Copyright (c) 2010 Whittier Law Review
Whittier Law Review

Spring, 2010

31 Whittier L. Rev. 421

LENGTH: 31039 words

ARTICLE: TO CACHE OR NOT TO CACHE - THAT IS THE QUESTION; P2P "SYSTEM CACHING" - THE COPYRIGHT DILEMMA

NAME: Assaf Jacob* and **Zoe Argento****

BIO: * Associate Professor, The Radzyner School of Law, The Interdisciplinary Center, Herzliya, Israel. S.J.D. 1998, University of Chicago; LL.M. 1995, University of Chicago; LL.B. 1993, Tel Aviv University.

** Assistant Professor, Roger Williams University Law School. J.D. 2007, Boston College Law School; B.A. 1999, Harvard University. We would like to thank Michael Birnhack, Amnon Lehavi, Elad Oreg, Guy Pessach and Tal Zarsky for their helpful comments. We would also like to thank Oron Afek for his research assistance.

LEXISNEXIS SUMMARY:
... Instead of a central server, these networks utilize "supernodes," high-bandwidth computers connected to the network, where information about other hosts and the files these hosts have available can be accessed by individual peer computers. ... Ambivalent Treatment by the Courts Although Internet users shared infringing files before the emergence of P2P file-sharing services, Napster and the like enabled infringement on a massive and unprecedented scale. ... P2P caching software on ISPa's server determines that the Harry Potter file is a popular file. ... After website owners lost several copyright cases in which the infringing materials were located on and downloaded from a single website, several entrepreneurs realized that, by decentralizing the sharing activity, they could avoid direct liability. ... The difference between P2P caching and expanding the infrastructure, however, is that P2P caching increases infringing file-sharing relative to non-infringing file-sharing. ... However, in the caching scenario, the ISPs may substitute the peers' supply with their servers - so, at least in theory and without any software constraint, it does not really matter how many peers are participating as suppliers. ... Restricting P2P caching to the process in Example Two would create too many identical copies on an ISP's servers and would not provide them with the same benefits in terms of decreasing the data transportation burden, increasing speed, and increasing consumer satisfaction.

TEXT:
[*421]

I. Introduction

Thus far, Internet Service Providers (ISPs) have managed to escape liability for the massive amount of infringement taking place on their networks. As enacted by the courts and legislature, public policy has protected ISPs because of their vital role in providing Internet services on which society increasingly relies. However, ISPs are under enormous pressure to meet consumer demand for bandwidth. Every time ISPs improve their infrastructure to increase bandwidth, consumer use catches up quickly, clogging the lines again. n1 One solution to the [*422] bandwidth problem is peer-to-peer (P2P) caching. n2 The question this article addresses is whether ISPs have stepped over the line by engaging in P2P caching. Are ISPs liable, and should they be liable, for the infringement they facilitate by using P2P caching?

One of the chief objectives in improving Internet services is the management and control of P2P file sharing. n3 By some estimates, P2P traffic takes up half of Internet bandwidth use, n4 and is particularly disruptive because users pass large files on relatively low bandwidth local lines, impeding the flow of all other information. n5

P2P caching capitalizes on the fact that many of its users request the same files. n6 Instead of allowing each user to transfer data from a distant peer, ISPs provide the user with a cached copy of the requested file from the ISP's local server. n7 The basic process is straightforward: after a file is requested by the first user and the data is received, the ISP mirrors, i.e., stores, the data on its server. n8 The next user to access the distant peer then retrieves the stored file from the ISP's server, a local [*423] computer that has a copy of the information and can provide it more quickly. n9 From the consumer's perspective, the whole process is hidden; she does not know whether the file she receives is from the distant peer or from the ISP's server. Because ISPs can reduce the bandwidth of international communication pipelines without compromising the quality of their service, P2P caching provides the consumer with better service while cutting the ISP's operating costs. n10

Caching is hardly a new idea. System caching, which is most commonly used by ISPs to cache websites, has been in use for some time. P2P caching has yet to be specifically addressed, however, by the courts or by the legislature. As this article will discuss, the legal approaches and consensus which have developed around system caching cannot be blindly applied to P2P caching. The interests of the parties involved and the nature of P2P sharing differ significantly from the interests involved in system caching and the nature of the primary platform which system caching serves, the World Wide Web (WWW).

Like system caching, courts are likely to find that P2P caching involves prima facie direct and indirect copyright infringement. After all, when a peer shares a popular infringing file, an ISP engaged in P2P caching not only copies, but distributes that file to other peers. The question is whether fair use, the Digital Millennium Copyright Act (DMCA), or some other exception to the general rule would protect ISPs from liability.

As will be shown, courts have found that under certain conditions, the fair use doctrine protects system caching. Whether fair use applies to P2P caching, however, depends in large part on court views of P2P sharing. Whereas legal opinion has more or less reached a consensus on the WWW, P2P software and P2P services (such as BitTorrent, eMule, Grokster, etc.) are highly controversial and are the subject of fierce legal battles. n11 P2P caching, as a practice which exacerbates the effects of P2P sharing, only deepens the controversy.

[*424] The DMCA provides explicit safe harbors to protect ISPs from liability for caching, at least in the context of website caching. n12 However, courts have held that the protections of the DMCA do not apply to P2P sharing. n13 Even if the DMCA was construed to apply to P2P caching, as will be discussed, the DMCA's balancing of interests between parties does not fit the P2P context.

Up to this point, ISPs often have generally been protected from liability for the infringement taking place on the Internet. n14 Courts have limited liability to users and software distributors, n15 and laws have been drafted to protect ISPs. n16 In P2P caching, however, ISPs stray far from their basic function as conduits of Internet traffic by copying copyrighted files themselves. This is a risky move. ISPs could suffer devastating legal consequences by engaging in P2P caching. Their willingness to do so reflects the immense challenge ISPs face in providing Internet services under the onslaught of P2P traffic. Therefore, in P2P caching, the public policy interest in protecting ISPs clashes directly with the rights of copyright holders.

The stakes are high: "Approximately [ninety percent] of the content on P2P systems is copyrighted movies, software, images, and music disseminated without authorization. It is estimated that more than 2.6 billion allegedly infringing music files are downloaded monthly." n17 At the same time, society increasingly relies on efficient, reliable Internet service. Consequently, to address whether ISPs should be liable for P2P caching practices in light of the fundamental principles of copyright law, we must explore the benefits of system caching in the realm of P2P sharing, as well as its drawbacks. This article will argue that P2P caching amplifies the pros and cons of P2P [*425] services. As a result, our view of this practice takes as its starting point the legal resolution of the P2P controversy.

II. P2P Networks and the Context of Decentralization

An analysis of P2P caching must begin with a description of how P2P sharing works and why it developed. Just as P2P caching is best understood in the context of P2P sharing, P2P sharing is best understood in the context of the interplay between decentralization and centralization which underlies the development of the Internet. n18

To a certain extent, the revolutionary aspect of the Internet is its decentralization of information transfer. At very little effort and cost, anybody can publish information and make it available to millions of people across the globe without resorting to an intermediary. At the same time, anybody can surf the Internet and read information published there. The extent of direct communication and equalization of all players in the exchange of information is unprecedented. While money and resources still make a difference on the Internet, to an extent never before realized, any individual can compete with the haves (e.g., governments and huge corporations) in terms of access to information and the ability to disseminate information.

This decentralization of information transfer has many benefits. Due to lower costs of communication and access, small enterprises can provide new products and satisfy small niches. The result is increased innovation, productivity, and consumer satisfaction, while freedom of speech and association are also enhanced. An individual can say what she wants and communicate freely with little regard for intermediaries, distance, or cost. This freedom and low barrier to entry also permits great diversity. Many different voices have the opportunity to be heard. Decentralization makes freedom of speech relatively impervious to attack because point source failure has only a small impact. That is, there is no particular printing press to shut down. Even if one user is impeded from saying something undesirable, millions of others can continue to do so. This is clearly apparent in the context of copyright infringement where complete enforcement has become virtually impossible.

[*426] Copyright infringement is a good segue to the disadvantages of decentralized information transfer. Decentralization and the corresponding lack of control provide opportunities for exploitation of the commons. n19 Spammers may take advantage of the unrestricted flow of information to overwhelm users with unwanted messages. n20 Hackers similarly take advantage by creating viruses which travel quickly from one computer to another. n21 Decentralization can also be quite inefficient. Without a centralized index for searching, for example, searching is slow and redundant. Communication itself may be slow because a message has to travel between many points to reach its goal.

Conversely, the primary advantages of centralization are efficiency and oversight. For example, a centralized server can offer filtering mechanisms to cut down on undesired messages and viruses. n22 It can achieve economies of scale by ensuring that most traffic is routed along a few high-bandwidth routes. n23 In short, centralization can improve efficiency and lower the costs of searching, storage, traffic, and a myriad other functions. n24 As a result, most uses of the Internet involve some hybrid of centralized and decentralized forms of information transfer. n25

P2P sharing is a relatively decentralized Internet use. The main idea of P2P services is simple: cut out the intermediaries. Each peer computer is transformed into a platform that can share and receive information on its own, via the Internet, without the need of intermediate dedicated servers. n26 This is achieved by using the Internet's backbone to transport the required information. P2P platforms, both software and networks, have become immensely popular in recent years. As of 2005, more than sixty percent of the usage of broadband bandwidth was consumed by P2P-related uses. n27

[*427] P2P sharing is hardly new to the Internet. In fact, the Internet owes its beginnings to P2P architecture. The original Internet, ARPANET, consisted of direct connections between hosts, which used the network for academic sharing of files. n28 Even in the early stages of the Internet's popularization, most files were exchanged via FTP and Telnet, which are P2P applications. n29

As the Internet became popular with the general population after 1994, its architecture became more centralized. n30 Most users wanted to receive information rather than publish information. n31 As a result, most uses of the Internet were based on a client/server model. n32 This was true even of services that appeared to be P2P, such as instant messaging. n33

In this context, the rise of Napster n34 and the resurgence in popularity of P2P architecture was somewhat surprising. It turned out that many people, a sizable percentage of the general public, were interested in publishing on the Internet. n35 Moreover, they were interested in publishing works that they had not even authored. n36 Of course, the emergence of Napster was not driven by the public's desire to publish. Napster was developed primarily to satisfy the demand for infringing digital files. n37

During the early years of the Internet, pirated copies of copyrighted songs were often distributed from one computer or one popular website. n38 However, by Napster's inception, this model of distribution had become risky. Because of their visibility, such popular [*428] websites became an easy target for copyright holders and were exposed to many lawsuits. WAREZ n39 and similar sites were targeted by the Recording Industry Association of America (RIAA) for infringing copyright laws by making unauthorized copies and by distributing those copies over the Internet. n40

The insight behind Napster was that many people would be willing to share their files if connected by a user-friendly interface. n41 Thus, Napster decentralized the sharing of files, allowing users to access files from a huge pool of other users each holding just a few files, rather than a centralized server which contained many files. n42 All these users were willing to make their files available to others because Napster's software made sharing easy and because having Napster's software on their computers made it possible for each user to obtain an almost infinite number of desirable files. n43 On Napster, the old maxim "give and you shall receive" was true.

Although Napster was shut down in 2001, it inspired many imitators. n44 There have already been several generations of P2P applications since then. These successor P2P networks all fall at different points along the spectrum of decentralization. Napster had a relatively centralized P2P architecture. Its designers sought to streamline the search process by maintaining a central index of songs on Napster's server. n45 The central servers kept all the important data [*429] about the peers: which computer contained what song, the Internet connection speed of the computer (which would affect downloading time), and whether the peer was online or offline, to name a few. n46 Thus, searching was centralized, while distribution of the protected files was decentralized.

Grokster n47 and BitTorrent n48 represent an intermediate step, a type of hybrid architecture. Instead of a central server, these networks utilize "supernodes," high-bandwidth computers connected to the network, where information about other hosts and the files these hosts have available can be accessed by individual peer computers. n49 The third generation P2P client is fully distributed in the sense that any computer on the network can act as an indexing server and there are no supernodes. n50

Thus, the different forms of P2P sharing all occupy points along the spectrum of decentralization and centralization of Internet uses. As relatively decentralized uses, however, it is not surprising that the development of P2P networks has gone hand-in-hand with the evolution of Internet-related copyright piracy. More freedom and less control on the Internet almost immediately translate into more opportunities to obtain copyrighted materials for free. The next chapter discusses how courts have confronted the challenge of determining liability for infringement in the context of P2P sharing, a technology that facilitates massive infringement while at the same time exercising very little control over its users.

III. Ambivalent Treatment by the Courts

Although Internet users shared infringing files before the emergence of P2P file-sharing services, Napster and the like enabled infringement on a massive and unprecedented scale. Before Napster, infringing songs were centrally distributed from one computer or one [*430] popular website. n51 However, by Napster's inception, this model of distribution had become quite risky. Because of high visibility, popular websites had become an easy target for copyright holders and were thus exposed to many lawsuits. Napster overcame this problem by providing software to allow users to easily share files directly with one another. n52 By doing so, Napster made enforcement of copyrights exponentially more difficult. Copyright holders could no longer enforce their rights by targeting one website which distributed the files. Instead, millions of users shared files directly with each other.

It did not take copyright owners long to learn that to fight the massive copyright infringement enabled by P2P sharing services like Napster, they had to target not only the end-users but also the P2P sharing service itself. The courts addressed P2P sharing in three major decisions: A&M Records v. Napster, n53 Aimster Copyright Litigation, n54 and Metro-Goldwyn-Mayer Studios v. Grokster. n55 In all three cases, the courts found that the P2P services could be liable for secondary copyright infringement. n56

Nevertheless, a review of these opinions shows a certain ambivalence on the part of the courts. On the one hand, the court in Grokster condemned the massive infringement facilitated by P2P services. n57 On the other hand, the Supreme Court appreciated the potential of these services. n58 Indeed, the Court introduced its discussion of Grokster by describing the benefits of P2P networks, n59 and lauded the improvements in cost, speed, and stability. n60

[*431] Even though the courts found the P2P networks liable in all three cases, the courts repeatedly expressed their concern with properly balancing protection for technological innovation and potential against a copyright owner's rights. n61 The cases all drew heavily from Sony v. Universal City Studios, the Supreme Court's landmark decision on secondary liability for copyright infringement. n62

In Sony, copyright holders sued Sony for facilitating infringement by selling what was, at the time, a new product, the video tape recorder (VTR). n63 Consumers used the VTR to copy television programs, thereby infringing copyrights held by the plaintiffs. n64 The plaintiffs argued that Sony should be liable for infringement just for selling a product which was used for infringement. n65 Seeking to balance the rights of the copyright holders to enforce their monopoly against "the rights of others to freely engage in substantially unrelated areas of commerce," the Supreme Court held that Sony would be secondarily liable only if the VTR was not capable of "commercially significant noninfringing uses." n66 The Court found that the VTR did have a "commercially significant noninfringing use," namely "time-shifting," the practice of taping television shows to watch them later. n67 As a result, the Court held that Sony was not liable for infringement. n68

Like the VTR, P2P services are a product that consumers use to infringe copyrights. Because P2P service providers themselves do not directly infringe, the question was whether they were liable for facilitating infringement. However, unlike Sony, none of the courts decided its case on a straightforward analysis of whether P2P services had "commercially significant noninfringing uses." n69

[*432] Rather, the courts focused heavily on the intentions and actions of the defendants and less on the nature of P2P sharing itself. Grokster was decided primarily on the evidence that Grokster's owners had promoted infringement through advertisement directed at infringers and the failure to develop any sort of filter to diminish infringing activity. n70 The Seventh Circuit in Aimster emphasized the promotion of infringement, too: the fact that Aimster's tutorial on how to use its service only gave examples of infringing use and that Aimster charged for delivery of the top forty infringing songs. n71 In Napster, the court concentrated on Napster's owners' missed opportunities to prevent

infringement. n72

Even when the courts discussed the design of P2P networks, as opposed to their owners' intentions, they did not go so far as to find that P2P networks made their owners liable for infringement simply by the nature of P2P design. In Aimster, for example, the court conducted an examination of the non-infringing uses, n73 and decided that there were no substantial non-infringing uses, but only that Aimster had failed to provide evidence of non-infringing use. n74 Both the Grokster and Napster courts did not even reach the issue of non-infringing uses. n75

Rather, the Aimster court emphasized the prescience of the Sony court in "striking the cost-benefit tradeoff in favor of Sony" because [*433] home VTRs opened an "enormous new market" for the movie industry. n76 In their approach, at least, the courts were open to recognizing the benefits of P2P networks.

Thus, no court has yet analyzed a P2P network purely on a comparison of infringing uses and non-infringing uses a la Sony. Given these cases, it seems possible that a P2P network which did not actively promote infringing uses, n77 took action when notified to stop infringement to the extent it could, n78 and had evidence of actual non-infringing use, n79 could escape liability altogether.

This brings us to the next chapter in which the benefits and drawbacks of the P2P platform will be discussed.

IV. P2P Networks - Cost Benefit Analysis

The P2P architecture has many advantages. First and foremost, the P2P architecture enables a great deal of freedom. Peers exchange files directly, free of central management or control. n80 The P2P services use common protocols that support a cross platform exchange of files. n81 The search mechanism is also decentralized. n82 All of these characteristics prevent "big brother" from shutting down the main server and eliminating or controlling the file search and exchange.

P2P architecture also enables the diffusion of political power and greater personal freedom for peers. n83 This, in turn, enhances diversity - if more peers have a better platform to share their work at a lower price, more voices can be heard on the Internet. n84 P2P platforms also provide an alternative noncommercial decision-making [*434] mechanism to sort available content. n85 As one commentator stated: "Choices regarding the music files or videos shared are made in a non-commercial setting, thus communicating information regarding users' preferences relatively free of market effects." n86

Advocates of P2P sharing point to the economic efficiencies of the P2P practice. They emphasize the fact that because no central computer server is needed to mediate the exchange of files, "the high-bandwidth communications capacity for a server may be dispensed with, and the need for costly server storage space is eliminated." n87 To take even greater advantage of the decentralized characteristics of the network, the new P2P programs do not treat large files as one. They break a big file into hundreds or thousands of smaller files with unique IDs. n88 When the user wants to download a big file, a parallel download occurs. n89 The user's computer downloads different parts from different peers simultaneously and in no specific order. n90 The downloading process therefore takes less time and consumes less computer resources from other peers. n91 When all parts are downloaded to the requesting computer, a process that can take several hours to several weeks, the software rejoins the parts based on their unique ID and recreates the big file. n92 In order to "enforce" sharing, the program is set to a mode that makes small files on a user's computer available for sharing (whether she likes it or not), whenever that user is downloading a big file. n93

Many P2P programs use one protocol. n94 Thus, sharing is not restricted to those who use the same piece of software. n95 Users can communicate across platforms and different networks and also can [*435] search and share files among many more users. n96 This practice extends the possibilities of exchanging information around the globe.

In addition, capacity is not "fixed" as it is when serviced by a centralized server, but grows as the network grows. In the P2P architecture, users not only consume services, but also provide the resources of computer storage, computing power, and bandwidth. n97 Whereas in the old architecture, adding clients could slow down data transfer for all users and in extreme cases lead to denial of service, in the new architecture, the total capacity of the system increases as demand on the system increases. n98

Decentralization also makes the system more stable and reliable. Single-point failure is reduced because if one computer fails, the rest can still communicate without interference. n99 Another benefit is that P2P sharing eliminates the need for costly server space, instead relying on the storage capacity of each peers' computers. n100

However, P2P platforms also have disadvantages. Critics point out that the decentralized search techniques make them less efficient in terms of information retrieval. n101 Searches "may not reach and uncover all available files because search requests may not be transmitted to every computer on the network." n102 Another disadvantage is that there may be redundant copies of popular files: instead of one copy residing on the main server, many copies will be spread around the Internet. n103 As the Supreme Court noted in Grokster, "the creator of the software has no incentive to minimize storage or bandwidth consumption, the costs of which are borne by every user of the network." n104

[*436] This leads to another related point. In many countries technology constraints make high speed Internet asymmetric. While downloading can take place at a high speed (1.5 Mbps and higher depending on one's Internet connection speed), uploading is usually restricted to a lower bandwidth (200 Kbps or higher depending on Internet connection speed). n105 Within non-P2P uses of the Internet upload speed is not a major problem, because, home users typically care only about how fast they can download web pages, files, etc. n106 In other words, the users care more about receiving than sending information. But in P2P services, this asymmetry is an obstacle. In the P2P world, users not only download information, but they also provide information to others. The high demand for files and the limited upload capabilities cause demand to be far greater than supply, n107 which in turn creates long queues for the receiving parties. Peers who share files are flooded with downloading requests, but their sharing capacity is limited by their upload capabilities. n108 Because of the long queues, sometimes several thousands of requests for a given file on any one peer's computer, n109 the downloading process is delayed. n110 Therefore, files [*437] that could have been downloaded in a matter of hours instead take days to download.

Finally, what may be an advantage to some is a disadvantage to others. The flip side of decentralization and freedom is lack of control. Thus, one of the major disadvantages, as noted by the Supreme Court in Grokster and observed by others, is that, in P2P networks, "it is more difficult to control the content of files available for retrieval and the behavior of users." n111 In other words, users use P2P networks to share infringing files on a massive scale.

V. Internet Service Providers and P2P - Caching P2P Files

For ISPs, the flourishing of P2P services was a mixed blessing. On the one hand, this practice substantially increased the demand for high speed Internet. n112 Users learned they could download many goods via P2P services which they would otherwise purchase in "hard copy," such as music, films, and books. n113 Sometimes P2P service could also provide goods that could not be purchased outside of the Internet - movies not yet released on DVD, TV episodes not yet broadcasted, or books still unpublished. n114 All these items, however, translate into many gigabytes of data. n115 In order to obtain them, users could not use a dial-up modem because it would take months to download a movie. Switching to high speed Internet allowed users to receive more information in less time.

But what seemed at first to be a blessing turned out to be a curse. Users of P2P services not only paid for more bandwidth, but actually [*438] used it. ISPs soon realized that many users stayed online for weeks, continuously downloading and uploading files. n116 This phenomenon was aggravated by the flat fee pricing policy. n117 Once the user paid for a whole month of usage the price stayed the same whether he stayed online for an hour or for four weeks. n118 Since the downloading process takes a long time, during which the user also participates in uploading, ISPs pipelines are jammed. n119 As a result, ISPs had to pay for costly improvements in their infrastructure - primarily by buying more bandwidth on the main lines that connect the ISP to the Internet. n120

Upgrades to the infrastructure, however, improved the situation only briefly because with higher bandwidth came better downloading results, which in turn increased the demand for higher bandwidth even further. n121 Consumers started to complain. They were unhappy with paying high prices for Internet services, while receiving slow service. n122 This put ISPs in a catch-22. On the one hand, they wanted customers with high speed Internet connections, because those customers provided more income. n123 On the other hand, they wanted to avoid further expansion of their infrastructure, because this would require a huge investment of resources. n124 This led ISPs to use an "old" technology in a "new" context. This technology was P2P caching.

A. ISPs Acting as a Conduit

In the conventional world of P2P services, the ISP merely serves as a conduit of information. Consider the following example. A1 has [*439] installed P2P software and now wants to download the new Harry Potter movie. He types the name "Harry Potter" and the software sends a search request to the Internet. Assume B1 also has the P2P software. B1's P2P software will respond to A1 with important information about the requested file: the file's size, computer B1's ISP address, and other such relevant material. n125 Then, when A1's request is delivered to B1, A1 joins the queue on B1 and, in due course, downloads the file to his computer from B1. n126 At the end of the process, both A1 and B1 have copies of the new Harry Potter film.

One should bear in mind that in order to get physical access to B1, A1 has to send and receive information through his ISP (i.e. ISPa) and through B1's ISP (i.e. ISPb). As mentioned above, both ISPs play only a passive role in this game as conduits of information. Another important aspect of this transaction is the effect of the quality of the infrastructure, or backbone, on the file's download speeds. In our example, the download time will be limited by the lower of A1's maximum download speed and B1's maximum upload speed. n127 In a typical case, download speed is far greater than any given upload speed. Therefore, A1 will often be limited by B1's upload speed. Additionally, if many computers are participating in the exchange of P2P files, the bottleneck of data transportation is between ISPa and ISPb. n128 This pipeline accumulates all network transportation, and therefore, carries the heaviest traffic. This is also the most expensive pipeline to upgrade since it is the gateway of both ISPa and ISPb to the [*440] Internet. In order to obtain greater bandwidth, both ISPs usually have to buy it from an outside source. n129 If the main pipeline is not expanded, it can slow traffic when interacting with the Internet - but not within each network. n130 Thus, if the main pipeline is clogged, A1 will not have high speed Internet access to B1 for file-sharing, but will still be able to quickly send A2 an e-mail message.

In terms of copyright law, both A1 and B1 may be considered copyright infringers: A1, for making an illegal copy of a protected work and B1, for distributing a copy of a protected work without the owner's permission.

[SEE ILLUSTRATION IN ORIGINAL]

B. Caching P2P Files

As discussed above, one way to alleviate network congestion is to increase Internet bandwidth. This solution, however, tends to be very expensive and caching is a cheaper solution to network congestion. As we will further elaborate, the caching technique can be used in several settings, even within the P2P environment, but the main principle of the caching system is simply this: ISPs create exact copies of popular files and provide their clients with these copies as a substitute for the [*441] actual requested files. n131 Because all copies are digitally made, they are identical to the client's requested file and therefore create a perfect substitute for the original. n132 As a result, the client usually doesn't realize he is retrieving copies from a different source. n133 What the client does observe is that he is downloading the file at a much greater speed. This is the precise reason ISPs provide this service - it allows them to provide consumers a better service without paying the high costs of expanding the network's actual bandwidth.

The caching practice operates in several different ways. These variations affect the ISPs' interests and the overall cost-benefit analysis, which in turn might affect the legal analysis. Therefore, we will provide some illustrations to elaborate on some of these caching practices. n134

[*442] The first case will be illustrated through Example Two. n135 A1 has downloaded, using P2P software, the Harry Potter movie from B1's computer. P2P caching software on ISPa's server determines that the Harry Potter file is a popular file. Expecting high future demand, ISPa used A1's first download request to make a copy of the Harry Potter file on ISPa's main server.

Here the ISP is playing an active role. This process may occur without human intervention, but it is still based on criteria dictated by the designer of the software. Not all files are kept on the ISPa's server and it is a matter of the ISP operator's policy to decide when to make a copy and how aggressive this process of file copying will be. Thus, after A1 first downloads the Harry Potter movie, there are not only two copies of the file, but three. The third copy is not located on A1 or B1's computer, but on the ISP's server.

Now, A2 wants to download the Harry Potter movie as well. He sends a search request for the file and discovers that a copy of it is located on B1. He then asks B1 for the file. At this point, ISPa becomes further involved in the process. ISPa's software realizes that the copy of the requested file is located on its server and instead of letting B1 deliver the copy, it delivers the copy from its own server.

ISPa enjoys a number of benefits as a result. First, the customer is satisfied. A2 receives the requested file faster because the transmission distance between ISPa and A2 is shorter than that between B1 and A2 and the bandwidth between ISPa and A2 may be greater.

Secondly, ISPa enjoys a substantial reduction in its costs. By providing the file directly from its server, no transportation of data is taking place on the main pipeline between ISPa and ISPb. Because the pipeline that connects ISPa and ISPb is the busiest and most expensive pipeline, downsizing the activity on this line cuts ISPa's costs dramatically and allows faster transportation speed for other services provided to users. n136

[*443] [SEE ILLUSTRATION IN ORIGINAL]

Now consider Example Three. In this example, A3 would also like to download the Harry Potter file. After sending a search request, A3 discovers that A1 and B1 have the required file. It sends a request to A1 to download it. ISPa discovers that A3 requested the file from A1, intercepts this transmission, and sends the file directly to A3 from the main server. Here, it is important to emphasize that ISPa is providing a cached file that was downloaded from B1's computer on a request made to a different computer (i.e. A1) for the "same" file. This is different than Example Two in which the caching practice was substituting future download requests from the same source.

Why does ISPa "interfere" with this activity? What are its interests in doing so? Unlike the second example, this time, providing the file will not cut ISPa's costs with regard to the main pipeline. As illustrated by the diagram, both A1 and A3 share the same ISP. The answer is that by providing the file directly from its server, ISPa still benefits. Recall that the uploading speed is often much slower than the downloading speed. By sending the file from the main server, A3 gets the file more quickly and ISPa saves A1's uploading capabilities. This benefits both clients (A1 and A3) and also reduces the demand for expanding uploading capabilities. Since these network connections are often asymmetric, extending their actual capabilities is very expensive and sometimes impossible. By using the caching mechanism, ISPs alleviate the pressure on their uploading capabilities. Moreover, even if these could be expanded - less transportation within the system [*444] means less clogged pipelines and more speed at a lower cost for all users.

[SEE ILLUSTRATION IN ORIGINAL]

Example Four deals with yet a different situation. This time C1 requests the Harry Potter movie. No one in C1's network has ever downloaded the Harry Potter file, so ISPc does not have a copy of it on its main server. C1 uses his P2P software to send a search request over the Internet to B1, who has a copy of the file on her computer. ISPb, which made a copy of the popular file and saved it on its main server, intercepts the request and delivers the Harry Potter file directly to C1 from its main server. What are the benefits to ISPb for doing so? ISPb does not save on the main pipeline's data transportation because it delivers the file outside its local network. In addition, unlike the previous example, ISPb does not benefit from helping C1. n137 By delivering the Harry Potter file itself, however, ISPb conserves its client's (B1) uploading availability, which makes uploading from B1 faster for other users in ISPb's network. In addition, delivering the file from its main server eliminated the need to send the information between B1 and ISPb, thus conserving bandwidth. Considering millions of requests are being delivered everyday, this caching practice reduces ISPb's costs dramatically.

[*445] [SEE ILLUSTRATION IN ORIGINAL]

The fifth and sixth examples can be characterized as important nuances of the third example. In Example Five, A1 first downloads the Harry Potter file from B1. When A1 downloads the file, ISPa makes a copy of the file on its main server. After the first download, B1 deletes the file from his computer. So now, copies of the file reside only on A1 and ISPa's server. At this point, A3 wants to retrieve a copy of the file. Using its P2P software, A3 searches the Internet and finds that the only computer that has this file is A1. A3 sends a download request to A1 but ISPa interferes with this download and provides A3 the cached copy of the file located on its server.

The important nuance in this example is that the original file no longer exists on B1. This deletion could happen for many reasons. B1 could have been the owner of the file and decided to stop sharing it. B1 might have been approached by the RIAA or received a court order and decided to delete the infringing file. B1 also could have deleted the file on his own initiative: to reduce the chances of being sued for copyright infringement, for example, or to free up more space on his hard drive (perhaps in order to download more movies).

Caching the file in this example makes the file much more available. It no longer matters where the file was downloaded from originally, or how popular it is. As long as one peer has it, other peers can get it from ISPa's cache memory through high speed connections. Contrast this to a world without P2P caching, where the popularity of a [*446] file greatly affects its downloading speed, its availability, and the time one has to queue to get it. Here, the ISP fulfills the demand and provides an alternative source of the file.

[SEE ILLUSTRATION IN ORIGINAL]

The scenario just described becomes even more acute in Example Six. In this example, after the first download, the file is deleted from both A1 and B1, so no peer has a copy of the Harry Potter file. At a later point A3 searches for the file. When A3 conducts this search, ISPa realizes that neither A1 nor B1 has the file, or because of the design of the P2P caching software, fails to check or verify whether they have a copy of it. Instead, ISPa automatically sends the file to A3, based on his request. n138

[*447] [SEE ILLUSTRATION IN ORIGINAL]

The end result of all this is a form of centralization: all of the popular files are saved on the main server. The P2P service thus essentially operates in two parallel modes. Popular files are distributed in a centralized fashion, and other uses, including P2P sharing of unpopular files, function in a decentralized manner.

VI. Caching P2P Files - Legal Analysis

As discussed above, caching P2P services is a very appealing practice for ISP providers. However, this practice is almost certainly prima facie infringement. The more difficult question is whether the fair use doctrine or the DMCA protects ISPs from liability.

A. ISP's Direct Copyright Liability

The first question is whether ISPs are directly liable for copyright infringement. The Napster court reaffirmed the time-honored requirements for direct copyright infringement in the P2P context. n139 The court held that in order to substantiate a direct infringement suit, a plaintiff must satisfy two requirements: that she has ownership in the copyrighted work and that at least one of her exclusive rights under United States Code (USC) Title 17, section 106, was infringed by the [*448] defendant. n140 In response, the ISP may still, however, assert an affirmative defense using the fair use doctrine. n141 For purposes of this discussion, we will assume that the plaintiff is indeed the rights holder, and therefore, we will concentrate on the issues of infringement and fair use.

1. Establishing Copyright Infringement

Section 106 gives a copyright owner the exclusive right to reproduce a protected work, and/or to distribute copies of it to the public. n142 It is enough that an ISP infringes one of these exclusive rights to be considered a direct infringer - the plaintiff does not have to prove that both rights were violated. n143

a. Infringement of the Right to Copy

Reviewing the history of P2P services, one of the main reasons for developing P2P platforms in the first place was to avoid making an infringing copy on the central server. n144 After website owners lost several copyright cases in which the infringing materials were located on and downloaded from a single website, several entrepreneurs realized that, by decentralizing the sharing activity, they could avoid direct liability. Thus, the providers of the P2P services made sure that a copy was only made on a peers' computer. And indeed it worked - in all of the P2P decisions mentioned above, the providers did escape liability for direct copyright infringement. n145 The case of P2P caching presents a different story. In P2P caching, an actual copy is made on the ISP's servers. n146 P2P caching essentially reverses the P2P process: ISPs once again centralize the files to allow faster downloads. n147 This raises the question of whether the copy made on an ISP's server in the [*449] process of caching is actually a "copy" for the purposes of copyright law.

In order to qualify as a copy under copyright law, the copy must be " "fixed' in a tangible medium of expression." n148 The ISPs might argue that the work is not fixed, because caching is only a temporary practice, after which the file is deleted. This argument, however, was already made and rejected in MAI Systems Corp. v. Peak Computer, Inc. n149 The Ninth Circuit held that even a temporary copy made in a computer's random access memory (RAM) was fixed in a medium and therefore a "copy" for the purposes of copyright law. n150

Distinguishing P2P caching from MAI would be difficult. A copy made on RAM is more temporary than a copy which is saved on the hard disk for caching purposes. n151 Moreover, the RAM electronic copy is less fixed because, unlike a copy which is saved on a hard drive, the RAM copy is lost once disconnected from electricity. n152 As section 101 of the Copyright Act states, a copy is "fixed" if it is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." n153 The P2P caching practice clearly comports [*450] with this requirement and with MAI. The whole purpose of a copy is to substitute the original files to allow greater download speed at a lower cost.

Perhaps a more productive argument for ISPs is that the cached copies are made without volition. The copies are made in an automated manner, based on their popularity (which is dictated by the peers). The roots of this argument go back to Religious Technology Center v. Netcom On-Line Communication Services, Inc. n154 In Netcom, the court ruled that automated copying by machines initiated by others was not sufficient for establishing direct infringement. n155

Recent cases on Google's search engine caching practices have dealt with the volition requirement and are therefore useful interpretive tools. In the process of mapping the net, Google's robots crawl and make copies of many websites. n156 Google then keeps a copy of the original web pages on its servers for archival purposes. n157 In Parker v. Google, Inc., one of the site owners, whose webpage was copied, filed suit for copyright infringement. n158 The court ruled against him based in part on Netcom. n159 The Parker court broadly interpreted the Netcom decision to cover Google's practices, stating:

> When an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition is missing. The automatic activity of Google's search engine is analogous. n160

The appellate court approved this ruling, noting: " "An ISP who owns an electronic facility that responds automatically to users' input is not a direct infringer.' " n161

[*451] However, there have been criticisms, for good reason, of the broad reading of Netcom in Parker. n162 One critic has noted that copying files for both temporary and archival purposes is contradictory. n163 Moreover this broad reading of the "automated process" exemption does not make sense if taken to its logical conclusion: that a software program designed to copy every file on the net would not be infringing because it is "non-volitional." Although the functioning of a software program itself is not "volitional," the decisions of the software programmer, when designing that software, clearly are. Software is just a tool, after all.

Indeed, the Ninth Circuit in Perfect 10 reached a different conclusion with regard to Google's volition, taking a much narrower view of Netcom. n164 This time, the issue was Google's display and distribution of cached "thumbnails," the miniaturized version of photographs that Google collected from the Internet. n165 Ruling in favor of Perfect 10 in this matter, the court noted that there was "no dispute that Google's computers stored thumbnail versions of Perfect 10's copyrighted images and [distributed] copies of those thumbnails to [its] users." n166 The important aspect of this part of the decision, however, lies in footnote 6, where the court commented on the Costar decision:

[*452]

> Because Google initiates and controls the storage and communication of these thumbnail images, we do not address whether an entity that merely passively owns and manages an Internet bulletin board or similar system violates a copyright owner's display and distribution rights when the users of the bulletin board or similar system post infringing works. n167

In other words, the court did not even address volition as an issue in Google's caching practice.

What lesson should we learn from these cases with regard to the P2P practices? A broad reading of the Netcom decision, as was adopted in Parker, might treat the caching practices as one without volition. Caching is an automated process which is triggered by the popularity of the files (based on the clients' initiative), without any human intervention to allow for faster delivery of the files to others.

In our opinion, however, this would be an overly broad reading of the Netcom decision. The ISP controls the caching practice, and sets the defaults for the copying activity. Knowing that most of the P2P activity is infringing, especially with regard to the popular files which are cached, and given the courts' rulings in the P2P trilogy, it would be hard for the caching ISPs to argue that their act of caching is without volition. In Netcom, users wanted to post on a bulletin board, which required the services of the ISP to copy and make available their posting. n168 In contrast, P2P sharing does not require caching to function. n169 Moreover, P2P caching is not a service provided automatically at the request of users. Most of the users do not even know about the practice - to them the whole process is hidden. Thus, since ISPs take the initiative to cache popular files, it is hard to argue that they are only playing a passive role.

[*453] The appropriate test might be one of control - in essence, who initiates and controls the caching process? In P2P caching, users do not have any control with regard to the actual caching. They do initiate the sharing of the files, but this process can work without the ISP's intervention. The ISP is the only one to control which files are copied and

on what terms. Therefore the decision about whether to make these copies is the ISP's, even if the ISP's policy is executed by an automated process.

b. Infringement of the Right to Distribute

Proving "distribution of a copyrighted work requires an "actual dissemination' of copies." n170 ISPs might try arguing that it is actually the peers who request the files. The ISP's P2P caching server simply accedes passively to a peer's request to upload a file. We think, however, that this argument stretches the truth too far. Distribution in the P2P context is effectuated by making files available to users in much the same way that a shop owner distributes infringing products by stocking them in her store. n171 Indeed, this is the "deemed distribution" approach that the Ninth Circuit took in Napster. n172 Peers in Napster who simply made works available for upload by other peers were found to infringe the copyright owners' right to distribute. n173 As with the right to copy, courts are likely to conclude that P2P caching is a prima facie case of violation of the exclusive right to distribute.

2. Fair Use Analysis

The ISP's can still prevail in a direct copyright infringement suit by showing their practice is protected by the fair use doctrine. This doctrine is especially important in new technology cases where courts [*454] have to carefully balance the promotion of innovation against protection for copyright owners. n174

a. Purpose and Character of Use

Section 107 of the copyright act enumerates four non-exclusive factors to be considered in every fair use analysis. n175 The first factor deals with the "purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes." n176 Under this factor, courts generally assess two main concerns - whether the use, as opposed to the defendant's characteristics (i.e. commercial vs. private entity), is commercial and the extent to which the use is transformative. n177 A use is considered transformative if it does not merely substitute the original work but adds something new to it "with a further purpose or different character, altering the first with new expression, meaning, or message." n178 The more transformative the use, the more likely the use will be considered fair.

The Ninth Circuit clearly articulated the current test to determine whether a use is transformative: "A use is considered transformative only where a defendant changes a plaintiff's copyrighted work or uses the plaintiff's copyrighted work in a different context such that the plaintiff's work is transformed into a new creation." n179 This test presents a problem for ISPs because cached works in P2P caching are exact copies of the originals. n180 In fact, they have to be exact copies for the purposes of P2P caching in order for the process to work properly.

Nevertheless, courts have found that even making an exact copy is transformative in some web caching cases. In Kelly v. Arriba Soft [*455] Corp., the court ruled that the caching of reduced size images was a transformative use. n181 The Ninth Circuit found that the images, although originally created to serve as an "artistic expression," were transformed into a new use as pointers, "improving access to information on the Internet." n182

The Kelly ruling was recently endorsed in Perfect 10, where the court decided that Google's use of Perfect 10's images as thumbnails was highly transformative due to use in a search engine, promotion of the purposes of copyright, and by serving the public interest. n183 This decision is important to the P2P context for more than merely upholding Kelly. Other web cases have dealt with infringement suits brought by website owners against search engines for copying their copyrighted images from their personal sites. In Perfect 10, however, the suit was filed by a third party, not a website owner, whose images were located on someone else's website. n184 This distinction is important because the court was driven by a different motivation. In many of the "regular" web caching cases where individual website owners sue, courts utilize the argument that, by placing materials on the web or not following common web protocols, the owner is willing to share those materials with the public. n185 Thus, the main concern is not only about public access to the materials, which is granted for free, but also about copying by the search engine. Courts made the determination that, by allowing search engines to cache these files, the owner loses little and the public benefits by having better access to their respective sites via the search engine, or the cached copy (when the site is not accessible). n186

[*456] Moreover, in most of these cases, the search engine generally complied with the terms introduced by the site owner. n187 Since the website owner can use robot exclusion clauses (in the site's meta-tag field) to keep search engine robots away from his site, not doing so puts him in an inferior position with respect to copyright infringement. n188 The site owner becomes "blameworthy" because he is the cheapest cost avoider. By simply adding an exclusion clause, he can prevent infringement. Reading the cases, one cannot escape the feeling that the court often wants to "punish" the website owner because he did not act in good faith. n189

This caching scenario is less common in the P2P context. It is true that any peer, assuming he is the copyright owner, can bring a claim against the ISP for making a copy of a file he distributed through the platform. But that just does not happen. Peers who place their materials on the Internet know that those materials will be available to everyone and in fact want the files to be circulated. Therefore, the caching practice can only promote the peers' goal. n190 The more common phenomenon occurs when a third party, like the record label companies, complains about copyright infringement. In this respect, Perfect 10 provides a closer example to the P2P services because it balances the public right of access against the rights of third parties. n191 Ruling in Google's favor meant that the court preferred the operation of the visual search engine, at the expense of "innocent" third parties. This provides fertile ground for similar arguments on behalf of the P2P industry.

[*457] Even if a court is receptive to the idea that an ISP can cache a file belonging to a third party, the ISP must still show that this caching is transformative. As in Kelly and Perfect 10, ISPs will have to show that caching creates copies which serve a different function. n192 Moreover, this function must have some socially desirable use. n193

An analysis of whether P2P caching benefits the public must begin with the activity it facilitates - P2P file sharing. As discussed in Part IV, P2P architecture has substantial benefits. To name some of the chief advantages, the decentralized structure provides great personal freedom to peers, which is highly resistant to control or suppression. This also promotes diversity. From a more economic point of view, P2P sharing eliminates the need for servers to provide costly storage space because much is saved on peers' computers instead. P2P architecture is also highly stable and reliable. n194

All of these benefits, however, do not come without a cost, and the cost, as mentioned above, is high - extensive copyright infringement. The more freedom and less control, the more the use of infringing materials. If one can get goods on the Internet for free, without being caught, the less likely one will buy them in stores. We should bear in mind that despite the great benefits of P2P services, all courts have been rather hostile to them due to the high piracy rate. In all three major cases discussed in this article, the courts ruled against the software manufacturers. n195

The next question is how the extra layer of P2P caching changes the analysis of the costs and benefits of P2P file sharing. In particular, is P2P caching transformative enough to comply with the first fair use factor? The benefits of P2P caching are clear. Caching reduces costs while minimizing data transportation among the peers because the ISP saves on bandwidth by storing information on servers. It reduces the need to exchange information among peers by providing the files locally. This allows ISPs to better serve their customers without [*458] paying for more international Internet connections. Another important benefit is that the caching solution provides files at greater speed. Sending the files from a faster computer, with more computing resources, faster routers and greater Internet bandwidth, through a shorter distance, better fulfills demand at a higher speed.

At first glance these advantages look very attractive. Providing better services on the same infrastructure by reducing unnecessary file exchange seems like a social goal the courts should promote. These benefits are passed on to the public, which ends up as better service at a lower cost.

However, this is not necessarily so. A second glance might reveal a different picture. As we have seen, the primary advantages of P2P sharing (freedom, reliability, reduced server storage expenses, and diversity) are due to its decentralized character. However, via caching, ISPs actually re-centralize power, control, and storage space. n196 Thus, P2P caching in reality undermines many of the justifications for the P2P platform.

This is a classic trade-off in the interplay between centralization and decentralization in uses of the Internet. As discussed in Part II, a decentralized architecture, though beneficial, may be quite cumbersome and inefficient to operate. The question becomes how much the benefits of decentralization are worth in terms of the trade-offs to heavy bandwidth traffic, efficiency, and cost. This, of course, is a fairly abstract question and difficult to answer.

A more practical question is how P2P caching compares to alternative solutions to the bandwidth-clogging caused by P2P sharing. The most obvious solution is simply to pay to expand network infrastructure. How does P2P caching compare to paying to improve the infrastructure? Both increase the available bandwidth and thus provide a better service for customers. However, as discussed, P2P caching is cheaper than paying to expand the infrastructure; otherwise, ISPs would not use P2P caching in the first place. Expense in building infrastructure, however, is just one cost that should be weighed in the [*459] comparison. Another cost is the cost of infringement born by copyright owners.

The fact is that both P2P caching and expanding the infrastructure increase infringement. Naturally, if there is more bandwidth available, then more P2P files can be transferred. Consumers tend to quickly take advantage of increases in available bandwidth. Since some percentage of those shared files will be infringing files, as the number of files transferred increases, the absolute number of infringing files transferred will increase as well.

The difference between P2P caching and expanding the infrastructure, however, is that P2P caching increases infringing file-sharing relative to non-infringing file-sharing. In contrast, improving the infrastructure appears to simply increase all file-sharing proportionately. That is, if bandwidth increases for all uses when the infrastructure is improved, then all uses should increase - both infringing and non-infringing. It seems, however, that P2P caching disproportionately increases infringement in at least two ways.

First, an ISP's P2P caching increases the speed of sharing infringing files more than it increases the speed of sharing non-infringing files because faster access to infringing files naturally increases infringing activity. It makes a significant difference to a user if it takes ten minutes to download the new Harry Potter movie via P2P instead of ten hours. The longer a user has to wait to get the file illegally, the more likely she is to pay to get the file from a legitimate source if it means a faster download. P2P caching on a network increases the speed with which infringing files are shared as opposed to non-infringing files by several means.

One of the ways in which P2P caching increases the speed of sharing infringing files is by caching popular files. n197 "Popular" files, files that P2P caching software chooses to cache because they have been requested many times, are likely to be infringing rather than non-infringing. After all, typically studios, authors, musicians, and other creators, are motivated to invest time and money in their creative works [*460] precisely because they hope those works will be popular. They also often pay heavily to market those works to increase demand. They then protect their copyrights because they want to profit from their works' popularity (or at least to recoup their investment). So, by the nature of the intellectual property rights system, most "popular" works are probably not only copyrighted but owned by protective copyright owners. As a result, the most popular files shared by peers, and therefore most files being "P2P cached," are likely to both be copyrighted and infringing. This translates into a speedier delivery to peers of these popular, infringing files. n198

Second, as discussed in Part IV, one of the bottlenecks in sharing files via P2P is that the uploading speeds on most peers' computers are quite slow. In contrast, upload speeds from a commercial server owned by a legitimate content distributor, iTunes for example, are likely considerably faster than the upload speed on the average peer's computer. As a result, based on upload speeds alone, it is slower for a user to obtain an infringing file from a peer than to obtain the same file legally from a commercial service. A server used by an ISP to cache P2P files, however, also has upload times which are much faster than that of the average peer - in fact, probably equivalent to a commercial service. Thus, when the file is cached by the ISP, a user can receive an infringing file just as fast from a caching server as she can receive a non-infringing file from a legitimate service. Naturally, her incentive to request the infringing file for free from another peer instead of buying from a legitimate service increases.

[*461] Commercial servers, like those used by iTunes, are also often closer in terms of transmission distance to a user. n199 These are called content delivery networks, which use their own services to provide geographically close content. n200 We will give the example of a service like iTunes. The music service is based in California, but it provides songs to people all over the United States (and the world) via the Internet. n201 Naturally, the songs have a long way to travel to get to different cities. To improve the situation, iTunes pays for a caching service. The caching service company has infrastructures all over the country, specifically servers in many cities which are connected to a local ISP. n202 So, for example, files are cached in a server close to New York so that when songs are requested from New York, the songs come directly from the New York caching server instead of all the way from California. n203 This essentially makes the music service "local" instead of "long distance" and increases the speed at which users get their requests.

In contrast, when a user requests an infringing song from a peer, that peer may be located across the country. As with upload speeds, a commercial service may be closer in terms of transmission distance than a peer, and therefore, provide a faster service. But again, if the ISP has cached that song on its local caching server, the requested song will come to the user from the local server instead of from the peer's computer across the country. The ISP's caching practice makes the [*462] infringing file just as accessible as the non-infringing file from the legitimate commercial service.

The final way in which ISP P2P caching makes infringing files more available is by making it harder for copyright owners to protect their copyrights. P2P caching software defines a file as "popular" when there is a high level of demand for the file. As previously discussed, one can only assume that the demand for popular pirated songs is also high. Under these conditions the amount of infringing activity would be limited by the supply.

In its war on piracy, the RIAA's goal is to reduce both the demand and the supply of infringing files, but in practice it seems to focus more on the supply side. n204 One of the methods copyright owners use to enforce their rights is to prosecute peers who distribute infringing works via P2P. n205 In the P2P context, supply, at least at the beginning of each cycle, is rather limited. n206 If many people desire the file but only one has it, the queue to download it will be very long. The upload ability of this one peer is limited. Also limited is the number of peers that can download the file in parallel from him. When more people download the file, the supply increases and allows for a speedier download. However, this takes time. Presumably, most peers like to download, but are less enthusiastic about sharing. The exact reason for this phenomenon - whether pure egoism, the desire to preserve resources on a personal computer, or fear of being sued for sharing files - does not matter. After the downloading process is completed, many stop sharing files. This means less supply or fewer sources to download from. The RIAA also contributes to this process by warning and taking down the infringing files. n207 However, in the caching [*463] scenario, the ISPs may substitute the peers' supply with their servers - so, at least in theory and without any software constraint, it does not really matter how many peers are participating as suppliers. If, in the extreme situation, one peer (as in Example Five), or even better, none (as in Example Six), is needed to keep the cached copy alive - fighting all the peers would not really help the copyright owners to reduce piracy. Supply would be less of an issue, because for every peer the RIAA takes down, the ISP will substitute its direct service. So the download activity would be controlled almost only by the high demand. This means more piracy.

So, what are the pros and cons of P2P caching relative to the alternative of improving the network infrastructure? Both increase the network's speed and efficiency. On the one hand, P2P caching disproportionately facilitates infringement relative to non-infringing use, whereas improving infrastructure has a neutral impact. On the other hand, P2P caching is cheap whereas improvements in infrastructure are expensive. The question really comes down to whether the cost of improving infrastructure outweighs the disproportionate increase in infringement caused by P2P caching.

Another consideration in comparing P2P caching to improving the infrastructure is that improvements in the infrastructure may be a self-defeating solution for ISPs. Each time ISPs improve the network infrastructure, consumer use of the bandwidth quickly catches up and the network becomes clogged with traffic again. n208 As the ISPs would probably argue, why spend money on improvements which are ultimately unhelpful when the real problem is inefficient use of the network? A large percentage of the bandwidth is taken up by users sharing the same popular files. Why not simply use P2P caching to more efficiently transfer the few popular files which take up a disproportionate amount of bandwidth?

The counterargument is that it is unfair for ISPs to externalize the costs of operating an efficient network onto copyright owners. Caching technology serves as a good solution for the ISPs. It provides them with technology to receive the consumers' money without spending it. Like a magician, they create an illusion of high speed connection without providing it. This point also helps answer the [*464] question of whether the cost of improving the infrastructure outweighs the disproportionate increase in infringement caused by P2P caching. When P2P caching increases infringement, it is the copyright owners who pay. At least in terms of distribution of costs, perhaps the more equitable solution is that the ISPs should pay for improvements in the network infrastructure and then pass those costs on to their consumers. Thus, those who use their service to download legal or illegal files would pay the real price of having an efficient network.

It certainly seems that the role of the legal system is to channel this demand for P2P services in the right direction. The free market and the high demand for P2P services provide pressure on ISPs to provide the real thing - better infrastructure. If costs increase, then that is the real price of the P2P world. Without caching, the P2P world would not disappear. After all, P2P file sharing was in existence before P2P caching began and will likely continue regardless of the fate of P2P caching. Thus, to return to the original question: whether P2P caching would be transformative under the first factor of the fair use analysis - the answer appears to be that it is not very transformative.

b. Commercial Use

The second part of the analysis of the first fair use factor is a consideration of the commercial nature of the practice in question. Courts typically balance the transformative nature of a practice against its commercial nature. n209 The more transformative P2P caching is, the less importance a court gives its commercial nature and vice versa. n210

Given the difficulty in showing that P2P caching is transformative, as discussed previously, a court would likely give full weight to any finding that P2P caching is commercial in nature. n211 Unfortunately for ISPs, P2P caching is quite clearly commercial. ISPs use P2P caching because it allows them to draw more clients to broadband Internet services without paying the real price of expanding [*465] their infrastructure. n212 In other words, ISPs use P2P caching because it saves them money.

In some caching cases, the courts found that the transformative nature of the use outweighed the commercial nature of the use even though the defendant was a commercial company. n213 Those cases, however, are unlikely to help ISPs in P2P caching. The courts in those cases emphasized that caching was not directly commercial. n214 For example, when the purpose of caching web images was to create a visual search engine, to keep a copy for archival purposes, or to serve other clients needs that could not be served in a different way, the courts declared more than once that the specific use was not commercial, n215 that its commerciality was not of significant effect, n216 or that its transformative characteristics dominated its commercial aspects. n217 However, where copies of files were made without such a purpose, courts have declared the use to be commercial. n218 Since P2P caching is not very transformative because it is commercial in nature, it [*466] is unlikely that the first fair use factor will favor P2P caching at any given point.

c. Nature of the Copyrighted Work

The second factor of the fair use analysis deals with the nature of the copyrighted work. Here, the time-honored rule is that the more creative the work, the stronger protection it will receive. n219 Works that are creative in nature "are closer to the core of intended copyright protection" and are therefore entitled to greater protection. n220 On its face, this factor clearly favors the copyright owners. Music and films are highly creative works, and therefore, receive the strongest protection against infringement. n221 Generally, this factor is not considered "terribly significant in the overall fair use balancing," n222 but it may be important for ISPs because they do not have a strong argument for transformative use.

The ISPs might look to the web caching cases again for support. In Kelly, Field, and Perfect 10, the courts downplayed the creativity of the works at issue because the copyright owners had already made the works available to the public on the Internet. n223 The fact that the works were "previously published" undermined the fact that they were highly creative works. n224 As the court stated in Kelly, "published works are more likely to qualify as fair use because the first appearance of the artist's expression has already occurred." n225 Moreover, the previous publication does not have to be on the Internet; publication in [*467] any medium qualifies as a first appearance. n226 The previous publication also does not have to occur in a context where the work was made available to the public for free. n227 Several cases have upheld the same principle even when the copyright owner charged a fee for access. n228 This argument would clearly help ISPs in defending P2P caching. n229

Nevertheless, in the web caching cases, the second factor favored the plaintiff, even if only slightly. n230 Therefore, at the minimum, the second factor will probably also favor a plaintiff copyright owner in the context of P2P caching. Our assumption is that due to the specific characteristics of the P2P industry, the second factor would be considered even more favorable to the plaintiff.

d. Amount and Substantiality of the Use

The third fair use factor deals with the amount and substantiality of the use. n231 The calculation under this factor is that the more material that is taken from the original work, the less likely the use will be considered fair. n232 This factor, however, like the other factors, will tolerate a greater amount of copying if the court finds the use highly transformative. n233 The Supreme Court in Sony concluded that even a work copied in its entirety "does not have its ordinary effect of militating against a finding of fair use" when the work is transformative and a work that the viewer has been "invited to witness [*468] in its entirety free of charge ... ." n234 Courts have used this approach in the context of web caching, to hold that the copying of entire images n235 or entire webpages n236 was not infringement.

The problem in using this argument for P2P caching is that, unlike web caching, the author of the copied work probably did not give permission for users to see the work in its entirety before it was copied. In contrast, in web caching, the authors of the webpages which Google caches in its search engine intentionally make their webpages available for public viewing on the Internet. n237 The court in Perfect 10, however, found copying an entire image was fair use even when the author had not given permission to the general public to view its images. n238 The Perfect 10 court instead focused on whether the copying was only as much as necessary and found that it was necessary for Google, like Arriba in Kelly, to copy the entire image in its search engine - therefore the use was fair. n239

Whether the same approach applies to P2P caching depends on whether a court finds P2P caching transformative. On the one hand, as in Perfect 10 and Kelly, ISPs' caching servers have to copy and distribute the entire work to fulfill their purpose. It is useless for a peer to receive only part of the file she requested because she wants the whole file. However, if a court does not find the ISPs' purpose transformative, then the court would likely find copying the whole file is an unfair use.

e. Effect on Potential Markets

The fourth and final fair use factor considers the effect of the infringing use on the potential markets for the copyrighted work or on [*469] the value of the copyrighted work. n240 In P2P caching, the question is whether the act of caching has an effect on the market or on the value of shared works.

Once again, the findings in the web caching cases that caching had a minimal effect on potential markets do not help ISPs. On the web, one can assume web page owners are willing to share their content, often for free. This assumption does not hold in the P2P world. The vast majority of the owners do not give permission to share their work over the Internet. n241 Some of the shared works are not even published by their owners. n242 Furthermore, webpage owners have methods to protect themselves against copying. They can easily use the "no robots" metatags to prevent the caching of their websites. In fact, not using "no robots" metatags is considered the owner's fault to some extent (especially where this is the industry standard). n243 This assumption does not hold for the vast majority of the P2P cases either.

ISPs could argue that the actual effect of P2P caching on the market is low. Caching takes place only after a peer has decided she wants the file located on another peer's computer and has requested the file. Even without P2P caching, the file would be infringed through regular P2P sharing. Therefore, the impact of caching on the market is arguably minimal. However, as discussed under the first fair use factor, P2P caching seems to increase infringement overall. In any case, arguing that infringement is inevitable has never been an effective defense. A DVD bootlegger, for example, is not protected by the fact that if his business closes down, buyers will just get their bootlegged copies elsewhere.

Quite clearly, P2P caching has an effect on potential markets for the copyrighted files. In some cases, copyright owners have prevailed in the fair use analysis by narrowly defining the market, but it is hard to imagine a successful argument for P2P caching. Indeed, if the copyright owners tried to define the market as licensing caching services, this argument is doomed to fail. The Supreme Court has ruled that courts should only consider the effects on markets that "creators of [*470] original works would in general develop or license others to develop." n244 It is hard to imagine that anybody except ISPs would be interested in such a market.

At the same time, caching certainly affects other markets. Clearly, a more attractive download option pushes peers away from the legitimate channels of distribution. Thus, for example, a user might get her music files via P2P sharing instead of by downloading a file from iTunes. In Napster, the court found that the infringing activity might have two effects on the potential market: reducing audio CD sales and raising barriers to plaintiffs' entry into the market for digital downloading of music. n245 With the advent of iTunes and other legitimate music downloading ventures, the loss in the market for digital music downloading is not a speculative one, as it was to an extent in Napster, but one that can be measured in real dollars. n246 Although P2P sharing can be done without it, caching makes P2P sharing more attractive, especially when dealing with large, slow-downloading files, such as movies.

Moreover, fighting supply is also an important aspect of the problem. As discussed in Examples Five and Six, if a file is deleted from one computer, a copy may still reside on the ISP's server. Thus, fighting the peers would not make much of a difference in terms of supply; it is enough that only one computer has the file. Every time someone requests a download, the ISP steps in and substitutes its file for the peer's. Again, this has a major effect on the copyright owners' fight against infringement and therefore would have a major effect on the market for their work.

f. Conclusion for Fair Use

Considering all these factors together, it seems that without any restrictions, P2P caching is doomed to fail the fair use analysis. This conclusion is further supported by the courts' attitude towards P2P services. Given courts' tendencies to disfavor these services, n247 it [*471] looks like caching only amplifies many of P2P's negative effects, and therefore, would be treated in a similar manner. As we argue, the caching practice has many advantages to the extent that it economizes on the transportation of information while enhancing speed. But these savings have their costs. Piracy increases and perhaps even more importantly, P2P services lose many of their decentralized aspects. Allowing the ISPs to cache their services without any modification misses an opportunity to channel the demand to the real thing: a steady, speedy, and efficient P2P network.

B. ISPs Secondary Liability

Even if courts did not find caching ISPs liable for direct infringement, they could be found liable for secondary infringement. In secondary infringement, a party is liable for facilitating in some way the direct infringement of third parties. n248 Copyright law recognizes two types of secondary infringement: contributory infringement and vicarious infringement. n249 Roughly, contributory infringement "is based on the defendant's failure to stop its own actions," whereas vicarious infringement is based on a defendant's failure to stop a third party's actions. n250

Consider Example One in Part V, subsection B. A2, a peer on the network, requests the Harry Potter movie from B1, another peer. The ISP's caching server intercepts the request and instead sends A2 a cached copy of the movie. By copying Harry Potter, a copyrighted file, without permission onto his computer, A2 has directly infringed the movie's copyright. As discussed above, perhaps the ISP is also liable for direct infringement by caching the file. The remaining question is whether the ISP is liable for secondary infringement. n251

[*472]

1. Contributory Infringement

To be liable for contributory infringement, a defendant must both have knowledge of a third party's direct infringement and materially contribute to that infringement. n252 At first blush, material contribution appears to be the easiest element to prove against caching ISPs. In P2P caching, ISPs both copy and distribute the copyrighted files. In Netcom, for example, the court found that copying an infringing article onto an Internet newsboard and distributing it via the Internet constituted material contribution to both copyright infringement and distribution infringement. n253 Here, the copying and distribution involved in P2P caching would seem to count as material contribution.

Netcom, however, can be distinguished because caching is not necessary for the functioning of P2P sharing. Peers can share files directly without the assistance of P2P caching. Moreover, caching occurs after users have already decided to request an infringing file. The act of infringement, from the point of view of causality, is not a "but for" cause of the infringement as it is in Netcom. Without P2P caching, peers' direct infringement would still take place. However, this view misses the whole picture. As discussed in the analysis of fair use, P2P caching makes infringement easier in part by making the sharing of infringing files faster. By making infringement faster, P2P caching encourages more infringement. Thus, it would seem that without P2P caching, some infringing file sharing would not occur. Using the logic of "but for" causality, material contribution seems to be satisfied here. n254

The other requirement for a finding of contributory infringement is that the provider had knowledge of the infringement. n255 Of course, if a plaintiff can show direct knowledge in a contributory infringement [*473] case, the knowledge element is easy to prove. In some cases, the plaintiff can simply show that she notified the ISP of the infringement and that the ISP continued to contribute to the infringement. n256

Failing direct evidence of knowledge, courts have found the knowledge element satisfied by proof of imputed intent. n257 The Supreme Court borrowed imputed intent from patent law to apply to copyright law in Grokster, but arguably, the Supreme Court had already taken this step in its decision in Sony. n258 In Sony, the Supreme Court held that the characteristics of a product itself could be enough to establish contributory infringement. n259 As the Court would later point out in Grokster, the Sony Court essentially allowed the imputation to a defendant of intent to contributorily infringe solely from the nature of the defendant's product. n260

In Grokster, the Supreme Court recognized imputed intent more explicitly. n261 The Court found that the defendant's statements and actions directed toward promoting infringement established the defendant's intent. n262 Thus, imputed intent can be found in at least two ways: through distributing a product lacking a substantial non-infringing use (Sony) or by actively encouraging infringement through specific acts (Grokster).

a. Acts Directed to Promote Infringement

We will address acts directed toward promoting infringement first. Several courts have addressed the issue of what constitutes inducement in the context of promoting infringement. In Grokster, the defendant's promotional conduct was quite blatant. The defendant openly advertised the use of its peer-to-peer software for sharing files [*474] as a way to copy copyrighted files. n263 The Supreme Court found this conduct clearly demonstrated intent to promote infringement. n264 An ISP engaged in P2P caching and seeking to avoid secondary liability can easily refrain from Grokster-like blatant promotional conduct. The question remains, however, whether more subtle conduct could get a caching ISP into trouble.

Grokster at least sets boundaries of behavior. Whereas advertising a product's use as a way to copy copyrighted files constitutes inducement, "ordinary acts incident to product distribution" do not. n265 The Supreme Court in Grokster gave the example of offering technical support or product updates as such "ordinary acts." n266

Conduct on the spectrum between these two extremes is a gray area. Grokster indicates clearly that any promotion of a service as a means of infringing copyrighted works would constitute inducement. n267 But, would promotion that did not advertise infringement subject an ISP to liability? For example, would advertising the fact that caching drastically decreases traffic on the network because more than two-thirds of files requested by users have already been requested by other users? n268 In other words, would simply advertising the fact that P2P caching makes P2P sharing easier be enough, or would the ISP have to advertise that P2P caching facilitates infringement to be liable? Perhaps as long as the ISP did not promote infringement specifically, the ISP could protect itself by including a warning that the use of its product for infringement was illegal and that the ISP would close the account of any infringing user. n269

[*475] In Perfect 10, the Ninth Circuit attempted to clarify what the Supreme Court meant by "intentional[] encourage[ment of] infringement through specific acts." n270 Borrowing from tort law definitions of intent, the Ninth Circuit found that contributory liability applies when the "actor knowingly takes steps that are substantially certain to result in such direct infringement." n271 In applying this test, the Ninth Circuit in Perfect 10 did not address the extent to which active promotion leads to liability, but instead addressed when a failure to act leads to contributory liability. n272 The court held that a computer system operator is liable for contributory liability when it " "has actual knowledge that specific infringing material is available using its system' and can "take simple measures to prevent further damage' to copyrighted works, yet continues to provide access to infringing works." n273

Applying the test in Perfect 10 to caching ISPs, then, requires analysis of two issues: what amounts to "knowledge" and whether caching ISPs have "simple steps" at their disposal. Regarding knowledge, a notification from a copyright holder could satisfy the knowledge requirement, as discussed above. The more worrisome question for a caching ISP, however, is whether it could be held responsible for knowledge or constructive knowledge that copyrighted items are being infringed using its system when it does not have notice.

Under the case law, a non-caching ISP is not held to have knowledge of infringing files which users pass through its network. Courts have concluded that ISPs should not be required to monitor their files for infringement or for other tortious behavior, such as slander. n274 Indeed, holding ISPs responsible for knowledge of whether [*476] files passed through their networks are infringing would be counter-productive. Under the current state of technology, ISPs could not function effectively if they had to somehow monitor every file for infringement. The Ninth Circuit described the magnitude of such a task, at least as applied to Google's image search engine:

> Google's software lacks the ability to analyze every image on the Internet, compare each image to all the other copy-righted images that exist in the world ... and determine whether a certain image on the web infringes someone's copyright. n275

Certainly, hobbling ISPs with such a responsibility would be bad public policy if it made operating a network no longer feasible and profitable.

The analysis changes, however, when the ISP caches files instead of merely acting as a conduit. On the one hand, the ISP engaged in P2P caching is already analyzing files to determine their popularity. Asking ISPs to identify whether a file is infringing in addition to popular seems like a small imposition, especially when the ISP would only be analyzing the small subset of P2P files which it has decided to cache. Thus, arguably, ISPs should be tasked with the constructive knowledge of whether cached files are infringing. Given this knowledge, it would be only a "simple step" for the ISPs to program their caching software not to cache the infringing files.

On the other hand, imposing this responsibility on ISPs could be a crushing burden which might ultimately make providing Internet service too expensive to be feasible. n276 To begin with, there are no failsafe methods at the moment to determine whether a file is infringing. n277 At best, ISPs could identify only a percentage of [*477] infringing files, with the added danger of incorrectly identifying some non-infringing files as infringing. Moreover, ISPs would be in a constant "arms race" with users (i.e. hackers) who would learn quickly how to outwit techniques ISPs used to identify infringing files. n278 Costs would mount for ISPs as they would bear the technical costs of applying counter-infringement techniques and monitoring their effectiveness. Add to this the cost of legal advice to determine whether ISPs were taking adequate steps and, of course, to fight legal liability suits and the burden becomes overwhelming. n279

Whether ISPs should be tasked with constructive knowledge of infringing files, and to what extent, appears to be essentially a question of the effectiveness and cost of technology available to analyze files. However, there is also a strong argument that, by engaging in P2P caching, ISPs should be made liable for any subsequent increase in infringement - and should therefore at least take simple steps to avoid caching infringing files. The possibility alone that P2P caching could lead to this crushing burden should arguably discourage ISPs from engaging in the practice.

b. Substantially Non-Infringing Use

A provider can also be found liable for contributory infringement, even if it does not take any actions towards promoting infringement, simply because the design of the product it offers does not have a "commercially significant noninfringing use." n280 It is unclear from case law what exactly "significant" means. It could be "significant" in absolute terms or "significant" relative to the infringing use or perhaps [*478] potentially significant. n281 Assuming the analysis considers relative magnitudes, it looks quite similar to the analysis under the first fair use factor, transformativity. The issue is whether the usefulness of P2P caching in increasing network efficiency, a "non-infringing use," outweighs the additional infringement P2P caching facilitates. As discussed under the first fair use factor, the balance of benefit versus harm does not seem to favor P2P caching. P2P caching appears to increase infringement relative to non-infringement, essentially externalizing the cost of improving the network onto copyright holders. The alternative, spending the money to increase network infrastructure, seems to be more fair and to better align the costs with the benefits.

But the meaning of "significant" in "commercially significant noninfringing uses" is not entirely clear. n282 A non-infringing use may not need to be significant relative to the infringing use. One interpretation of Sony is that the significant use must be potentially large. n283 In Sony, the non-infringing use was "time-shifting," the practice of using the technology at issue, VTRs, to tape a television show and watch it later. n284 A distinction between VTRs and P2P caching, however, is that VTRs made possible a new non-infringing use: "time-shifting." Prior to VTRs, it was not possible for an ordinary American to watch a show at a time of her choosing. Perhaps in Sony, the Supreme Court chose to be deferential to a new technology. Indeed, the Supreme Court's decision not to burden VTR-makers with secondary liability for infringement appears quite far-sighted since it [*479] undoubtedly contributed to the emergence of the home video industry. Here, however, P2P caching only facilitates the already existing practice of P2P sharing. P2P caching does not enable a new non-infringing use with unforeseen potential. Rather, since P2P sharing of non-infringing files already exists, it is relatively easy to predict how much non-infringing use will result from P2P caching. As a result, this interpretation of "significant non-infringing" use does not seem to favor P2P caching either.

Another approach is that of Judge Posner in Aimster. Judge Posner held that even when a service has substantial non-infringing uses, the product's provider must show that "it would have been disproportionately costly for him to eliminate, or at least reduce substantially, the infringing uses." n285 Taking this approach, the analysis might be similar to that discussed in the previous section: whether ISPs could feasibly identify and prevent the caching of infringing files. n286 This seems in large part a function of the technology available to do so. However, the ISPs and the courts may be disinclined to enter the morass of determining what steps are "enough" as both the technology to detect infringing file sharing and the counter-technology rapidly evolve. Engaging in P2P caching appears to be a risky practice for ISPs with regard to contributory liability.

2. Vicarious Liability

A finding of vicarious infringement rests on two criteria: that the provider had the right and ability to control the direct infringer's acts, and that the provider received a direct financial benefit from the infringement. n287 How far the doctrine of vicarious liability extends is not certain. Although there has been a trend in recent cases to broaden [*480] vicarious liability, courts have been reluctant to apply this "strong" version of vicarious liability to ISPs. n288

Under the strong version of vicarious liability, as exemplified in Fonovisa v. Cherry and Ellison v. Robertson, among other cases, ISPs would almost certainly be liable for P2P caching. n289 The first requirement, the right and ability to control a direct infringer's acts, may simply be shown from the ISP's ability to terminate a user who is discovered to be engaging in infringing activity. In Fonovisa, the appellate court determined there was a valid claim for vicarious infringement against the operator of a swap meet because the owner could "terminate vendors for any reason whatsoever and through that right had the ability to control the activities of vendors on the premises." n290 In the Internet context, the court in Perfect 10, found that a company selling adult verification software to websites had the right and ability to prevent infringement of the plaintiff's images on those sites, because it could simply stop providing its services to infringing websites. n291

With regard to the second requirement, that the service provider benefits from the direct infringement, the strong version of vicarious liability requires only an indirect connection between the infringement and the benefit. n292 The fact that the availability of infringing goods acts as a " "draw' for customers" is enough to show a benefit. n293 For example, in Napster, the court found that users were attracted to Napster's service because they could obtain infringing music by using it. n294 The court considered Napster's financial benefit from these increased users a "benefit" for purposes of vicarious liability. n295

[*481] Applying this reasoning to P2P caching, ISPs appear to meet the benefit requirement. An ISP that offers P2P caching is likely to develop a reputation for providing better services for infringing activity, specifically making infringing files and faster downloads more available, which will almost certainly act as a draw for customers. In turn, the ISP will benefit financially because they will receive more subscription fees from more customers.

However, under the weaker version of vicarious liability, an ISP's liability is not as clear. With regard to the "right and ability to control" requirement, some courts have required significantly more evidence of control than just the ability to terminate a customer. n296 As one court in this line of cases stated, a defendant has the right and ability to control a direct infringer only if their paths "crossed on a daily basis, and ... the party against whom liability is sought is in a position to control the personnel and activities responsible for the direct infringement." n297 In the Internet context, courts have required some practical ability to recognize and prevent infringing actions within the constraints of the system. In Netcom, the court found there was a genuine issue of fact as to whether Netcom had this right and ability because the plaintiffs brought evidence of multiple expectations and usages showing a relationship of control. n298 The plaintiffs argued that Netcom set terms and conditions for users, that custom and usage had established a "netiquette" in which service providers act to prevent infringement, that Netcom had sanctioned users before, and that Netcom could identify postings that contained particular words. n299 Similarly, in Napster, the court did not end its analysis with the finding that Napster could terminate users. n300 The court analyzed whether Napster could [*482] control users within the architecture of its system. n301 Finding that Napster could search its file index for infringing names, the court found that Napster did have the ability to "police." n302

Under this analysis, a court would consider a variety of factors in evaluating an ISP's right and ability to control infringement when engaging in P2P caching. The court might consider whether the ISP sets terms and conditions for users, has sanctioned users before, and whether it could prevent infringement within the constraints of its system. n303 In considering the ISP's ability to "police," the court might conduct an analysis of an ISP's technical ability to identify and prevent infringement similar to the analysis we conducted for contributory infringement. n304 As discussed, the outcome of such an analysis would hinge to a great extent on the technology available to the ISP.

With regard to the benefit requirement, courts have found no direct financial benefit from infringement where users pay a fixed fee to the defendant. n305 The courts reason that the ISP only benefits from infringement if it receives a portion of the income from each infringed work. n306 In the Internet service provider business, users typically pay a monthly fee for the right to use the Internet service. As a result, ISPs do not directly benefit if customers use the service to engage in infringing activity. An argument against allowing a broader definition of benefit is that ISPs benefit too little from the "draw" of infringement to penalize them for it. As Nimmer states in his treatise, "large, commercial ISPs derive insufficient revenue from isolated infringing bits, in the context of the billions of bits that cross their servers, to characterize them as financially benefiting ... ." n307

Which version of vicarious liability would be applied to ISPs is not a clear-cut question. Courts have shied away from making ISPs liable in the past. n308 Cases, however, show a trend toward the stronger [*483] version of vicarious liability. n309 Under the strong version, it seems clear that ISPs would be liable.

All in all, P2P caching should tip the balance, if only slightly, toward vicarious liability for ISPs. When ISPs engage in P2P caching, they have demonstrated some right and ability to control infringement by choosing which files to facilitate P2P sharing. Although ISPs may have no foolproof method to distinguish infringing from legitimate files, it seems that P2P caching tends to encourage infringement. After all, ISPs have the right and ability to control the resulting infringement by simply refraining from P2P caching, and the fact that ISPs engage in P2P caching for financial reasons seems to show some financial benefit. Nonetheless, this is a borderline case.

C. DMCA Safe Harbor - How Courts Should Implement Section 512(b), if They Do

Assuming arguendo that ISPs are liable as direct or indirect infringers, would they be entitled to the DMCA safe harbor protection with regard to system caching?

Case law holds that section 512 safe harbor provisions apply to both direct and indirect infringements, and therefore provide shelter against both. n310 However, as the following discussion will show, it is unclear whether section 512(b) can be construed to apply to P2P caching.

Section 512(b), entitled "System Caching," provides shelter from copyright infringement for "intermediate and temporary storage of material" on the ISP's system. n311 This section carefully delineates the conditions under which such protection is granted. n312 In setting these [*484] conditions, Congress clearly had a specific technology in mind: web caching. The purpose of section 512(b) was to allow ISPs to cache web pages and by doing so, to allow them to provide services at greater speed. n313 Since the caching could potentially involve unauthorized duplication and distribution of information, the ISPs asked for specific provisions to protect them from liability. n314

To fall within the safe harbor boundaries, the ISP has to show that the cached material was made available online by "a person other than the service provider," that "the material is transmitted from the person described ... through the system or network to a person other than the person described ... at the direction of that other person," and "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 ... request access to the material from the person described ... ." n315

However, complying with these terms is not enough. An ISP must also comply with several more requirements. The role of the vast majority of these requirements is to ensure that the interests of website owners that made materials available online are not compromised. Thus, in order to prevent distortion of the owner's speech, ISPs cannot modify the website's content in any way during caching. n316 The ISP must also comply with the protocols set by the person who made the material available online regarding refreshing, reloading, or other updating of information. n317 Another requirement forbids the ISP from tampering with information-gathering technology associated with a website. n318 Essentially, the website owner should be able to gather information about users to the same extent that they could if the users accessed the website directly rather than through the cached version. n319 [*485] These requirements are concerned with "cookies" and similar technologies. Moreover, if the website owner has set up a barrier to entry on his website (such as a password, a fee, or both), the ISP must ensure that users comply with the terms of entry on the cached copy, as well. n320 For example, if access to a pay-per-view site requires a password, a user should not be able to access the file via caching, unless she has the password. n321 These requirements reflect the legislature's concern when enacting the law: to balance protection for distributors of online material against user interest in minimizing traffic when many users try to access the same website simultaneously.

The requirements above protect the party who put the information online. However, the last safe harbor requirement for ISPs protects the interests of third parties, specifically, copyright owners. n322 If copyrighted material is made available online without the copyright owner's permission, the service provider should respond expeditiously to remove or disable access to it "upon notification of claimed infringement." n323

Reading these very specific conditions, one cannot escape the conclusion that, when enacting section 512(b), Congress had a specific action in mind: distribution of information via the web platform. The question is whether we can apply this section to the P2P caching practice. The courts have not specifically addressed this issue yet. They have, however, addressed the application of other subsections of section 512 to the P2P industry.

In RIAA v. Verizon, the D.C. Circuit discussed the duties imposed on ISPs when acting as mere conduits of P2P traffic. n324 In the process, the court had to examine the legislative history of the safe harbor provisions with regard to their scope and applicability. The court ruled that "the legislative history of the DMCA betrays no awareness [*486] whatsoever that Internet users might be able directly to exchange files containing copyrighted works ... P2P software was "not even a glimmer in anyone's eye when the DMCA was enacted.' " n325 The court ruled with respect to section 512(h) that "Congress had no reason to foresee [its] application ... to P2P file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along." n326

In Verizon, this conclusion worked against the RIAA. It prevented the RIAA from getting information from ISPs about the infringing peers. n327 Referring to Sony, n328 the court stated:

> We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen Internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress. n329

Given the Verizon court's firm position, would this same dismissive approach be applied to section 512(b) as well? This time, however, the same approach would work in RIAA's favor by removing the protective shield from ISP caching practices. Section 512(h) covers situations in which an ISP can be subpoenaed, holding that subsection (h) does not apply to P2P sharing and thus protects ISPs from being [*487] subpoenaed. n330 Section 512(b), however, covers the safe harbors which protect ISPs from liability. n331 If subsection (b) does not apply to P2P caching, then ISPs do not have the benefit of those safe harbors to protect them from liability in P2P caching. Whether section 512(b) applies to P2P caching has not yet been addressed by the courts.

The paradigmatic scenario addressed by section 512(b) is that in which someone makes the information available online and others access that information via the cached copies. Section 512(b) balances the interests of the parties in the context of the World Wide Web, particularly web caching. Does it make sense applied to P2P caching? The answer is that it clearly does not, because the interests of the parties are different in the P2P context.

P2P sharing involves the same three principal parties as in web caching: users, copyright owners, and those who make material available online (for convenience's sake, we will call them "distributors"). The interest of users in both P2P and web contexts is to gain access to material which is available online. However, users in the web context care more about getting material from the right distributor. For example, a P2P user cares little about which distributor put the Harry Potter movie online (as long as it is a good copy), whereas a web user looking for the J. Crew storefront website wants the website which the J. Crew company put online. n332

The interests of the distributors also differ. Distributors of websites are more likely to be the creators of the material they publish online. n333 As a result, they are more likely to care how their material is used. Moreover, a website, by nature, is more interactive than a P2P file. The owner of the website often wants to continue interacting with [*488] the user by gathering information about the user, conducting transactions, or updating information on the website. A P2P file is more like a "fire and forget" missile. Once the distributor publishes the file, he typically has no more interaction with either the file or the user. Therefore, the section 512(b) conditions which require an ISP to comply with the distributors' restrictions regarding accuracy, n334 information-gathering, n335 and access n336 serve less of a purpose in the P2P context.

The interests of copyright owners, however, are the same in both contexts in that they do not want copies made and distributed without their permission. As mentioned, section 512(b)(2)(E) protects the interests of copyright owners by requiring ISPs to remove or disable access to cached copies of works that the copyright owner has stated are infringing. n337 Section 512(b)(2)(E), however, only requires ISPs to remove or disable the cached copy if the copyright owner provides notice that the source from which the cached copy was obtained has also been disabled or the copy removed. n338 This section is less useful for copyright owners in the P2P context because the cached file could be downloaded from many different sources. In the web context, the ISP caches a website from one specific source, so it is easier for the copyright owner to confront the source of the website.

The courts could theoretically solve this problem by restricting P2P caching to the process described in Example Two: caching a file from one peer and providing the cached copy only to other peers who specifically request that particular copy. However, this would not provide the efficiency ISPs want. Restricting P2P caching to the process in Example Two would create too many identical copies on an ISP's servers and would not provide them with the same benefits in terms of decreasing the data transportation burden, increasing speed, and increasing consumer satisfaction. The ISP's practice is therefore to cache a file from any peer, while providing the cached copy to every peer who wants the file, irrespective of whether the file is requested from the original peer or from another (Examples Three, Five or Six). The extreme situation is that in which a file is not located on any peer's [*489] computer, but is still available on the ISP's caching server (Example Six). In the world of P2P caching, copyright owners find themselves in a weak position because fighting piracy, even given the tools that are provided by section 512, is doomed to fail.

The rationale of the court's ruling in Verizon seems to apply to section 512(b) as well. Both from the text and legislative history, it is clear that P2P technology was not predicted. While one can try to fit the narrow P2P caching practice (Example Two) into the DMCA text, fitting the broader caching practice seems impossible. The black letter interpretation thus favors the conclusion that P2P caching is not shielded under the DMCA. Although the argument could be made that section 512(b) should be interpreted more broadly due to major technology shifts, that would conflict with the rationale in RIAA. n339 The DMCA safe harbor clauses were technology-specific amendments. n340

They were carefully tailored to balance the interests of users, ISPs, and rights holders. n341 The P2P platform has radically changed the rules of the game. At a minimum, as discussed, the interests of the parties are significantly different, and allowing P2P caching will exacerbate these changes even further.

Therefore it is the role of Congress to broadly re-think these issues. An extensive protective shield should not be conferred on ISPs without deliberation. These deliberations should consider the legitimacy of the P2P platform, its benefits, drawbacks and alternatives. Finally, Congress should consider how adding P2P caching alters the balance of interests of the P2P platform.

[*490]

VII. Conclusion

Thus far, ISPs have by and large escaped liability for the massive infringement taking place on their systems. Instead, software networks which operate as an additional layer of organization on top of the ISP's physical networks have faced liability: Napster, Grokster, Aimster, and Netcom, for example. But, by caching, ISPs have entered the realm of copying and distributing infringing files themselves. Under our analysis, unless ISPs can show that the benefits outweigh the costs of P2P caching, they should be and likely will be, found liable for infringement. The advantages of P2P caching are the increases in efficiency and money saved by not paying for the equivalent improvement in infrastructure. The cost is the increase in infringement facilitated by P2P caching. Our analysis indicates that P2P caching should not be considered a fair use because ISPs use caching to externalize the costs of operating an efficient network onto copyright holders, whereas investing in improved infrastructure would more equitably spread the costs among consumers.

More importantly, even if ISPs could present evidence that might justify granting them protection from liability for P2P services, P2P caching must be closely analyzed before granting ISPs a safe harbor. The laws and consensus which have developed to protect web caching cannot be blindly applied to P2P caching. The processes involved and the interests of the parties are too dissimilar in both the web and P2P contexts. Therefore, the courts and Congress must evaluate this evidence in order to determine whether or not P2P caching, like web caching, should be accorded its own safe harbors and fair use protection.

Legal Topics:

For related research and practice materials, see the following legal topics:
Communications LawRelated Legal IssuesCopyrightComputer & Internet LawCopyright ProtectionGeneral OverviewCopyright LawCivil Infringement ActionsElementsCopying by Defendants

FOOTNOTES:

n1. European ISPs Find Solution to P2P Bandwidth Problem, Bus. Wire (July 10, 2003) (available at http://findarticles.com/p/articles/mi_m0EIN/is_2003_July_10/ai_105048914/).

n2. P2P caching is file sharing where a "user's computer uses ... information to establish a connection with the host user and downloads a copy of the contents ... from one computer to the other ... ." *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1012 (9th Cir. 2001).*

n3. Comcast, a large ISP, has been the subject of bitter consumer complaints regarding a technique it used to prevent P2P sharing from slowing its networks. Comcast limited the use of its networks for files using the protocols of popular P2P services (such as BitTorrent). Consumers complained on the grounds that Comcast had limited their use of Internet services without any disclosure or reduction in price. Vishesh Kumar, Comcast, BitTorrent to Work Together on Network Traffic, Wall St. J. B7 (Mar. 27, 2008); Tom Pullar-Strecker, ISPs Try to Turn Torrent; P2P Traffic Light "Amber,' N. Z. Infotech Wkly 6 (Jan. 28, 2008); see also Lim Pun Kok, Speeding up App Traffic, New Straits Times 10 (Aug. 21, 2006); Sandvine, Traffic Management, http://www.sandvine.co.uk/products/traffic_management.asp (accessed Apr. 25, 2010).

n4. Cisco, Cisco Visual Networking Index: Forecast & Methodology, 2008-2013 at 1-2, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf (June 9, 2009).

n5. See Nelson Minar & Marc Hedlund, A Network of Peer-to-Peer Models through the History of the Internet, in Peer-to-Peer: Harnessing the Power of Disruptive Technologies, 3-4 (Andy Oram ed., O'Reilly Media 2001).

n6. Guy Pessach, An International-Comparative Perspective on Peer-to-Peer File-Sharing and Third Party Liability in Copyright Law: Framing the Past, Present, & Next Generations' Questions, *40 Vand. J. Transnatl. L. 87, 124 (2007);* see also Mark Lander, The Media Business; For Music Industry, U.S. is Only the Tip of Piracy Iceberg, N.Y. Times A1 (Sept. 26, 2003).

n7. Pessach, supra n. 6, at 124.

n8. Id.

n9. Id.

n10. Sebastian Rupley, Offload Those Music Files; A UK-based Company Says it Has a Solution for the Bandwidth Drain Associated with File Sharing, http://www.pcmag.com/article2/0,2817,1126275,00.asp (June 13, 2003).

n11. The major cases are: *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 918 (2005); In re Aimster Copy. Litig., 334 F.3d 643, 645 (7th Cir. 2003); A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).*

n12. *17 U.S.C. § 512*(b) (2006).

n13. E.g. *Rec. Indus. Assn. of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003).*

n14. For a useful overview of ISP liability in the U.S., see Xavier Amadei, Note: Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with a Specific Focus on Copyright Defamation, and Illicit Content, *35 Cornell Intl. L.J. 189, 198-203, 213-16 (2001);* see also Alfred C. Yen, Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, & the First Amend., *88 Geo. L.J. 1833, 1871-72 (2000).*

n15. See e.g. *Grokster, 545 U.S. at 919-20; Aimster, 334 F.3d at 654-56; Napster, 239 F.3d at 1027.*

n16. See *17 U.S.C. § 512*(b) (2006).

n17. *In re Charter Communs., Inc., 393 F.3d 771, 773 (8th Cir. 2005).*

n18. Minar & Hedlund, supra n. 5, at 16. ("In a fully decentralized system, not only is every host an equal participant, but there are no hosts with special or administrative roles.").

n19. See id. at 10.

n20. Id.

n21. See Philip W. Esbenshade, Student Author, Hacking: Juveniles and Undeterred Recreational Cybercrime, *23 J. Juv. L. 52, 52-54 (2003).*

n22. See Minar & Hedlund, supra n. 5, at 16-17.

n23. See id.

n24. See id.

n25. See id. at 17.

n26. Id. at 3-4

n27. Cisco, Cisco Service Control Application for Broadband-Usage Analysis & Reporting 1, http://www.cisco.com/en/us/prod/collateral/ps7045/ps6129/ps6133/ps6151/prod_white_paper9099aecd802b0756.pdf (accessed Apr. 25, 2010).

n28. Minar & Hedlund, supra n. 5, at 4.

n29. Id. at 5.

n30. See id. at 8-9.

n31. Id. at 9.

n32. Id.

n33. Id.

n34. Napster is an Internet website that allows digital sound recordings to be shared among users that download its software. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).*

n35. Minar & Hedlund, supra n. 5, at 15-16.

n36. Id. at 16.

n37. See *Napster, 239 F.3d at 1011.*

n38. Intuitively, it makes sense that as more people use the Internet, there will be a need for more sources to provide the information the users are requesting. P2P technology has attempted to meet this demand.

n39. WAREZ is an Internet site where a user can search for shared information or media. Warez.com, http://www.warez.com (accessed Apr. 25, 2010). Also, " "warez' ... is well-known Internet slang for pirated content ... ." *Arista Recs. LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 133 (S.D.N.Y. 2009).*

n40. Placing infringing files on other websites, with or without pointing to them via links, was not a very successful practice either. See *Intell. Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290, 1291-95 (D. Utah 1999)* (The court extended liability to the actors in this case, targeting both the referring and the referred-to sites); *Arista Recs., Inc. v. Mp3Board, Inc., 2002 WL 1997918 at 1* (S.D.N.Y. Aug. 29, 2002).

n41. Tim Wu, When Code Isn't Law, *89 Va. L. Rev. 679, 709, 728 (2003).*

n42. *Id. at 709.*

n43. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001);* Wu, supra n. 41, at 709.

n44. Alec Klein, Going Napster One Better; Aimster Says Its File-Sharing Software Skirts Legal Quagmire, Wash. Post A1 (Feb. 25, 2001).

n45. *Napster, 239 F.3d at 1011-12.* Napster's programmers must have carefully read the law and realized that, based on the interpretation of the law at that point in time, indexing songs without keeping a copy of the actual files on the main Napster's servers, was not a copyright violation. Wu, supra n. 40, at 707-09, 728-29.

n46. See Minar & Hedlund, supra n. 5, at 17; *Napster, 239 F.3d at 1011-12.*

n47. Grokster is a software company that allows users to download and share files on the *Internet. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 912, 919-20 (2005).*

n48. David W. Opderbeck, Peer-to-Peer Networks, Technological Evolution, & Intell. Prop. Reverse Priv. Atty. Gen. Litig., *20 Berkeley Tech. L.J. 1685, 1698 (2005).*

n49. Id.

n50. *Id. at 1699.*

n51. See Minar & Hedlund, supra n. 5, at 15-17.

n52. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).*

n53. See id.

n54. *In re Aimster Copy. Litig., 334 F.3d 643, 645-46 (7th Cir. 2003).*

n55. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 919-20 (2005).*

n56. *Id. at 941; Aimster, 334 F.3d at 654-55; Napster, 239 F.3d at 1024.*

n57. *Grokster, 545 U.S. at 919.*

n58. *Id. at 920.*

n59. Id.; see also *Aimster, 334 F.3d at 647* ("What we have described so far is a type of Internet file-sharing system that might be created for innocuous purposes such as the expeditious exchange of confidential business data among employees of a business firm.").

n60. *Grokster, 545 U.S. at 920.* The Court followed the description of the advantages of P2P networks with a footnote on the disadvantages, namely inefficient searches, no incentive to minimize storage or bandwidth consumption and, most importantly, a lack of control, particularly over infringement. *Id. at 920 n. 1.*

n61. *Grokster, 545 U.S. at 928* ("The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the tradeoff."); *Aimster, 334 F.3d at 649-50; Napster, 239 F.3d at 1021-22.*

n62. *Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).*

n63. *Id. at 420.*

n64. Id.

n65. *Id. at 436.*

n66. *Id. at 442.*

n67. Id. ("One potential use of the Betamax plainly satisfies this standard, however it is understood: private, noncommercial time-shifting in the home.")

n68. *Id. at 446-47.*

n69. See *id. at 442; Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 941 (2005); In re Aimster Copy. Litig., 334 F.3d 643, 654-55 (7th Cir. 2003); A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).*

n70. *Grokster, 545 U.S. at 939-40.*

n71. *Aimster, 334 F.3d at 651-52.*

n72. *Napster, 239 F.3d at 1022-23.* In its contributory liability analysis, the court concluded, "the record supports the district court's finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material." *Id. at 1022* (emphasis in original). And, the court ended its vicarious liability analysis with the statement: "Napster's failure to police the system's "premises,' combined with a showing that Napster financially benefits from the continuing availability of infringing files on its system, leads to the imposition of vicarious liability." *Id. at 1024.*

n73. *Aimster, 334 F.3d at 652-53.*

n74. *Id. at 653.*

n75. *Grokster, 545 U.S. at 938* ("Here, the summary judgment record is replete with other evidence that Grokster and StreamCast, unlike the manufacturer and distributor in Sony, acted with a purpose to cause copyright violations by use of software suitable for illegal use."); *Napster, 239 F.3d at 1021* ("Regardless of the number of Napsters' infringing versus noninfringing uses, the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights.").

n76. *Aimster, 334 F.3d at 649-50.*

n77. See *Grokster, 545 U.S. at 941* ("Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement.")

n78. See *Napster, 239 F.3d at 1022-23.*

n79. See *Aimster, 334 F.3d at 653* ("If the only effect of a service challenged as contributory infringement is to enable copyrights to be infringed, the magnitude of the resulting loss, even whether there is a net loss, becomes irrelevant to liability.").

n80. Niva Elkin-Koren, Making Tech. Visible: Liability of Internet Service Providers for Peer-to-Peer

Traffic, 9 N.Y.U. J. Legis. & Pub. Policy 15, 19 (2005-2006) [hereinafter Elkin-Koren, Making Tech. Visible].

n81. Id.

n82. Id. at 20.

n83. Id. at 23.

n84. Id.

n85. Id.

n86. Id.

n87. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 920 (2005).*

n88. See The Torrent Becomes a Flood, Personal Computer World, "Divide & Conquer" (July 12, 2007).

n89. Id. at "Swarming."

n90. Id.

n91. Id.

n92. See id. at "Divide and Conquer" & "Swarming."

n93. Id. at "Swarming."

n94. See id. at "Peer Pressure" & "Naming Names."

n95. For example, the users of Emule also have access to peers in the Edonkey and Kazaa networks. Id. at "Naming Names."

n96. See id. at "Swarming."

n97. Elkin-Koren, Making Tech. Visible, supra n. 80, at 21.

n98. Id.

n99. Id.

n100. Id. at 22.

n101. Kirk L. Kroeker, P2P Networks Evolve: An Interview with StreamCast CEO Michael Weiss, http://www.technewsworld.com/story/32673.html?wlc=1248223400 (Jan. 26, 2004).

n102. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 920 n. 1 (2005).*

n103. Id.

n104. Id. The Supreme Court's argument is not very clear. If the files are popular, many users will download them anyway. It does not matter whether a central server is involved or not. Each peer who makes the file available to others downloaded it herself in the first place.

n105. See BroadbandInfo.com, The Difference between Upload & Download Speed for Broadband DSL, http://www.broadbandinfo.com/cable/speed-test/the-difference-between-upload-and-download-speed-for-broadband-dsl.html (accessed Apr. 25, 2010); U.S. Govt. Accountability Off., Broadband Deployment Plan Should Include Performance Goals & Measures to Guide Fed. Investment 3-6 (May 12, 2009) (available at http://www.gao.gov/new.items/d09494.pdf).

n106. *BroadbandInfo.com, supra n. 106.*

n107. Sandvine, Inc., Meeting the Challenge of Today's Evasive P2P Traffic: Serv. Provider Strategies for Managing P2P Filesharing 2-4, http://www.larryblakeley.com/Articles/P2P/Evasive_P2P_Traffic.pdf (Sept. 2004).

n108. Peers can further restrict their upload capabilities by adjusting the number of simultaneous uploads. The Torrent Becomes a Flood, supra n. 88, at "Peer Pressure." The software on many personal computers makes these adjustments available to improve the functionality of the sharing computer. Uploading takes computer resources away from other tasks. This limitation, however, has its price: The more the user limits the upload, the more he restricts his download capabilities. See id. at "Torrents, Seeds & Trackers" & "Swarming."

n109. This does not mean the overall request for a file located on many computers on the Internet, but rather the request for a specific file located on a single peer computer. See id. at "Peer Pressure."

n110. See Sandvine, Inc., supra n. 107, at 2-3.

n111. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 920 n. 1 (2005).*

n112. Elkin-Koren, Making Tech. Visible, supra n. 80, at 18.

n113. The Torrent Becomes a Flood, supra n. 88, at "Smart Moves."

n114. See e.g. Mark McCracken, Feeding That Foreign TV Habit: You Don't Have to Rely on Videotapes from Mom Anymore: Many Shows Can Be Found Via Broadband & P2P, Japan Inc. (Jan. 1, 2003) (available at http://www.thefreelibrary.com/Feeding+that+foreign+TV+habit+you+don't+have+to+rely+on+videotapes...-a0104732911); Ben Levanger, Unreleased Movie Downloads-Can This Be True, http://www.articlesbase.com/movies-articles/unreleased-movie-downloads-can-this-be-true-490829.html (July 20, 2008).

n115. See e.g. McCracken, supra n. 114; Peter Svensson, Company Will Charge Heavy Internet Users Extra: Frontier Communications to Impose Caps on Free Downloads & Uploads, http://today.msnbc.msn.com/id/27519819/ns/technology_and_science-tech_and_gadgets/ (Nov. 3, 2008).

n116. See John Borland, CNET News, Putting a Lid on Broadband Use, http://news.cnet.com/2100-1034_3-5079624.html (Sept. 22, 2003).

n117. Svensson, supra n. 115; Borland, supra n. 118.

n118. This is not the only billing method. ISPs are starting to experiment with charging according to the traffic actually used. See e.g. Svensson, supra n. 115.

n119. Elkin-Koren, Making Tech. Visible, supra n. 80, at 22; Sandvine, Inc., supra n. 107, at 3.

n120. Stefanie Olsen, P2P Caching: Unsafe at Any Speed?, http://news.cnet.com/2100-1025_3-1027508.html (July 18, 2003); Sandvine, Inc., supra n. 107, at 4.

n121. Sandvine, Inc., supra n. 107, at 4-5.

n122. Brad Reed, Q&A: Robert Shapiro Talks Tiered ISP Pricing & the Digital Divide, The Standard (Sept. 9, 2009) (available at http://www.thestandard.com/news/2009/09/10/q-robert-shapiro-talks-tiered-pricing-and-digital-divide?page=0%2CO).

n123. Id.; Svensson, supra n. 115.

n124. *Reed, supra n. 122;* see Sandvine, Inc., supra n. 107, at 4-5.

n125. The user's P2P software asks a network of peers for the file. Matthew Lucas, What Are P2P Networks?, http://www.billingworld.com/articles/feature/What-Are-p2p-Networks.html# (Mar. 1, 2007). Each peer passes on the query until the file is found. Id.

n126. To keep the example simple, we assumed A1 gets the entire file from B1. However, this is not always the case. Because the file is broken into many sub-parts, each could be downloaded from a different computer. For a brief description of how BitTorrent has changed P2P file sharing, see The Torrent Becomes a Flood, supra n. 88, at "Torrents, Seeds & Trackers" & "Divide and Conquer."

n127. If several computers are involved, A1 will simultaneously download the file parts from several computers and therefore the download speed will be limited by his downloading speed or the slowest uploading computer's speed. Manaf Aghaibeh & Kostas G. Anagnostakis, On the Impact of P2P Incentive Mechanisms on User Behavior 2, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.5763&rep=rep1&type=pdf (accessed Apr. 25, 2010).

n128. The Torrent Becomes a Flood, supra n. 88, at "Peer Pressure" (on how the client-server method created this same problem).

n129. Sandvine, Inc., supra n. 107, at 4.

n130. See generally id. at 4-5; Lucas, supra n. 125.

n131. See PeerApp, UltraBand Technology for Media Caching & Content Delivery Solutions, http://peerapp.com/technology/videocaching.aspx (accessed Apr. 25, 2010).

n132. Elkin-Koren, Making Tech. Visible, supra n. 80, at 19.

n133. Even if the client does realize that the file is a copy and is provided from a different source, he probably does not care about the source as long as the files are identical. ISPs use masquerading techniques to conceal this practice. To the customers and copyright holders, the whole process is hidden - they are not aware of whether the information is provided from the cache or directly from a peer. In the industry White Papers, P2P software providers note that they keep the peer connection alive even when there is no P2P transfer of data for "transparency" reasons. That is, the caching techniques are "transparent" in the sense that they are invisible. We could not think of any good reason for keeping the peer connection alive except to conceal the caching practice. For example, one P2P caching site states: "The UltraBand is a network cache, which transparently intermediates delivery of Internet content to the subscriber from Internet content sources. The deployment of the cache in ISP network doesn't affect Internet application behavior and doesn't require configuration change on the subscriber side." PeerApp, select The New Ultraband 5000 Platform http://www.peerapp.com (accessed Apr. 25, 2010). It is unclear why the software maintains this illusion. Perhaps the software designers thought the user would feel more comfortable receiving the file from another user instead of from a faceless server? Conceivably, a consumer concerned about getting caught for infringement might feel that the interference of the ISP seems like "big brother" is watching. Perhaps the software designers hoped to fool content providers themselves as to the ISPs' interference with P2P file exchanges.

n134. The following examples are extrapolated from the P2P caching descriptions in Oversi, OverCache P2P Caching & Delivery Platform, http://www.oversi.com/products/overcache-msp/overcache-p2p.html (accessed Apr. 25, 2010); European ISPs Find Solution, supra n. 1; Sandvine, Inc., supra n. 107, at 6-7. The providers of P2P caching software and hardware do not explain their techniques in exhaustive detail, but the basic structure of the system is apparent.

n135. Info. Tech. Serv. Ctr., Risks in Peer-to-Peer File Sharing, http://www.cuhk.edu.hk/itsc/about/p2p-risk.html (accessed Apr. 25, 2010); Oversi, supra n. 134.

n136. It is possible to lower bandwidth costs by caching content accessed via P2P networks. PeerApp's UltraBand and Oversi's OverCache P2P reduce the amount of overall Internet backbone bandwidth an ISP is required to support subscriber demand. PeerApp, PeerApp UltraBand 200SP, http://www.peerapp.com/App_FCK/file/UB200SPdatasheet.pdf (accessed Apr. 25, 20100); Oversi, supra n. 134 (diagram of how P2P caching avoids using the expensive connections between networks).

n137. As ISPa did in Example Three, when it provided the file at a greater speed to A3.

n138. We would like to emphasize that this feature is not necessarily installed in the current systems but technically it can be incorporated to both the ISP and P2P protocols.

n139. *A&M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1013 (9th Cir. 2001).*

n140. Id. (citing *17 U.S.C. § 106* (2006)).

n141. *Id. at 1014.*

n142. *17 U.S.C. § 106* (2006).

n143. *Napster, 239 F.3d at 1013-14.*

n144. See Elkin-Koren, Making Tech. Visible, supra n. 80, at 22.

n145. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 941 (2005); In re Aimster Copy. Litig., 334 F.3d 643, 654-55 (7th Cir. 2003); Napster, 239 F.3d at 1022, 1024.*

n146. See supra n. 2.

n147. See supra nn. 112-38 and accompanying text.

n148. *17 U.S.C. § 101* (2006).

n149. *MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993).* Numerous other courts have since endorsed this opinion. See e.g. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 717 (9th Cir. 2007).* The Second Circuit, however, recently reassessed MAI, finding that it only addressed the fixation requirement of creating a "copy" under section 101 of the Copyright Act and not the "more than transitory duration" requirement. *Cartoon Network LP, v. CSC Holdings, Inc., 536 F.3d 121, 127 (2d Cir. 2008).* In Cartoon Network, the Second Circuit found that a digital video recording system that held a digital file in its buffer for at most 1.2 seconds held it for a "transitory duration" and therefore that the file was not "fixed." *Id. at 129-30.* Under the Cartoon Network analysis, whether P2P caching creates copies, then, depends on how long the digital file is held in the cache. *Id. at 130.* This would, of course, depend on the technology. It seems likely, however, that files are held in the cache for at least 1.2 seconds because popular files, such as movies and songs, are typically popular over a period of days, if not weeks or months. To be useful, a cache would have to hold files over a period related to the surge in human demand, which does not occur on a split second time frame.

n150. *MAI, 991 F.2d at 519.*

n151. Douglas J. Masson, Fixation on Fixation: Why Imposing Old Copyright Law on New Technology Will Not Work, *71 Ind. L.J. 1049, 1056 n. 63 (1996).*

n152. Id.; Computer Hope, RAM, http://www.computerhope.com/jargon/r/ram.htm (accessed Apr. 25, 2010).

n153. *17 U.S.C. § 101* (2006).

n154. *Relig. Tech. Ctr. v. Netcom On-line Commun. Servs., Inc., 907 F. Supp. 1361, 1368-69 (N.D. Cal. 1995).*

n155. *Id. at 1369-70.* In a more recent decision, Costar Group, Inc. v. Loopnet, Inc., the Fourth Circuit agreed with the Netcom analysis holding that "automatic copying, storage and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement under§§501 and 106 of the Copyright Act." *Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 555 (4th Cir. 2004).*

n156. *Parker v. Google, Inc., 422 F. Supp. 2d 492, 495 (E.D. Pa. 2006).*

n157. Id.

n158. *Id. at 495-96.*

n159. *Id. at 497.*

n160. Id.

n161. *Parker v. Google, Inc., 2007 WL 1989660 at 3* (3d Cir. July 10, 2007) (quoting *CoStar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 550 (4th Cir. 2004)).* The same issue was dealt with differently in *Field v. Google, Inc., 412 F. Supp. 2d 1106, 1109 (D. Nev. 2006).* In Field, the court decided in Google's favor. *Id. at 1115.* This court, however, sidestepped the direct question of whether Google's caching constituted copyright infringement. Id. Instead, the court noted that the plaintiff did not allege that Google committed infringement when its robots, like an ordinary Internet user, made the initial copies of the web pages containing the plaintiff's copyrighted works and stored the copies in Google's cache. Id. The court instead focused on the end users. Id. The court ruled that "when a user requests a Web page contained in the Google cache by clicking on a "Cached' link, it is the user, not Google, who creates and downloads a copy of the cached Web page." Id. Google's role in the last practice is passive and "the automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement ... ." Id.

n162. See e.g. Nicole Bashor, The Cache Cow: Can Caching & Copyright Co-Exist?, 6 John Marshall Rev. Intell. Prop. L. 101, 112 (2006).

n163. Id. at 117.

n164. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 726-29 (9th Cir. 2007).*

n165. *Id. at 711-12* (quotations omitted).

n166. *Id. at 716.*

n167. *Id. at 716-17 n.6.* Since the Ninth Circuit's decision in Perfect 10, a district court within the Ninth Circuit has expanded on the Perfect 10 court's rejection of volition as a factor in whether caching constitutes infringement. *Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1109-10 (C.D. Cal. 2007).* In Ticketmaster, the court found that the fact that the caching was automatic not dispositive in a fair use determination. *Id. at 1109.* Rather, a finding that caching is a fair use must depend on whether the caching is " "noncommercial, transformative ... and has a minimal impact on the potential market for the original work.' " *Id. at 1109-10* (quoting *Perfect 10, 487 F.3d at 726).*

n168. *Relig. Tech. Ctr. v. Netcom On-line Commun. Servs., Inc., 907 F. Supp. 1361, 1365-68 (N.D. Cal. 1995).*

n169. See supra nn. 112-24 and accompanying text.

n170. *Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 844 (C.D. Cal. 2006).*

n171. The copyright owner has " " the right to control the first public distribution of an authorized copy ... of his work.' " *Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 552 (1985)* (quoting H.R. Rpt. 94-1476 at 5675-76 (Sept. 3, 1976)).

n172. *A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011-14 (9th Cir. 2001).* The Ninth Circuit recently acknowledged the " "deemed distribution' " approach in Perfect 10. *487 F.3d at 719.* Although the court distinguished Perfect 10 from Napster, noting that Google did not have Perfect 10's full size images on its computers and therefore could not communicate these images to Google's users (Google only had the thumbnails stored on their computer), the Ninth Circuit followed the Napster analysis. Id.

n173. *Napster, 239 F.3d at 1014.*

n174. E.g. *Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429-30 (1984).*

n175. *17 U.S.C. § 107* (2006).

n176. Id.

n177. *Campbell v. Acuff-Rose Music, 510 U.S. 569, 578-79 (1994).*

n178. *Id. at 579* (citing Pierre N. Laval, Toward a Fair Use Standard, *103 Harv. L. Rev. 1105, 1111 (1990)).*

n179. *Wall Data, Inc. v. L.A. Co. Sheriff's Dept., 447 F.3d 769, 778 (9th Cir. 2006)* (citing *Campbell, 510 U.S. at 578-79).*

n180. The copied work is often broken into many small files, but it is designed to be reconstituted as an exact copy. See The Torrent Becomes a Flood, supra n. 88, at "Divide and Conquer."

n181. *Kelly v. Arriba Soft Corp., 336 F.3d 811, 818 (9th Cir. 2003)* n182. *Id. at 819.* While the Kelly court was not prepared to extend their analysis to the photos full size images (un-reduced graphics), it seems that the Ninth Circuit was willing to take the next step in Perfect 10. See *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 721-22 (9th Cir. 2007).*

n183. *Perfect 10, 487 F.3d at 721-22* (citing *Kelly, 336 F.3d at 818-19).*

n184. Id. at 713.

n185. See e.g. *Kelly, 336 F.3d at 815* (explaining that Leslie Kelly, a professional photographer, sued Arriba Soft Corp. when he found out Arriba's search engine stored some of the copyrighted photographs from his website in their database); *Field v. Google, Inc., 412 F. Supp. 2d 1106, 1116 (D. Nev. 2006);* Parker v. Yahoo!*, Inc., 2008 WL 4410095 at 3-4* (E.D. Pa. Sept. 25, 2008); Tamber Christian, Internet Caching: Something to Think about, *67 UMKC L. Rev. 477, 487 (1998).*

n186. See *Kelly, 336 F.3d at 820.*

n187. With the exception of Kelly, where the search engine merely made a mistake. *Id. at 816.*

n188. See *Field, 412 F. Supp. 2d at 1112-14, 1115-16* (by not including a "no-archive" meta-tag in website, website owner gave search engine an implied license to cache a copy of the website).

n189. See e.g. *id. at 1115-67; Parker, 2008 WL 4410095 at 3-4.* Or perhaps because the website owner wasted the court's time with a frivolous suit.

n190. A peer could potentially object that she only wanted to share the file for a limited time - and then remove it. She might argue that she did not give permission for the file to circulate indefinitely on the Internet. However, if the peer really wanted to control the level of distribution, she could have used, or at least tried to use, some form of digital rights management. Without some effort to control distribution, it seems unlikely a court would respect a peers' withdrawal of permission to use a file. See e.g. *Field, 412 F. Supp. 2d at 1115-17; Parker, 2008 WL 4410095 at 3-5.*

n191. See *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 720-23 (9th Cir. 2007).*

n192. See *id. at 721-22; Kelly, 336 F.3d at 819.*

n193. See *Perfect 10, 487 F.3d at 721; Kelly, 336 F.3d at 820.*

n194. *Grokster, 545 U.S. at 920* ("Since file exchanges do not travel through a server, communications can take place between any computers that remain connected to the network without risk that a glitch in the server will disable the network in its entirety.").

n195. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); In re Aimster Copy. Litig., 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).*

n196. This makes the entire practice less stable. See e.g. Intl. Engr. Consortium, Comparing P2P Solutions: P2P Caching, http://www.iec.org/online/tutorials/p2p_solutions/topic04.asp (accessed Apr. 25, 2010); PeerApp, PeerApp White Paper: Why QOE Is Important to Service Providers 4-6, http://www.peerapp.com/App_FCK/file/PeerApp_QOE_White_Paper.pdf (Sept. 2008).

n197. See e.g. PeerApp, PeerApp White Paper: Why QOE Is Important to Service Providers 4-6, http://www.peerapp.com/App_FCK/file/PeerApp_QOE_White_Paper.pdf (Sept. 2008) ("PeerApp's UltraBand(R) product line uses intelligent media caching to enable service providers meet the content demands of subscribers. The solution relieves congestion at the critical problem areas, caches popular content and accelerates its delivery to subscribers providing the best possible QoE.").

n198. A potential flaw in this argument is that legitimate sources of content (e.g. iTunes) may be treated like peers as far as P2P caching is concerned. That is, P2P caching may also cache non-infringing files requested from legitimate sources like iTunes, not just files shared by peers from their PCs. Therefore, while it seems likely that most files cached in P2P caching are copyrighted, it may be that many of them are also authorized and, as a result of the copyright owners' authorization, not infringing. It appears, however, that legitimate content distributors often use different networks of distribution which may not be assisted by P2P caching. See

Matthew Lucas, Peer-to-Peer Networks: DRM & OSS/BSS, Billing & OSS World (Mar. 1, 2007) (available at http://www.billingworld.com/articles/Feature/Peer-to-Peer-Networks-DRM-and-OSS-BSS.html#) ("Enterprises have adapted P2P technology to develop private content delivery networks. For example, CacheLogic and Kontiki (recently acquired by VeriSign) use P2P technology to help enterprises distribute large files, such as software images and video training materials.").

n199. See Rajkumar Buyya, Al-Mukaddim Khan Pathan, James Broberg & Zahir Tari, A Case for Peering of Content Delivery Networks, 7 IEEE Distrib. Sys. Online 10, 12 (Oct. 2006) (available at http://www.gridbus.org/reports/CDNPeering.pdf).

n200. Id. at 1-2. CDNs utilize several strategically placed mirrored web servers in various locations, thereby enabling a user to communicate and retrieve files from a server close to them. Id.

n201. See iTunes Store: "Terms & Conditions," http://www.apple.com/legal/itunes/us/terms.html#SERVICE (last updated Oct. 29, 2009); iTunes Store Terms & Conditions, http://www/apple.com.legal/itunes/ww/ (Apr. 25, 2010).

n202. Akamai, Press Release, Apple & Akamai Reveal Apple Invest. to Cement Strategic Agreement (Aug. 18, 1999) (available at http://www.akamai.com/html/about/press/releases/1999/press_081899c.html).

n203. In fact, Apple, Inc. uses the services of Akamai, Inc. for this type of service. Id.; Peter Burrows, Why BitGravity Attracted Tata, Business Week Online, http://www.businessweek.com/print/technology/content/sep2008/tc2008098_785702.htm (Sept. 9, 2008). Other content delivery networks focus on finding the most efficient path, rather than the shortest distance; either way the point is to reduce bandwith usage.

n204. See RIAA, Press Release, RIAA Continues Enforcement of Rights with New Lawsuits against 784 File Sharers (June 29, 2005) (available at http://www.riaa.com/newsitem.php?news_month_filter=6&news_year_filter=2005&resultpage=&id=8B83713E-4BD3-F311-29I

n205. Pursuant to the DMCA, content owners serve subpoenas to ISPs to determine the identity of peers who distribute infringing files. See *17 U.S.C. § 512*(h)(1) (2006). Content owners then prosecute those individuals. See *RIAA, supra n. 204.*

n206. Especially when there is no legitimate market, such as, for example, pre-released movies. See Digital Watermarking Alliance, White Paper, http://digitalwatermarkingalliance.org/docs/papers/dwa_whitepaper_p2p.pdf (accessed Apr. 25, 2010).

n207. See e.g. Greg Sandoval, Copy of RIAA's New Enforcement Notice to ISPs, http://news.cnet.com/8301-1023_3-10127050-93.html (Dec. 19, 2008).

n208. PeerApp, PeerApp White Paper: Accelerating the Video Internet 3-4, http://www.peerapp.com/App_FCK/file/Accelerating the Video Internet PeerApp October 2009.pdf (Oct. 2009).

n209. See e.g. *Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 578-79, 584-85 (1994)* (citing *Sony Corp. of Am. V. Universal City Studios, Inc., 464 U.S. 417, 448-49, 449 n. 32, 455 n. 40 (1984)).*

n210. See id. at 579, 583-84 ("The more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use.").

n211. See id.

n212. And indeed this is how the caching software companies advertise themselves. For example, one caching company states:

P2P Caching is the only solution that enables ISPs to fully and affordably embrace P2P on their networks. Instead of growing bandwidth to meet increasing demand or limiting P2P usage through policies or traffic shaping, P2P caching lets ISPs simultaneously serve the needs of P2P and non-P2P users without negatively impacting either audience. In fact, P2P caching provides an improved experience for all subscribers - P2P users whose file sharing is improved through using the cache, and non-P2P users who experience better performance from networks uncongested from P2P traffic.

Intl. Engr. Consortium, supra n. 196.

n213. See *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 722-23 (9th Cir. 2007); Field v. Google, Inc., 412 F. Supp. 2d 1106, 1119-20 (D. Nev. 2006).*

n214. *Perfect 10, 487 F.3d at 722-23; Field, 412 F. Supp. 2d at 1118-20.*

n215. *Perfect 10, 487 F.3d at 722-23; Field, 412 F. Supp. 2d at 1120.*

n216. As the court stated in Field, "while Google is a for-profit corporation, there is no evidence Google profited in any way by the use of any of Field's works... . The fact that Google is a commercial operation is of only minor relevance in the fair use analysis. The transformative purpose of Google's use is considerably more important ... ." *412 F. Supp. 2d at 1120.*

n217. Thus, in Perfect 10, the court held that "the transformative nature of Google's use is more significant than any incidental superseding use or the minor commercial aspects of Google's search engine and website." *487 F.3d at 723.*

n218. See *Infinity Broad. Corp. v. Kirkwood, 150 F.3d 104, 108-09 (2d Cir. 1998); Worldwide Church of God v. Phila. Church of God, 227 F.3d 1110, 1117-18 (9th Cir. 2000).*

n219. *Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994); Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 496-97 (1984)* (Blackmun, Marshall, Powell and Rehnquist, JJ., dissenting); *Worldwide Church of God, 227 F.3d at 1118.*

n220. *Campbell, 510 U.S. at 586.*

n221. See e.g. *Zomba Enters., Inc. v. Panorama Recs., Inc., 491 F.3d 574, 583 (6th Cir. 2007)* (citing *Campbell, 510 U.S. at 586).*

n222. *Dr. Seuss Enters., L.P. v. Penguin Bks. USA, Inc., 109 F.3d 1394, 1402 (9th Cir. 1997).*

n223. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 723 (9th Cir. 2007); Kelly v. Arriba Soft Corp., 336 F.3d 811, 820 (9th Cir. 2003); Field v. Google, Inc., 412 F. Supp. 2d 1106, 1120 (D. Nev. 2006).*

n224. *Perfect 10, 487 F.3d at 723; Kelly, 336 F.3d at 820; Field, 412 F. Supp. 2d at 1120.*

n225. *Kelly, 336 F.3d at 820* (citing *Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 564 (1985)).*

n226. *Perfect 10, 487 F.3d at 723* ("An author exercises and exhausts this one-time right by publishing the work in any medium.").

n227. See id.

n228. *Perfect 10, 487 F.3d at 723.*

n229. The argument is not helpful, of course, if the files being shared have not yet been published (e.g. pre-screened movies, pre-published books, music, etc.). See e.g. Farhad Manjoo, The Potter Leak: Winners & Losers (No Spoilers), http://www.salon.com/tech/machinist/blog/2007/07/18/potter_leak/index.html (July 18, 2007).

n230. *Perfect 10, 487 F.3d at 723-24; Kelly, 336 F.3d at 820; Field v. Google, Inc., 412 F. Supp. 2d 1106, 1120 (D. Nev. 2006).*

n231. E.g. *Field, 412 F. Supp. 2d at 1120.*

n232. *Kelly, 336 F.3d at 820-21* (citing *Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586-87 (1994); Worldwide Church of God v. Phila. Church of God, 227 F.3d 1110, 1117-18 (9th Cir. 2000)).*

n233. *Campbell, 510 U.S. at 586-88; Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 449-50 (1984).*

n234. *Sony, 464 U.S. at 449-50.* As the court stated in Field, "even copying of entire works should not weigh against a fair use finding where the new use serves a different function from the original, and the original work can be viewed by anyone free of charge." *412 F. Supp. 2d at 1120.*

n235. E.g. *Field, 412 F. Supp. 2d at 1120.*

n236. *Parker v. Google, Inc., 422 F. Supp. 2d 492, 502 (E.D. Pa. 2006).*

n237. See *Field, 412 F. Supp. 2d at 1112-13.*

n238. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 713 (9th Cir. 2007).* Perfect 10 operated a subscription service for the images of its naked models, but users illegally copied some images and made them available to the public on the Internet. See id.

n239. *Id. at 724* (quoting *Kelly v. Arriba Soft. Corp., 336 F.3d 811, 821 (9th Cir. 2003)).*

n240. *17 U.S.C. § 107* (2006).

n241. See Stuart Kemp, New Suits Target P2P File-sharers, 396 Hollywood Rep. (Oct. 18, 2006).

n242. Bill Holland, Artists' Groups Criticize P2P Study, 116 Billboard (Dec. 18, 2004).

n243. *Field v. Google, Inc., 412 F. Supp. 2d 1106, 1116 (D. Nev. 2006).*

n244. *Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 592 (1994).*

n245. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1016 (9th Cir. 2001)* (quoting *A&M Recs., Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 913 (N.D. Cal. 2000)).*

n246. Id. (citing Memo. & Or. Re Admissibility Expert Rpts. 2-3 (Aug. 10, 2000)).

n247. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 912, 923-26 (2005); In re Aimster Copy. Litig., 334 F.3d 643, 645-46 (7th Cir. 2003); Napster, 239 F.3d at 1020.*

n248. *Grokster, 545 U.S. at 929-30* (citing *Gershwin Publg. Corp. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); Shapiro, Bernstein & Co., Inc. v. H.L. Green Co., Inc., 316 F.2d 304, 307 (2d Cir. 1963)).*

n249. *Grokster, 545 U.S. at 929-30; Shapiro, 316 F.2d at 307.*

n250. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 731 (9th Cir. 2007).*

n251. The DMCA protects ISPs from secondary liability if they qualify for the safe harbors set forth in subsections (a) through (d) of Section 512. *17 U.S.C. § 512* (2006). This section "protects qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement." Sen. Rpt. No. 105-190 at 20 (May 11, 1998). We will address the application of the DMCA to caching ISPs in the next section. For this section, we assume that caching ISPs are not protected by the DMCA from secondary liability.

n252. *Gershwin, 443 F.2d at 1162.*

n253. See *Relig. Tech. Ctr. v. Netcom On-line Commun. Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).*

n254. We should distinguish here between Examples One through Three of P2P caching and Examples Five and Six. The analysis of material contribution in Netcom clearly applies to Examples Five and Six. See id. In those examples, the peers who originally held the file deleted it. The only copy remains in the ISP's server cache. When a user requests the file using P2P software, she would not receive the file at all if not for P2P caching. In contrast, in Examples One through Three, copies exist on other peers' computers and in the ISP's cache. Accordingly, a user can receive the file from other peers without the benefit of P2P caching.

n255. *Netcom, 907 F. Supp. at 1373* (quoting *Gershwin, 443 F.2d at 1162).*

n256. For example, in Netcom, the court found that plaintiff's notice to defendants that one of Netcom's clients had posted an infringing document on defendant's posting service, was enough to raise a question of fact as to defendant's knowledge. *907 F. Supp. at 1374-75.*

n257. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 933-34 (2005)* (citing *Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 439-40 (1984)).*

n258. *Sony, 464 U.S. at 442.*

n259. Id.

n260. *Grokster, 545 U.S. at 933-35.*

n261. *Id. at 934-37.*

n262. *Id. at 939-40.*

n263. *Id. at 924-26.*

n264. *Id. at 940.*

n265. *Id. at 937.*

n266. Id.

n267. *Id. at 936-37.*

n268. See PeerApp, UltraBand Technology for Media Caching & Content Delivery Solutions, http://peerapp.com/technology/videocaching.aspx (accessed Apr. 25, 2010). Here, however, PeerApp seems to be advertising its caching software to ISPs, not to the end user. It seems a stretch to find PeerApp guilty of inducing infringement by consumers.

n269. Such a warning might then subject the ISP to vicarious liability because the warning could be construed as indicating the ISP's right and ability to control infringing use. See *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).*

n270. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 727 (9th Cir. 2007)* (citing *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005)* (citing *Shapiro, Bernstein & Co., Inc. v. H.L. Green Co., Inc., 316 F.2d 304, 307 (2d Cir. 1963))).*

n271. Id.

n272. *Perfect 10, 487 F.3d at 728* (citing *Napster, 239 F.3d at 1022).*

n273. Id. at 729 (citations omitted, emphasis in original) (citing *Napster, 239 F.3d at 1022; Relig. Tech. Ctr. v. Netcom On-line Commun. Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)).*

n274. *Zeran v. America Online, Inc., 129 F.3d 327, 330-31 (4th Cir. 1997)* (noting that Congress created a tort immunity for Internet service providers in the Communications Decency Act of 1996, *47 U.S.C. § 230* (2006), because "it would be impossible for service providers to screen each of their millions of postings for possible problems"); *Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 962 n.7 (C.D. Cal. 1997)* ("Even though Internet service providers directly provide the storage and communications facilities for Internet communication, they cannot be held liable merely for failing to monitor the information posted on their computers for tortious content.").

n275. *Perfect 10, 487 F.3d at 731* (quoting *Perfect 10 v. Google, Inc., 416 F.2d 828, 858 (C.D. Cal. 2006)).*

n276. See *In re Aimster Copy. Litig., 334 F.3d 643, 653 (7th Cir. 2003)* ("Even when there are noninfringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.").

n277. Digital fingerprinting, digital watermarking, identifying "hash" marks, and maintaining lists of Internet sites which distribute massive numbers of infringing files are all only partially successful. See Lucas, supra n. 198, for discussion of technical solutions to infringement on P2P networks. Moreover, these techniques also run the danger of over-enforcement, which has the deleterious effect of chilling speech. Yen, supra n. 14, at 1871-72.

n278. See Lucas, supra n. 198. One fairly simple solution for P2P users is to encrypt the files they share. At the minimum, encryption programs would slow down ISPs' efforts to identify the nature of the file.

n279. The situation is different if the ISP receives notification of a specific case of infringement. In that case, the ISP can easily delete the copyrighted file from its computers. If it does not, it is most likely liable and will also lose its protection under the DMCA safe harbor provisions. *17 U.S.C. § 512*(b)(2)(E) (2006).

n280. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 933-34 (2005)* (citing *Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984)); In re Aimster Copy. Litig., 334 F.3d 643, 648-49 (7th Cir. 2003).*

n281. See *Sony, 464 U.S. at 442*. Justice Breyer stated in Grokster:

To be sure, in quantitative terms these uses account for only a small percentage of the total number of uses of Grokster's product. But the same was true in Sony, which characterized the relatively limited authorized copying market as "substantial" ...

Importantly, Sony also used the word "capable," asking whether the product is "capable of" substantial noninfringing uses. Its language and analysis suggest that a figure like 10%, if fixed for all time, might well prove insufficient, but that such a figure serves as an adequate foundation where there is a reasonable prospect of expanded legitimate uses over time... . And its language also indicates the appropriateness of looking to potential future uses of the product to determine its "capability."

545 U.S. at 953-54 (Breyer, J., concurring) (citations omitted).

n282. See *Sony, 464 U.S. at 442* ("In order to resolve this case we need not give precise content to the question of how much use is commercially significant.").

n283. *Grokster, 545 U.S. at 953-54* (Breyer, J., concurring).

n284. *Sony, 464 U.S. at 493.*

n285. *In re Aimster Copy. Litig., 334 F.3d 643, 653 (7th Cir. 2003).*

n286. This is similar to the negligence standard in the law of Torts. For a discussion of the benefits and costs of such a regime, see Richard Posner, Economic Analysis of Law 163-67 (4th ed. Little Brown 1992).

n287. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001)* (citing *Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996)* (quoting *Gershwin Publg. Corp. v. Columbia Artists Mgt., 443 F.2d 1159, 1162 (2d Cir. 1971))).*

n288. Yen, supra n. 14, at 1843-44; see e.g. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 732-33 (9th Cir. 2007);* see *Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004).*

n289. See *Ellison, 357 F.3d at 1078-79; Fonovisa, 76 F.3d at 263.*

n290. *Fonovisa, 76 F.3d at 262-63.*

n291. *Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173-74 (C.D. Cal. 2002).* The court also found that the defendant had the right and ability to control infringement because it could control customer access through passwords. *Id. at 1157, 1161, 1173.*

n292. See *Fonovisa, 76 F.3d at 263-64.*

n293. Id. In Fonovisa, the court found the benefit requirement was met because the availability of infringing music at the swap meet attracted more customers. Id. The defendant profited because more customers paid for concessions, entrance fees, and parking fees. *Id. at 263.*

n294. *A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001)* (citing *Fonovisa, 76 F.3d at 263-64).*

n295. Id.

n296. The first in this line of cases is *Shapiro, Bernstein & Co., Inc. v. H.L. Green Co. Inc., 316 F.2d 304, 306-08 (2d Cir. 1963)* (the Second Circuit found the right and ability to control because the defendant controlled most aspects of the direct infringer's business, a store which sold music records. The defendant controlled the conduct of employees, their payment, and the handling of revenue).

n297. *Banff Ltd. v. Limited, Inc., 869 F. Supp. 1103, 1109 (S.D.N.Y. 1994).*

n298. *Relig. Tech. Ctr. v. Netcom On-line Commun. Servs., Inc., 907 F. Supp. 1361, 1375-76 (N.D. Cal. 1995).*

n299. Id.

n300. *Napster, 239 F.3d at 1023-24.*

n301. *Id. at 1024.*

n302. Id.

n303. See *id. at 1024; Netcom, 907 F. Supp. at 1375-76.*

n304. See *Napster, 239 F.3d at 1024; Netcom, 907 F. Supp. at 1375-76.*

n305. *Shapiro, Bernstein & Co., Inc. v. H.L. Green Co., Inc., 316 F.2d 304, 307 (2d Cir. 1963); Netcom, 907 F. Supp. at 1376-77; Artists Music, Inc. v. Reed Publg. (USA), Inc., 1994 WL 191643 at 6* (S.D.N.Y. May 17, 1994).

n306. *Netcom, 907 F. Supp. at 1376-77.*

n307. Melville B. Nimmer & David Nimmer, Nimmer on Copyright vol. 3, § 12B.01[A][1] (Lexis 2009).

n308. Yen, supra n. 14, at 1837; see e.g. *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 729-31 (9th Cir. 2007)* (holding that the plaintiff did not establish the elements necessary to prove vicarious liability against defendant Google); *Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004).*

n309. See e.g. *Napster, 239 F.3d at 1024* (supporting vicarious liability claim against Napster); *Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002)* (finding "a strong likelihood of success on Perfect 10's claims for vicarious copyright infringement liability.").

n310. "We have held that the limitations on liability contained in *17 U.S.C. § 512* protect secondary infringers as well as direct infringers." *Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 732 (9th Cir. 2007)* (citing *Napster, 239 F.3d at 1025).*

n311. *17 U.S.C. § 512*(b) (2006).

n312. Id. at § 512(b)(2).

n313. See id. at § 512(b).

n314. See id. at § 512(b)(1).

n315. Id.

n316. Id. at § 512(b)(2)(A).

n317. Id. at § 512 (b)(2)(B). An ISP must only comply with these requirements so long as they are in accordance with accepted industry standards and are not used to prevent or unreasonably impair the caching process. Id. The purpose of such requirements is to accurately represent the nature of the site in a given moment. An active site (such as a news website) must be updated at a much higher rate than a static site (such as an online dictionary).

n318. See id. at § 512(b)(2)(C)(i).

n319. See id. at § 512(b)(2)(C).

n320. See id. at § 512(b)(2)(D).

n321. See id. The ISP should grant access "to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions." Id.

n322. Id. at § 512(b)(2)(E).

n323. Id. The service provider should not remove or disable access to the material unless that material has been removed from the originating site and the party giving the notification includes in the notification a statement confirming that the material has been removed. See id.

n324. *Recording Indus. Assn. of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1233-38 (D.C. Cir. 2003).*

n325. *Id. at 1238* (citing *In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 38 (D.C. Cir. 2003)).*

n326. Id.

n327. Id.

n328. "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." *Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).*

n329. *RIAA, 351 F.3d at 1238.* The Eighth Circuit endorsed this approach in In re Charter Communs., Inc., Subpoena Enforcement Matter, ruling that "it is the province of Congress, not the courts, to decide whether to rewrite the DMCA "in order to make it fit a new and unforeseen Internet architecture' and "accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.' " *393 F.3d 771, 777 (8th Cir. 2005)* (quoting *RIAA, 351 F.3d at 1238).*

n330. *17 U.S.C. § 512*(h) (2006); *RIAA, 351 F.3d at 1238.*

n331. *17 U.S.C. § 512*(b).

n332. The fundamental difference is that the P2P file is the end good which the user seeks. In contrast, a web user is often looking for an item which she knows she can get from a given distributor. The website is often the means to finding this end good (The "end good" may be available on the actual website, such as news provided on the New York Times website, or it may be a product that the user thinks she can order from Amazon.com, J. Crew, or Target, to name a few merchandisers with websites). Thus, the web user looks for the distributor and then the end good, whereas the P2P user requests the end good directly.

n333. Distributors have at least commissioned and paid the designers, writers, or other creators to create their website. Of course, some website owners put material they did not create online, just as some P2P distributors make files available online that they did create.

n334. *17 U.S.C. § 512*(b)(2)(A).

n335. Id. at § 512(b)(2)(B).

n336. Id. at § 512(b)(2)(C).

n337. Id. at § 512(b)(2)(E)(i).

n338. Id. at § 512(b)(2)(E)(ii).

n339. *Recording Indus. Assn. of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003).*

n340. "Each safe harbor applies to a particular ISP function... . The second safe harbor, under § 512(b), protects ISPs for "system caching,' that is, instances when they provide intermediate and temporary storage of material on a system or network under certain conditions." *In re Charter Communs., Inc., 393 F.3d 771, 775 (8th Cir. 2005).*

n341. *Id. at 773-74* (citing H. Rpt. 105-551 § 2 at 23 (July 22, 1998)). As stated by the court:

The DMCA has been the principal legislative response to such activities; it was enacted, however, in 1998, prior to the emergence of P2P systems. The DMCA is designed to advance "two important priorities: promoting the continued growth and development of electronic commerce[] and protecting intellectual property rights.' Title II of the DMCA was the product of lengthy negotiations between copyright owners and Internet service providers. It was designed to strike a balance between the interests of ISPs in avoiding liability for infringing use of their services and the interest of copyright owners in protecting their intellectual property and minimizing online piracy.