, video-sharing website such as YouTube allows user to share contents on the Internet. YouTube allows users to upload video contents and view video contents with their computer. The major difference between YouTube and other file sharing technology is that YouTube users can view video contents without downloading them.[18] Thus, YouTube users are able to view video contents on YouTube so long as their devices are connected to the Internet.[19]

4. Liability of P2P network

Before P2P file sharing, music lovers downloaded music from websites operated by the website owner. In *UMG Recordings, Inc. v. MP3.com,* users were able to access music recordings posted on MP3.com website by proving that they already owned the CD version of the recording or by purchasing the CD from one of defendant's cooperating online retailers. Then, the users could access the recordings with a computer from anywhere via the Internet.[20]

The court rejected the defendant's fair use and other defenses and held that the defendant has infringed plaintiff's copyrights. The court explained that, for the first

---

[17] *See id.*

[18] *See* Lior Katz, *Viacom v. YouTube: An Erroneous Ruling Based on the Outmoded DMCA*, 31 Loy. L.A. Ent. L. Rev. 101 (2011). Available at: http://digitalcommons.lmu.edu/elr/vol31/iss2/2

[19] *See Id.*

[20] *See UMG Recordings, Inc. v. MP3.COM, Inc.,* 92 F.Supp.2d 349, 350 (S.D.N.Y. 2000).

factor of the fair use, defendant's "space shift" use of MP3.com was not transformative. It was essentially retransmitting unauthorized copies in another medium. Moreover, defendant's activities infringed plaintiff's right to license the copyrighted sound recordings to others for reproduction.[21]

Although P2P file sharing programs such as Napster provided many advantages over the client-server architecture, it also represented a huge threat to the music industry. Majority of the users shared copyrighted music by using Napster on the Internet without permission.[22] In 2001, the United States Court of Appeals for the Ninth Circuit held that plaintiffs demonstrated a likelihood of success on their infringement claims and upheld the district court's preliminary injunction with modified scope.[23]

1. The Napster Case

The Court of Appeals' opinion discussed, among other things, (I) Napster's contributory liability;[24] (II) Napster's vicarious liability;[25] (III) applicability of Audio Home Recording Act;[26] and (IV) Napster's claim that it was entitled to the protection of the "safe harbor" under Digital Millennium Copyright Act ("DMCA").[27]

I. Contributory Liability

Contributory liability requires that the defendant knew or have reason to know of direct infringement and materially contributes to the infringing activity.[28] The Ninth

---

[21] *See id.* at 351-353.
[22] *See A&M Records, Inc. v. Napster, Inc.,* 239 F.3d 1004, 1014 (9th Cir. 2001).
[23] *See id.*
[24] *See id.* at 1020.
[25] *See id.* at 1022.
[26] *See id.* at 1024.
[27] *See id.* at 1025.
[28] *See id.* at 1020-1022.

Circuit found that Napster had both actual and constructive knowledge of direct infringement.[29] However, the court refused to "impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights."[30] For a computer system operator to have sufficient knowledge, the copyright holder must inform the computer system operator that infringing material is available on his system. If the computer system operator fails to remove such materials after the copyright holder's notice, the operator knows of and contributes to direct infringement. However, the computer system operator cannot be liable for contributory infringement merely because the system allows for exchange of copyrighted material if there is no specific information that identifies infringing activity.[31] Because Napster had actual knowledge that specific infringing material is available on its system and it failed to remove the material, Napster was found to have the knowledge requisite to contributory infringement. The court also found that Napster materially contributed to the infringing activity.[32] Because Napster had knowledge, both actual and constructive, of direct infringement and materially contributed to the infringing activity, the court concluded that plaintiffs had demonstrated a likelihood of success on the merits of the contributory copyright infringement claim.

---

[29] *See id.* at 1020. Napster had actual knowledge because "(1) a document authored by Napster co-founder Sean Parker mentioned 'the need to remain ignorant of users' real names and IP address since they are exchanging pirated music'; and (2) the Recording Industry Association of America ("RIAA") informed Napster of more than 12,000 infringing files, some of which are still available." Napster had constructive knowledge because "(a) Napster executives have recording industry experience; (b) they have enforced intellectual property rights in other instances; (c) Napster executives have downloaded copyrighted songs from the system; and (d) they have promoted the site with 'screen shots listing infringing files.'"

[30] *See id.* at 1020-1021.

[31] *See id.* at 1022.

[32] *See id.*

II. Vicarious Liability

To find a defendant liable for vicarious liability, it must be shown that the defendant has the right and ability to supervise the infringing activity and has a direct financial interest in such activities.[33] Napster was found to have financial benefit because the availability of infringing material attracts customers and Napster's future revenue is directly dependent upon the size in its user base.[34] As for the supervision requirement, Napster retained the right to control access to its system because Napster expressly reserved the "right to refuse service and terminate accounts in its discretion." To escape vicarious liability, the reserved right to police must be exercised to its fullest extent. The court concluded that even though Napster's ability to police was limited by their system's architecture, it had the ability to locate infringing material listed on its search indices and the right to terminate users' access to the system.[35] Therefore, based on the finding that Napster failed to police the infringing activity and its direct financial interest from such activity, the court concluded that plaintiffs have demonstrated a likelihood of success on the merits of the vicarious liability.

III. Defenses

Napster raised the protection under Audio Home Recording Act ("AHRA") and of the "safe harbor" from copyright infringement suits for Internet service providers under the Digital Millennium Copyright Act ("DMCA") as two of its defenses.[36] The

---

[33] *See id*.
[34] *See id.* at 1023.
[35] *See id.* at 1023-1024.
[36] *See id.* at 1024-1025.

court rejected Napster's AHRA defense[37] and indicated that whether Napster was eligible for the section 512(d) safe harbor protection for service providers was an issue to be more fully developed at trial. The undecided questions for determining whether Napster was eligible for the safe harbor protection includes: " (1) whether Napster is an Internet service provider as defined by 17 U. S. C. 512(d); (2) whether copyright owners must give a service provider 'official' notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; (3) whether Napster complies with 512(i), which requires a service provider to timely establish a detailed copyright compliance policy."

2. The Grokster case

After Napster was shut down, other P2P file sharing programs emerged such as Kazaa, Grokster, Morpheus, and Streamcast. Grokster and StreamCast did not use servers to intercept the content of the search requests or to mediate the file transfers by the users with the software. They allowed users to exchange files directly from one computer to another. Grokster and Streamcast were sued for copyright infringement. The suit was dismissed by the district court and the Ninth Circuit affirmed. However, the U.S. Supreme Court reversed the Ninth Circuit's ruling.[38]

The Ninth Circuit held that Grokster and Streamcast were not contributorily liable because the software was capable of substantial noninfringing uses. They had no actual knowledge of the infringing activities because of the decentralized architecture of their

[37] *See id.* Napster's AHRA defense failed because computers and their hard drives are not digital audio recording devices under the plain meaning of the AHRA's definition because their primary purpose is not to make digital audio copied recordings. Furthermore, computers do not make digital music recordings as defined by the AHRA.

[38] *See MGM Studio Inc., v. Grokster*, 545 U.S. 913, 922.

software. Moreover, Grokster and Streamcast did not materially contribute to their users' infringing activities because they did not provide search, retrieval, or storage of the infringing files.[39]

The Ninth Circuit also held that Grokster and Streamcast were not vicariously liable because they did not have the power to control or supervise. Grokster and Streamcast did not have the ability to monitor or control the use of the software, did not reserve the right to control the use of the software, and had no independent duty to police infringing activities.[40] Based on these findings, the Ninth Circuit affirmed the district court's ruling that Grokster and Sreamcast were not contributorily or vicariously liable.

The Supreme Court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[41] In order not to compromise legitimate commerce or discourage innovation having a lawful purpose, the Supreme Court also said that neither mere knowledge of infringing uses, potential or actual nor ordinary acts incident to product distribution would be sufficient to subject a distributor to liability.[42] Evidence supported a finding of liability was identified by the Supreme Court. First, both of Grokster and StreamCast advertised themselves as Napster's replacement. Their efforts to supply services to former Napster users indicate an intent on the part of each to bring about infringement. Second, Neither company attempted to develop any mechanism to reduce infringing activity using their software. Third, their profits come from selling advertisement space,

[39] *See id.* at 927-928.
[40] *See id.*
[41] *See id.* at 936-937.
[42] *See id.*

by directing ads to the screens of computers running their software. The more the software is used, the more ads are sent out and thereby the higher profits for them.[43] Because of substantial evidence showing Grokster and StreamCast's intent to induce the users of their software to commit copyright infringement, the Supreme Court reversed the Ninth Circuit's ruling in favor of Grokster and StreamCast.

Based on *Napster* and *Grokster*, the knowledge and inducement of infringing activities are the key component to attach liability to a P2P file sharing software distributor. Thus, to avoid liability, the P2P file sharing software distributor must not maintain a central search index and not induce users to exchange copyrighted works without permission using the software.

5. Liability of File-Hosting Service

A second kind of file sharing technology is called file-hosting service or one-click hosting. Examples of file-hosting service are RapidShare and MegaUpload. As in the case of RapidShare, the users must register for a free account or acquire a premium account by paying a fee. The registered users can upload files from her computer. The servers automatically generate a download link (a URL) for each uploaded file and send the URL to the uploader. The uploader can share the uploaded files with other users by sharing the URL. RapidShare's website does not offer a search function and does not have an index for files stored on its servers.[44]

The district denied Perfect 10's motion for preliminary injunction because Perfect 10 did not establish that it is likely to succeed on the merit. To find the defendant liable

[43] *See id.* at 939-940.
[44] *See Perfect 10, Inc. v. RapidShare A.G.*, Case No. 09-CV-2596 H at p. 2-3.

for contributory infringement, the plaintiff must show that the defendant (1) has knowledge of another's infringement and (2) either (a) materially contributes to[45] or (b) induces that infringement.[46] The district court concluded that RapidShare had actual, specific knowledge of direct infringement because RapidShare received notice of hundreds of copyrighted Perfect 10 images that were found on its servers.[47]

However, the district court ruled that RapidShare did not materially contribute to the infringement because it did not index user materials and did not have a search function for the users to search for particular files. Also, RapidShare was using information provided by Perfect 10 to locate and remove infringing images, and was taking independent steps to identify, locate, and remove infringing materials.[48]

The district court also concluded that RapidShare did not induce users' infringing activity. There are a number of substantial lawful uses for the RapidShare service.[49] Also, RapidShare's Condition of Use prohibit copyright infringement, and RapidShare removes infringing materials, terminates infringers' accounts, and independent searches for and remove infringing materials when given takedown notices by copyright owners.[50]

Therefore, because of the lack of sufficient evidence to prove that RapidShare materially contributed to the infringements of its uses and that RapidShare induced its

---

[45] *See A&M Records v. Napster, Inc.* 239 F.3d 1004.
[46] *See MGM Studios Inc, v. Grokster,* 545 U.S. 913.
[47] *See RapidShare*, Case No. 09-CV-2596 H at p. 7-8.
[48] *See id.* at 8-10.
[49] *See id.* at 10-11. "For example, RapidShare provides users with a secure location to store and access files from anywhere that there is Internet access. Additionally, RapidShare provides data storage capacity which may present businesses with an economical alternative to buying and maintaining their own storage-related computer hardware. RapidShare has presented evidence that the German edition of PC world magazines has twice used RapidShare to host file of anti-virus software for its reader to download. Moreover, Plaintiff has not presented evidence to show that RapidShare's software system was 'engineered, disseminated, and promoted explicitly for the purpose of facilitating piracy of copyrighted [material] and reducing legitimate sales of such [materials] to that extent.'"
[50] *See id.*

users' infringing activity, the district concluded that Perfect 10 is not likely to succeed on the merit. Thus, the district court denied Perfect 10's motion for preliminary injunction.

The file-hosting service, RapidShare, was not liable to infringement because RapidShare had a substantial number of lawful uses, actively and independently removed infringing materials, and promptly removed infringing materials in response to the takedown notice from the copyright owners. It demonstrated the importance of the host's cooperation with the copyright owners and its actively policing of the infringing activities. Therefore, to avoid liability, the host will have to actively police infringing activities on its site.

6. Liability of Video Sharing Website

The Digital Millennia Copyright Act ("DMCA") offers a series of safe harbors that allow qualifying service providers to limit their liability for claims of copyright infringement based upon (a) "transitory digital network communications," (b) "system caching," (c) "information residing on systems or networks at the direction of users," and (d) "information location tools."[51] To be protected by any one of the safe harbors, one must in fact be a "service provider," defined as "a provider of online services or network access, or the operator of facilities therefor."[52] A qualifying service provider must satisfy "condition of eligibility," including the adoption and reasonable implementation of a policy that "provides for the termination in appropriate circumstances of subscriber and account holders of the service provider's system or network who are repeat infringers," and "accommodates and does not interfere with standard technical measures" that are

[51] 17 U.S.C. 512(a)-(d)
[52] 17 U.S.C. 512(k)(1)(B)

"used by copyright owners to identify or protect copyrighted works."[53] Moreover, a qualifying service provider must satisfy the requirements of a specific safe harbor.

A third kind of file sharing technology is the video sharing website such as YouTube. YouTube permits registered users to upload and view video clips for free. During the registration process, the users are required to accept YouTube's Terms of Use agreement, which states that the user "will not submit material that is copyrighted … unless he is the owner of such rights or has permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein."[54] YouTube makes one or more exact copies of the video in its original file format. During the transcoding process, YouTube makes one or more additional copies of the video in "Flash" format. When users request playback of a video, the content is streamed to the user's computer. YouTube also uses a computer algorithm to identify and recommend clips that are related to a video the user watches.[55]

The Second Circuit held that 17 U.S.C. 512 (c)(1)(A) requires knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement.[56] The record raises material issues of fact regarding YouTube's actual knowledge or awareness of specific instances of infringement.[57] Because of numerous instances point to the direction that YouTube might actually knew about specific instances of infringement, The Second Circuit vacated the summary judgment granted to

---

[53] 17 U.S.C. 512(i).
[54] *See Viacom international v. YouTube*, 676 F.3d 19, 28 (2nd Cir. 2012).
[55] *See id.*
[56] *See id.* at 32.
[57] *See id.* at 33-34. For example, Patrick Walker, director of video partnerships for Google and YouTube, requested that any "clearly infringing, official broadcast footage" from a list of top Premier League clubs be taken down in advance of a meeting with the heads of "several major sports teams and leagues." YouTube ultimately decided not to make a bid for the Premier League rights, but the infringing content allegedly remained on the website.

YouTube and remanded the case for further proceeding on whether "any specific infringements of which YouTube had knowledge or awareness correspond to the clips-in-suit in these actions."[58]

The Second Circuit held that the willful blindness doctrine may be applied to demonstrate knowledge or awareness of specific instances of infringement under 512(c)(1)(A). 17 U.S.C. 512 (m) provides that safe harbor protection shall not be conditioned on "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)." The Second Circuit reasoned that a common law principle is abrogated only if the statute "speaks directly to the question addressed by the common law." Because the statute does not "speak directly" to the willful blindness doctrine, section 512(m) only limits the doctrine but does not abrogate it.[59]

The Second Circuit concluded that the "right and ability to control" infringing activity under 512(c)(1)(B) "requires something more than the ability to remove or block access to materials posted on a service provider's website." However, the case law does not provide how to define the "something more" that is required. Some cases involve a service provider exerting substantial influence on the activities of users, without necessarily acquiring knowledge of specific infringing activity. Thus, this issue is remanded to the district court for further proceeding.[60]

The Second Circuit concluded that 512(c) covers service providers including YouTube. The broader definition of "the term 'service provider' means a provider of

[58] *See id.*
[59] *See id.* at 35.
[60] *See id.* at 38.

online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)." Because of the absence of a limitation on the ability of a service provider to modify user-submitted content, 512(c) covers more than mere electronic storage lockers.[61] Upon reviewing the record, the Second Circuit held that three of the YouTube software functions - replication, playback, and the related video feature – occur "by reason of the storage at the direction of a user" within the meaning of 17 U.S.C. 512(c)(1). However, further factfinding regarding the syndication of YouTube videos to third parties is required.[62]

In *Cartoon Network v. CSC Holdings*, the Second Circuit held that CSC holdings ("Cablevision") was not liable for direct infringement. First, the court found that the work was embodied in the buffer because every second of an entire work was placed, one second at a time, in the buffer. However, the data did not remain in any buffer for more than 1.2 seconds and the data was quickly and automatically overwritten as soon as it was processed, so the work were embodied in the buffer for only a "transitory" period. Thus, the work was not "fixed" in this case.[63]

Second, the court concluded that copies made by the RS-DVR system were made by the customer, and Cablevision's contribution to this "reproduction by providing the system does not warrant the imposition of direct liability." The court based its conclusion on "by selling access to a system that automatically produces copies on

---

[61] *See id.* at 39.

[62] *See id.* at 39-40. "Transcoding involves 'making copies of a video in a different encoding scheme' in order to render the video 'viewable over the Internet to most users.'" "The playback process involves 'delivering copies of YouTube videos to a user's browser cache' in response to a user request." The related videos function's "indexing and display of related videos retain a sufficient causal link to the prior storage of those videos." Its "algorithm 'is fully automated and operates solely in response to user input without the active involvement of YouTube employees.'" Thus, the Second Circuit affirmed the district court's ruling that these three software functions are protected by the 512(c) safe harbor.

[63] *See Cartoon Network v. CSC Holdings, Inc.,* 536 F.3d 121, 129-130 (2nd Cir. 2008).

command, Cablevision more closely resembles a store proprietor who charges customers to use a photocopier on his premises, and it seems incorrect to say, without more, that such a proprietor 'makes' any copies when his machines are actually operated by his customers." Thus, Cablevision did not make the playback copies.[64]

Third, the court held that the transmissions were not performances to the public. To determine whether the performances were to the public, the court examined "who precisely is 'capable of receiving' a particular transmission of a performance." The court concluded that the transmissions were not performances to the public because each RS-DVR playback transmission was made to a single subscriber using a single unique copy produced by that subscriber.[65]

It appears that the *Cartoon Network* case may help video-sharing website such as YouTube to avoid direct liability. However, YouTube's uploading process may not fit the holding articulated by the Second Circuit in *Cartoon Network.* First, YouTube stores copies of the video uploaded by the users in its server. Thus, it cannot say that the copies were not "fixed" for more than a transitory period. Second, YouTube broadcasts the video contents to its users (both registered and not registered). In contrast, each RS-DVR playback transmission was made to a single subscriber using a single unique copy produced by that subscriber. Therefore, the transmission may likely constitute a public performance.

However, the YouTube may be able to say it did not make copies. The copies were made at the users' requests because when users upload the videos, YouTube website triggers a series of automated software functions. Similarly, in the *Cartoon Network*,

---

[64] *See id.* at 132.
[65] *See id.* at 139.

when users issue "a command directly to a system, which automatically obeys commands and engages in no volitional conduct." Therefore, one may conclude that YouTube did not engage in volitional conduct.

7. Liability of User

Users play a very important role in using file sharing. Not only because there must be users to use the file sharing systems, but also how the users use the file sharing systems often, if not always, determine whether copyright infringement exists. Also, there are two kinds of users: the downloader and the uploader. Are downloaders and uploaders equal? Do pure downloaders have fair use defense?

The *Napster* case dealt with the issue of whether Napster users entitled to the fair use defense. The opinion covered both the uploaders and the downloaders. Napster identified three specific alleged fair uses: sampling, where the users temporarily copied the music before purchasing; space-shifting, where users listened to the music that they already purchased in CD format; and permissive distribution of music by both independent and established artists. However, the Ninth Circuit first went through the fair use factors: "(1) purpose and character of the use; (2) the nature of the copyrighted work; (3) the 'amount and substantiality of the portion used' in relation to the work as a whole; (4) the effect of the use upon the potential market for the work or the value of the work." The Ninth Circuit then affirmed the district court's rejection of the alleged sampling and space-shifting fair uses, and the plaintiffs did not seek to enjoin the permissive distribution of music by independent and established artists.[66]

[66] *See A&M Records v. Napster, Inc.* 239 F.3d 1004, 1015, 1018 – 1019.

The "purpose and character of the use" requires the determination of whether the allegedly infringing use is commercial or noncommercial. Direct economic benefit is not required to show a commercial use. Commercial use may be found if repeated and exploitative copying of copyrighted works occurs, even if the copies are not offered for sale.[67] Napster's users were engaging in commercial use of the copyrighted works because (1) the uploaders were not engaging in personal use; they were distributing copyrighted work without permission and (2) the downloaders got for free the music that they would ordinarily have to buy.[68]

The "nature of the use" factor focuses on whether the works are creative in nature. If the works are creative in nature, then they are "closer to the core of intended copyright protection" than are more fact-based works. Because the plaintiffs' copyrighted musical compositions and sound recordings are creative in nature, it weighs against a finding of fair use.[69]

The "amount of the portion used" factor focuses on the amount of the portion of the copyrighted works are used. Copying the entire work weighs against a finding of fair use although it does not preclude fair use per se. Because file transfer between Napster users involves transferring the entire copyrighted work, it weighs against a finding of fair use.[70]

The "effect of use on market" factor focuses on whether the copying materially impairs the marketability of the work, which is copied.[71] This factor also weighed against a finding of fair use in *Napster*. The evidence showed that Napster materially

---

[67] *See Id.* at 1015.
[68] *See id.*
[69] *See id.* at 1016.
[70] *See id.*
[71] *See id.*

impaired the market for the copyrighted musical compositions and sound recordings by "reducing CD sales among college students" and "raising barriers to plaintiffs' entry into the market for digital downloading of music.[72]

The Ninth Circuit affirmed the district court's rejection of Napster's fair uses: sampling and space-shifting. Based on the evidence, the court determined that Napster had adverse effects on the sales of audio CD and the developing digital download market. Plaintiffs controlled free promotional downloads on the Internet. They collected royalties on song samples available on retail Internet websites. Free downloads offered by the plaintiffs consisted of thirty-sixty second samples or are full songs programmed to expire in a short time. In contrast, free downloads from Napster were a full, free and permanent copy of the songs. Thus, the purpose and character of sampling was commercial.[73]

In addition to sampling, space-shifting was also rejected by the court. Napster argued that space-shifting is fair use because users accessed the mp3 version of the songs that they already owned in CD format. However, the fatal flaw of this argument was that once the songs were listed on the Napster system, the songs would be available to millions of others, not just the CD owner.[74] Therefore, listing a song on the Napster system was essentially distributing the song to the world without permission of the copyright owners.

With discussion as to the fair use defense in the *Napster* case, we could analyze whether the fair use defense is available to the users of file-hosting service and video-sharing website. Let us address the situation for the uploaders first. When a user uploads a copyrighted work such as a movie without permission onto either a file-hosting service

[72] *See id.* at 1017.
[73] *See id.* at 1018.
[74] *See id.* at 1019.

or a video-sharing website, the user immediately infringes at least the reproduction right and the distribution right of the copyright owner. The uploaded movie would be available to other users of the file-hosting service or the video-sharing website. Thus, the users who upload copyrighted work will unlikely have a fair use defense.

There are users who only download copyrighted work from the file-hosting service or watch copyrighted movies on video-sharing website; they never upload any copyrighted works onto the file-hosting service or the video-sharing website. At first, it appears that they might have a fair use defense because their use of the copyrighted contents is personal use. However, according to *Napster*, the downloaders "get for free something they would ordinarily have to buy." Also, the downloading will most likely adversely affect the sale of the movie in DVD, Blu-ray, and Internet streaming format. Therefore, the pure downloaders will unlikely have a fair use defense.

8. Conclusion

With the foregoing discussion of case law involving the liability of the P2P file sharing software distributor, the host of the file-hosting service, the owner of the video-sharing website, and their users, there are several important features that determine whether one is liable for copyright infringement. If the distributor, host, or owner of the service have knowledge about the infringing activity and failed to police the infringing activities, then they are liable to at least contributory infringement according to the current case law. The users who upload and/or download the copyrighted materials from these services without permission from the copyright owner will likely have no fair use defense and be liable for copyright infringement.

As the Internet technology continues to evolve, the clashes between technology and copyright laws will surely continue. Perhaps, in the near future, the copyright laws might have to be reformed to accurately perform its function to "promote the progress of science…."

Sources

1. *A&M Records, Inc. v. Napster, Inc.,* 239 F.3d 1004 (9th Cir. 2001).

2. Howard P. Goldberg, Note, *A Proposal for an International Licensing Body to Combat File Sharing and Digital Copyright Infringement,* 8 B.U. J. SCI. & TECH. L. 272 (2002).

3. Chunhsien Sung and Po-Hsian Huang, *Copyright Infringement and Users of P2P Networks in Multimedia Applications: The Case of the U.S. Copyright Regime,* Peer-to-Peer Networking and Application, Springer Science + Business Media, LLC 2012.

4. *Cartoon Network v. CSC Holdings, Inc.,* 536 F.3d 121 (2nd Cir. 2008).

5. Hayward, J., *Grokster Unplugged: It's Time to Legalize P2P File Sharing,* Selected Works, 2007, located at http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=john_hayward.

6. *MGM Studio Inc., v. Grokster,* 545 U.S. 913.

7. Dongyu Qiu and R. Srikant. *Modeling and Performance Analysis of BitTorrent-Like Peer-to-Peer Networks,* SIGCOMM'04 Aug. 30-Sept. 3, 2004.

8. Demetris Antoniades, Evangelos P. Markatos, and Constantine Dovrolis. *One-click Hosting Services: a File-sharing Hideout*, In Proc. of ACM IMC '09.

9. Richard Swope, Comment, *Peer-to-Peer File Sharing and Copyright Infringement: Danger Ahead for Individuals Sharing Files on the Internet,* 44 Santa Clara L. Rev. 861 (2004).

10. *Perfect 10, Inc. v. RapidShare A.G.,* Case No. 09-CV-2596 H at p. 2-3.

11. *UMG Recordings, Inc. v. MP3.COM, Inc.*, 92 F.Supp.2d 349 (S.D.N.Y. 2000).

12. Lior Katz, *Viacom v. YouTube: An Erroneous Ruling Based on the Outmoded DMCA*, 31 Loy. L.A. Ent. L. Rev. 101 (2011). Available at: http://digitalcommons.lmu.edu/elr/vol31/iss2/2

13. *Viacom international v. YouTube*, 676 F.3d 19 (2nd Cir. 2012).

14. www.lk.cs.ucla.edu/Personal_history.html