8/17/2001

HACKING DIGITAL VIDEO RECORDERS: POTENTIAL COPYRIGHT LIABILITY FOR DVR HACKERS AND SERVICE PROVIDERS

To what extent does Sony's *time-shifting fair use argument extend to recent innovations that make it easier for hackers use DVR technology to generate copies of protected material? The author assesses the potential liability of DVR manufacturers against the backdrop of traditional fair use doctrines.*

I. Introduction

¶ 1 In the Age of the Digital Millennium, technological innovations continue to "revolutionize" the way we interact with the world around us. Many of these "revolutions" have been based in the entertainment industry, altering the behavior, demands, and expectations of consumers and society at large. Developments in consumer electronics and digital technologies have increased the accessibility of content such as music and videos, while allowing for virtually instantaneous copying with negligible costs to the copier.

¶ 2 Less publicized in the societal conscience than the Napster controversy, struggles between meeting the consumer demand of personalization and preserving the rights of copyright owners are also occurring in the television industry. Controversy over technological developments and their interaction with copyright laws is not a new battle for this industry. Such a battle once raged over the advent of a device then known as video cassette recorders (VCRs). Now, a new video recording technology that has recently been released, Digital Video Recorders (DVRs)[1] is speculated to revolutionize the way consumers view television. This technology, just like its VCR predecessor, has sparked controversy over the copyright implications of its use.

II. Digital Video Recorders

DVRs in General

¶ 3 There have been three main players in the DVR market to date: ReplayTV, TiVo, and most recently UltimateTV.[2] DVRs are basically mini-PCs that allow a user to record TV broadcasts, cable, or DirectTV transmissions, depending on the model, in digital form on a hard drive located inside the recorder. Providers of DVR service require a monthly subscription fee.

This allows for the device to access the companies' server, which regularly downloads program guides into the device via a modem. Thus, DVRs provide the same recording and time-shifting functions as a VCR, just in a different medium.

Hacking the DVR

¶ 4 DVRs also have another unintended feature: hackability. Computer hackers have long loved the challenge of reverse engineering and customizing computer hardware and software. DVRs are just another computer system with which they can play. Because UltimateTV is so new to the market and utilizes proprietary software of Microsoft, it's hackability is yet unknown. However, hacking of ReplayTV and TiVo is well documented. While ReplayTV's operating system is proprietary and thus more difficult to hack, TiVo uses the open-source Linux operating system and standard "off the shelf" IDE hard drives. However, the format for storing video files is proprietary.[3] Hackers of ReplayTV and TiVo have added extra hard drives to the devices, allowing for more storage space for recorded programming. Some have also customized format of the user interface and menus to suit their personal needs.

¶ 5 On one hand, hackers have been a blessing to DVR companies, developing an extremely loyal customer base when the product was relatively unknown to the population at large. Hackers regularly share their praise for the products and results of their hacking with each other at websites and chat rooms on the Internet[4] On the other hand, the DVR companies soon may become wary of the potential results of such hacking exercises.[5] Producers of DVRs do not endorse officially hacking activities, do not offer technical support for hacks, and make it clear that any hacking voids the warranty of the unit. Therefore, hacking has been limited to a small number of technophiles, estimated from a handful up to 1,000, who are willing to take such risks and have the skills to execute such hacks.[6] The posted hacking FAQs are highly technical and a typical non-skilled DVR user does not have the capability to decipher posts or engage in such hacking. Any effort by such user will most likely result in a $600 paperweight.

¶ 6 At the recent CEA Digital Download Conference in March, 2001, TiVo's General Counsel and Chief Privacy Office Matthew Zinn participated in a panel discussing the "delicate balancing act that technology creates when attempting to align the needs of the copyright owner while allowing consumers access to digital content."[7] This notion has the potential to become particularly important to TiVo due to two new hacks growing in popularity. First is the addition of an Ethernet port to the TiVo. As purchased by the consumer, the TiVo unit accesses programming guides from the TiVo server through a modem in the unit. This modem has

Ethernet capabilities, but lacks an adapter to which an Ethernet card can be attached. Hackers have now built an adapter to which they can connect a standard ISA Ethernet card.[8] Also, at least one ReplayTV hacker has claimed to connect a DVR to a PC to access programming information through a cable modem.[9] Second is the more recent release of ExactStream program and source code, which allows for the extraction of video from the TiVo.[10] The release of ExactStream is highly controversial among hackers, some fearing this will jeopardize their relationship with TiVo.[11]

¶ 7 Depending on the uses to which these hacks are put, they may have the potential to affect content security and violate copyright laws. Hacker postings on the Internet claim the Ethernet adaptation will be used largely to access the program guides from the TiVo server, which is much faster on an Ethernet connection than a modem.[12] Another capability includes distributing compressed video within home networks for private use. The hacker writing and distributing the ExtractStream program also stresses that "the code be used only in a legal manner."[13]

¶ 8 While content providers such as studios and broadcasters are not worried about such copying for personal use, which is fair use under *Sony* as discussed later in this iBrief, they are concerned that digital copies of the programming may now be retransmitted without authorization on the Internet. TiVo CEO Mike Ramsay claims, "It's one thing to record what you see onto the TiVo drive, but the format on that drive and how you get access to that drive is totally proprietary to us. It would be very difficult for somebody to actually hack into that."[14] However, with the release of ExtractStream, this may become a reality. Prior to this time, the hacking community had declined to release such information, in order not to jeopardize its relationship with TiVo.[15] Section IV will examine the potential liabilities of the DVR companies if hackers should extract the video files and make digital copies of programming available on websites for downloading by the general public.

III. Fair Use and Time-Shifting Under *Sony*

¶ 9 In *Sony Corp. of Am. v. Universal Studios, Inc.*, the issue before the Supreme Court was whether the sale of copying equipment (VCRs) violated rights conferred by the Copyright Act on the copyright owners of broadcasted TV programming.[16] To prevail, the owners of the copyrighted programs had the burden of proving that VCR users directly infringed their copyrights, and that by selling the VCRs to consumers, Sony was liable for contributory infringement.[17] The Court focused on the private home recording of TV broadcasts for later

viewing, holding that such "time-shifting" of copyrighted programs was fair use under §107.[18] Despite the fact that entire works were copied, the Court found that the private non-commercial viewing did not harm the market for the copyrighted work.[19] "The timeshifter no more steals the program by watching it once than does the live viewer."[20] The district court even suggested that VCRs might increase the number of people who view the copyrighted broadcasts, thus helping the market.[21]

¶ 10 The Court was also not willing to impose contributory infringement on Sony because of the VCR's substantial non-infringing uses and the limited involvement of Sony with the user after the point of sale. First, VCRs could be used to make authorized copies of sporting events, religious, and educational programming.[22] The Court agreed with the district court that "an injunction which seeks to deprive the public of the very tool or article of commerce capable of some non-infringing use would be an extremely harsh remedy, as well as one unprecedented in copyright law."[23] Second, after the point of sale, Sony did not have an ongoing relationship with the VCR users and was in no position to control or have actual knowledge of their use of the VCR.[24] The Court found that Sony did not induce VCR users to make infringing copies. Moreover, there was no precedent in copyright law to impose contributory infringement on those who sell equipment with merely constructive knowledge that it may be used to make unauthorized copies.[25]

IV. Application of Copyright Law to DVR Use and Service

¶ 11 The typical user of a DVR uses the device for time shifting, whether she records broadcasted programming to view later or pauses live TV. The mere fact that the recording is now in digital form instead of on a tape does not change the nature of the use. Thus, under *Sony*, private non-commercial home viewing of DVR recordings is fair use. Neither the consumer nor a DVR company is liable for any copyright violations. However, potential copyright infringement may result from making extracted video available to the public through the addition of an Ethernet connection and the use of programs such as ExtractStream.

Direct Infringement

¶ 12 First, it is possible that a hacker may connect the DVR to her own home network to view recorded programs as streaming video. By viewing the program on another computer, numerous "copies" are created automatically in the transmission path as it is streamed to the computer.[26] The copy viewed on the computer is a work of authorship as defined by the Copyright Act because it is sufficiently fixed so that it can be perceived or reproduced with the

aid of the computer.[27] However, these copies are also viewed for time-shifting purposes and are private and non-commercial if the network is secure and only accessible to the user in her home. Thus, this is likely fair use under *Sony*. Since there is no direct infringement in these cases, DVR makers cannot be held liable for contributory infringement.

¶ 13 Once a hacker is able to transfer recorded programs from a DVR and makes them available for download on a website, she has moved out from under *Sony's* fair use umbrella. The District Court in *Sony* did not consider the issues of copying cable or satellite programming, using recordings for public performances, and transferring recordings to other people, and the Supreme Court did not address those issues.[28] These uses go beyond private non-commercial time shifting. The hacker may be liable for violating the copyright owners' exclusive right to reproduction, distribution, and public display.[29] Recent cases have addressed such actions in the Internet context.

¶ 14 In *Twentieth Century Fox Film Corp. v. iCraveTV*, iCraveTV captured broadcasted TV into digital form and made it available as streaming video on a website.[30] The court issued a preliminary injunction, holding that the plaintiff would likely succeed in showing that the defendant's transmission of the programming to the public through streaming technology on the Internet violated the copyright owners' exclusive right of public performance.[31] The court also held that iCraveTV engaged in contributory infringement by putting programming on the Internet, with knowledge that third parties would further transmit the copyrighted programs, thus materially contributing to further violation of the right of public performance.[32] The court also held that the owners of the copyrights in the TV programs would suffer an irreparable harm without the injunction: "they have lost the ability to offer particular outlets exclusive rights in particular programs or series, and they have suffered a loss of customer good will."[33]

¶ 15 In *UMG Recordings, Inc. v. MP3.com, Inc.*, MP3.com purchased copyrighted CDs, copied them into digital files and made them available to the public on a website.[34] The court held this was a prima facie case of infringement and rejected MP3.com's fair use defense.[35] It concluded the use of the copies was commercial and "space shifting" was not transformative in nature.[36] Under *Infinity Broadcast Corp. v. Kirkwood*, copies do not qualify as transformative merely because they are retransmitted in a new medium.[37] Also, the works that fell in the core of intended copyright protections were being copied in their entirety.[38] Most importantly, the court said MP3.com's free service harmed any potential market the plaintiffs may want to create by licensing recordings for such use in a way that would protect their interests.[39] The court also rejected MP3.com's argument that it should be allowed as a useful service, stating this argument

"amounts to nothing more than a bald claim that defendant should be able to misappropriate plaintiffs' property simply because there is a consumer demand for it. This hardly appeals to the conscience of equity."[40]

¶ 16 Another recent case yet to be decided is *Metro-Goldwyn-Mayer Studios, Inc. v. RecordTV.com.*[41] RecordTV operated a website where users could select broadcasted and cable TV programs to be recorded, and view the programs later on their computers as streaming video. RecordTV copied these programs into digital form from its cable TV provider. David Simon, operator of RecordTV, claimed, "I wasn't offering anything they couldn't do with their own VCR."[42] The complaint against RecordTV alleges that it was

> doing nothing more innovative than using modern computer technology to make bootlegged copies and offer unauthorized public performances and public displays of Plaintiffs' works on an advertiser-supported web site. [The Defendants] have taken what is not theirs, duplicated it, and distributed it for their own commercial gain to millions of Internet users around the world.[43]

¶ 17 In its answer and counterclaim, RecordTV claims that the recordings were not unauthorized, but "made at the direction of Internet users [and] were legitimate extensions of legal rights in directions made available by new technology."[44] The answer claims an affirmative defense of fair use, but does not explain fully how it falls under this defense. It does state that users were required to have pre-existing rights to view the programs to be able to record them for later viewing.[45] It also claims that transmitting recorded programs to a user is not a public performance.[46] However, *Columbia Pictures Industries, Inc. v. Redd Horne, Inc.* held that the transmission of a performance to members of the public even in private areas constitutes a public performance.[47] Also, the House Report accompanying the 1976 revisions to the Copyright Act determined that in the case of a cable subscription, even though individuals view the broadcast privately at home, cable TV transmissions create a public performance because it is disseminated to the public.[48]

¶ 18 In light of these recent cases, if a hacker uses a DVR with Ethernet connection and video extraction program to make copyrighted programming available for viewing on the Internet, she will be liable for direct infringement. Such a service would be exactly like those offered by iCraveTV.com, MP3.com, and RecordTV.com. The second and third fair use factors are dismissed easily, because TV programs fall under the core of what the Copyright Act is meant to protect, and they would be copied in full. Whether the hacker profits or not, the use of

the material is not transformative under *Infinity* and *MP3*, as required by the first factor. Most importantly, under the fourth factor, such actions could harm the market for the copyrighted programs. Just like in *iCraveTV*, the rebroadcast of programming robs the copyright owners of the ability to grant exclusive licenses to networks for transmission of their programs. Also, this hinders the development of any derivative "TV over the Internet" market that the copyright owners may legitimately want to develop, in terms that will protect their own rights. Such access to programs may also harm the current cable and satellite TV markets. If users were able to access cable or satellite programming for free over the Internet, then there would be no need to subscribe and pay for such services.

Contributory Infringement

¶ 19 While DVR companies[49] are not directly liable for copyright infringement, they may be liable for the hackers' actions in this scenario under the doctrine of contributory infringement. To be liable for contributory infringement (i) there must be direct infringement by the hacker, (ii) the DVR maker must induce, cause or materially contribute to the infringing activity, and (iii) the DVR maker must know or have reason to know of the infringing activity.[50] Previous analysis covers the first element. Thus, the question remains whether the DVR companies' actions meet the second two elements.

- Material Contribution

¶ 20 Most of the contributory infringement cases dealing with downloading and streaming of copyrighted content on the Internet have examined whether third parties such as Internet Service Providers (ISPs), Bulletin Board Systems (BBSs), and website operators can be liable for content put on their systems by direct infringers. However, such service providers now have a safe harbor if they meet the statutory requirements of §512. The DVR companies are different in this scenario because they are not providing networks, servers, or sites on the Internet, to be used by hackers in uploading the programs recorded on their DVRs for others to access. Therefore, to be liable, their continuing interaction with hacking and infringing subscribers must somehow "materially contribute" to the infringing activity. In *Fonovisa, Inc. v. Cherry Auction, Inc.*, operators of a swap meet were held to have materially contributed to the infringing acts of vendors at the swap meet who were selling pirated music recordings by providing services such as the provision of parking space, advertising and utilities.[51] The Ninth Circuit concluded that such services were instrumental in creating the environment necessary to engage in infringement.[52]

¶ 21 DVR companies' services are probably not enough to rise to the level of material contribution. Even though the companies are actively involved with their subscribers on a daily basis, through the uploading of program guides, the companies do not "encourage or assist" the infringement.[53] DVRs are similar to Napster in that both provide software that enables users to make digital copies of copyrighted content on their own hard drives. However, Napster also maintains its own servers that allow users to see directories of files, leading them to the files they want to copy. "Napster provides the site and facilities for direct infringement."[54] DVRs do not provide such a directory or site. DVR software stores the programming in proprietary or encrypted space on the hard drive. When DVRs dial into the companies' servers, they are merely accessing program schedules, providing no way for users to know what programs are stored on other users' DVRs.[55]

¶ 22 Moreover, hackers could post copyrighted TV programs on the Internet without having a subscription to a DVR service. The DVR itself can still be used just like a VCR to record files by manually recording at the time of a show, instead of programming the unit in advance. The subscription merely provides a user-friendlier interface with program scheduling.[56] The hacker could still use the Ethernet adaptor to access the Internet without the scheduling information, and post content on a website using the video extraction program and her own ISP.

¶ 23 DVR opponents argue that DVR companies materially contribute by not speaking out against hacking, thus indirectly promoting infringing activities. This is especially the case for TiVo, which maintains a direct link from its website to the TiVo Community chat site maintained by AV Science Forum. This site has a forum named "TiVo Underground," which is devoted entirely to posting information on how to hack TiVos. Theoretically, if hackers post copyrighted programs extracted from their units on this website, it could amount to material contribution. However, disclaimers on the AVS Forum site have recently countered this argument: "Please take note that this site is not operated by TiVo, Inc."[57] Also, the thread with the original post for ExactStream was removed and replaced with a notice: "Due to the issues that this post has raised, this thread has been removed until further notice if not totally. AVS Forum/TiVo Community in no way had any input in this matter and had NO association to this tool or it's makers. We wish for this topic to be 100% dead on this site from this point forward."[58] TiVo could also cancel a hacker's subscription to the company's services.

- Knowledge

¶ 24 Whether the element of knowledge is met will probably depend on the locale of the copied programs. If the programs are posted on a website affiliated with or well known by the DVR company, then the company may have actual knowledge of infringing activity. Otherwise, it would be hard for the companies to have actual knowledge of such sites unless specifically notified of the location, considering the vast structure of the web. The companies probably would have constructive knowledge that hackers were engaging in infringing activity due to the proliferation of hacking FAQ websites and chat rooms. The Ethernet adaptor kits and ExactStream program and source code are also now available online.[59]

¶ 25 The Ninth Circuit noted in the *Napster* decision that the *Sony* Court "declined to impute the requisite level of knowledge where the defendants made and sold equipment capable of both infringing and substantial non-infringing uses."[60] Even though the court held Napster had actual knowledge of acts of infringement, it did "not impute the requisite level of knowledge to Napster merely because...the technology may be used to infringe Plaintiffs' copyrights," based on *Sony*.[61] *Napster* refers to this as the "staple article of commerce" doctrine derived by *Sony* from patent law.[62] *Religious Technology Center v. Netcom On-Line Communication* also suggests that absent notification of specific infringing activity, an Internet system operator "cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[63] If there were notification, then failure to remove the infringing material would constitute material participation, as discussed above.[64]

¶ 26 Thus, DVR companies with constructive knowledge do not meet the requisite level for contributory infringement. DVRs may assert the "staple article of commerce" defense because DVRs, like VCRs, are capable of substantial non-infringing use. However, actual knowledge or notification without corrective action may expose the DVR companies to contributory liability.

Vicarious Liability

¶ 27 To be liable for vicarious infringement, a DVR company must have (i) "the right and ability to supervise the infringing activity" and (ii) "a direct financial interest in such activities."[65] Unlike contributory infringement, vicarious infringement does not require knowledge of the infringing activity.[66] DVR companies probably do not have the right and ability to supervise infringing activity, but may have a financial interest in the activity as defined by recent expansive case law.

- Supervision

¶ 28 Cases discussing the right and ability to supervise infringing activity focus on whether the defendant had the right to terminate or exclude the infringer from its services. In *Fonovisa*, the swap meet operators had the right to terminate vendors' operations and controlled public access to the vendors' services.[67] In *Netcom* the court suggested that ability and right to supervise infringing activity could be shown by control over subscribers through the ability to screen postings and terminate or suspend users' accounts.[68] Also, in *Napster* the Ninth Circuit held that Napster had such ability and right to supervise because it had the ability to police its system to locate infringing material and had the right to terminate users' access to its system.[69]

¶ 29 In all these cases, the defendants actually controlled the environment where the users of their services were engaging in infringing activity. Therefore, they could cut down on infringing activity by eliminating access to infringers or remove infringing copies. DVR companies probably lack the ability to control the environment in which the hackers make copyrighted TV programming available. While DVR companies maintain websites to provide customer service information, they do not allow users to upload information onto their sites. These websites aren't like a BBS, nor are they ISPs[70] However, TiVo does maintain a link to the AV Science Forum, which hosts TiVo chat rooms. If this is the site where the hackers post infringing content or hacking instructions on how to access infringing files, TiVo does not have the ability to control access or content on the site, because it is an independent site. However, to be safe TiVo should police the site and encourage AVS Forum moderators to edit or eliminate any infringing content immediately. It may also wish to either eliminate the links to the chat room or request that AV Science Forum remove the "TiVo Underground" chat site, which is devoted to discussing hacking techniques. As discussed above, there is already a disclaimer on the AV Science Forum site explaining TiVo does not operate the site. If the hackers posted infringing copies of TV programming on websites other than those maintained by the DVR companies, the companies have no right and ability to control these sites.

¶ 30 All of the DVR companies do have the ability to cancel subscriptions of users. However, as discussed above, this will only eliminate the downloading of program guide information and software updates, and will not eliminate the ability of the DVR unit to record programs, connect to an Ethernet card, or run a video extraction program. Thus canceling a subscription and ending the continuous relationship with the user will not affect the environment in which the hacker engages in infringing activity.

- Financial Benefit

¶ 31 Beginning with *Fonovisa* in the Ninth Circuit, recent caselaw has expanded the definition of financial benefit. Under this broad definition, DVR companies may have a financial benefit from the infringing activities of the hackers. In *Fonovisa* the court held that the swap meet operators had a financial benefit in vendors selling infringing recordings because customers paid admission to the meet, the vendors paid rentals fees, and the availability of pirated music enhanced the attractiveness of the venue.[71] The court in *Netcom* did not hold the ISP vicariously liable for infringing posts because the court did not find any evidence that the infringing activity enhanced the ISP's service.[72] In *Napster* the Ninth Circuit restated the *Fonovisa* definition that "financial benefit exists where the availability of infringing material acts as a draw for customers."[73] Also, Napster's financial business model depended on increasing its userbase, which would also increase the number of infringing recordings available for download.

¶ 32 In the case of the DVR companies, their business model is also dependent on expanding user base. While UltimateTV is backed by Microsoft and does not have immediate financial concerns, ReplayTV left the market and TiVo has yet to break even, currently incurring a loss with every unit sold.[74] DVR companies' revenues depend on the subscription service,[75] which will not allow TiVo to break even until there is a critical mass of subscribers.[76] Therefore, these companies may have a financial benefit in selling subscriptions to infringing users to increase the userbase. However, as noted above, DVRs can record broadcast TV without a subscription. Thus, the companies would have no financial interest in a hacker without a subscription who uses a DVR to post infringing TV programs.

¶ 33 The DVR companies may fall under *Fonovisa* and *Napster's* broad definition of financial interest because the infringing activity may enhance the attractiveness of using DVRs and subscribing to DVR service. This is especially the case for TiVo, which uses an open Linux operating system. Many hackers buy TiVo units over other systems merely for the hobby of hacking Linux machines. Also, postings on the TiVo Underground chat site show that hackers enjoy the neutral relationship with TiVo and might not continue to hack if it became antagonistic.[77]

¶ 34 However, hacking DVRs to make the program guides more tailored to personal preferences, adding hard drive space and increasing the speed at which the program guide can be uploaded using an Ethernet is much different from actually extracting video files and posting the content on the internet. If the DVR companies can show that only the former form of hacking, and not the latter, enhances the attractiveness of the DVRs, then they may escape meeting this

element of financial benefit. The companies are taking steps to increase the protection of the copyrighted programs recorded on the units and hackers have spoken outwardly against breaking into the programming encryption and releasing programs such as ExtractStream.[78] Thus, it is probably not the ability to post shows on the web that attracts hackers to the service. Also, the average user of a DVR does not have the ability to perform such complicated hacks, and most do not purchase DVRs for this feature.

V. Conclusion

¶ 35 In the end, it is also important to ask whether it is equitable to hold DVR makers responsible for the infringing actions of hackers, who break through proprietary software put in place by the DVR Makers to protect the storage of recorded files, alter the units to utilize an Ethernet connection, and ultimately post copyrighted TV programs on the Internet. As a spokesperson for TiVo noted, "There are people out there that will hack into anything."[79] Currently, DVRs are most frequently utilized for legal personal time shifting of programs, a substantial non-infringing use. But they have the potential to be manipulated by a small minority for infringing activities.

¶ *36* *Sony* made it clear that staple articles of commerce widely used for legitimate purposes should be protected because the public has an interest in access to the article of commerce.[80] As digital technology continues to thrive in the television world, DVRs will become the new standard of recording technology.[81] The public will have an interest in being able to utilize such technology. Regardless of the acts of hackers, a flat prohibition against the sale of DVRs is unlikely to occur. DVR makers, networks, copyright owners, and Congress will have to work together to find a mutually agreeable path on which to take this technological revolution.

By: Ashley A. Johnson

Footnotes

1. DVRs are also referred to as "Personal Video Recorders," particularly by TiVo. This may be an effort to highlight the personal nature of DVR use to bolster fair use arguments.

2. ReplayTV left the personal DVR market in October 2000, choosing instead to license its technology. UltimateTV was launched in April 200 by Microsoft. TiVo has been the longest

continuous player, since 1998.

3. *See* Fried, Ian, "Hackers don't upset TiVo - yet," CNET News.com (http://news.cnet.com/new/0-1006-200-2436238.html?pt.salon, visited 1/27/01.)

4. For example: http://www.replaytvfaq.com/, http://tivofaq.com/hack/faq.com, http://tivo.samba.org/, http://linuxcare.come.au/tridge/tivo-ethernet, http://www.tivocommunity.com/, and the TiVo Underground at AV Science Forum http://www.avsforum.com/ubbcgitivo/Ultimate.cgi.

5. "While current hacking apparently is not of much concern to TiVo, other modifications might be. Hill [a known hacker who maintains a hacking FAQ website] said he has heard of people who are working to crack TiVo's proprietary format for storing video files...[a modification] that might be less palatable to TiVo and the rest of the entertainment industry." Fried, Ian, "Hackers don't upset TiVo - yet," CNET News.com.

6. *See* Savetz, Kevin, "Breaking It Open, Making It Better," The Washington Post, March 2, 2001, p. E1.

7. "CEA Digital Download Conference Features Hot Debates Over Copyright And Consumers' Home Recording and Fair Use Rights," PR Newswire, March 7, 2001.

8. *See* http://linuxcare.caom.au/tridge/tivo-ethernet/ (visited 1/22/01).

9. *See* Savetz, Kevin, "Breaking It Open, Making It Better," The Washington Post, March 2, 2001, p. E1.

10. See http://www.9thtee.com/extractstream.html(visited 6/7/01).

11. "You've done Tivo, AVSForum, and ethical hackers everywhere a disservice. You are not one of us, and as far as I'm concerned you are not welcome here." See http://www.avsforum.com/ubbtivo/Forum6/HTML/005446.html (visited 6/7/01); "If you expect that most hackers of TiVo like the TiVo...then any tool that puts TiVo (the corp, the service, the box, etc.) at risk is not worth releasing to the public. Developing a hack for private use is one thing; releasing to a site that prying eyes will see is another." Tivo 2 Tivo tread on the TiVo Underground AVSForum, http://www.avsforum.com/ubbtivo/Forum6/HTML/004113.html(visited 4/2/01).

12. Using the modem, the process takes about two hours, and is usually programmed to be done in the middle of the night so as not to tie up phone lines. A faster connection allows for more flexibility as to when this connection can be made.

13. http://www.9thtee.com/extractstream.html(visited 6/7/01).

14. *See* Blount, Alan, "TiVo is One Jack Short," http://www.tvminder.com/features/tivo.html(visited 2/19/01).

15. "We have been nice to them, so they in turn have been nice to us...by releasing stuff they have asked us not to...we declare war...And I would not find it enjoyable to continue to hack in such an environment." See Tivo 2 Tivo tread on the TiVo Underground AVSForum, http://www.avsforum.com/ubbtivo/Forum6/HTML/004113.html(visited 4/2/01).

16. 464 U.S. 417, 420 (1984).

17. *See id.* at 434.

18. *See id.* at 454-55.

19. *See id.* at 451.

20. *Id.* at 450.

21. *See id.* at 454.

22. *See id.* at 444.

23. *Id.*

24. *See id.* at 438.

25. See id. at 439.

26. See *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 519 (9th Cir. 1993) (holding that computer files transferred from permanent storage to a computer's RAM is a copy.)

27. §102.

28. *See id.* at 425.

29. §106

30. Preliminary injunction, W. Dist. Penn., Findings of fact, conclusions of law #3.

31. *See id.* at # 22. *See also Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F.Supp. 543, 553 (NDTX 1997) ("The display right precludes unauthorized transmission of the display from one place to another, for example, by a computer system. (*Quoting* H.R. Rep. No. 1476, 94th Cong., 2d Sess. 80 (Sept. 3, 1976)).

32. *See id.*

33. *See id.* at 25.

34. 92 F. Supp. 2d 349, 350 (SDNY 2000).

35. *See id.*

36. *See id.* at 351.

37. 150 F.3d 104, 108 (2d Cir. 1998). (*Holding* that changing the format of a broadcast to be available by phone rather than radio was not a transformation. Merely repackaging the original leaves the character of the broadcast unchanged, adding neither new expression, new meaning nor new message.)

38. See *MP3.com* at 351-52.

39. *See id.* at 352.

40. *Id.*

41. Case No. 00-06443 MMM (MANx), CD Cal.

42. *See* "The iCrave TV Case," available at http://www.townleys.co.uk/scl/icrave.htm(visited 3/26/01).

43. *See* Complaint available at http://www.mpaa.org/Press/RecTVComplaint.htm. (visited 3/26/01).

44. *See* Answer of Defendants, available at http://www.recordtv.com/ (visited 3/26/01).

45. *See id.*

46. *See id.*

47. 749 F.2d 154, 159 (3d Cir. 1984).

48. *See* H.R. Rep. No. 94-1476 at 65 (1976).

49. This analysis applies to the DVR companies (i.e. TiVo, ReplayTV, and UltimateTV), and not the manufacturers of DVR devices such as Sony or Phillips. DVR companies have granted Sony and Phillips license to manufacture the device, while the DVR companies provide the subscription service, programming, and customer support. Under *Sony*, Sony and Phillips are not liable because just like Sony in that case, their involvement with the customer ends at the point of sale. The DVR companies are different in that they continue to have involvement after the point of sale through the subscription service.

50. *See Gershwin Publ'g Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971). *See also Sega Enters. v. MAPHIA*, 948 F.Supp. 923, 932 (N.D. Cal. 1996).

51. 76 F.3d 259, 264 (9th Cir. 1996).

52. *See id.*

53. *A&M Records, Inc. v. Napster*, 2001 U.S. App. LEXIS 5446, 35 (9th Cir. 2001), (*quoting Matthew Bender & Co. v. West Publ'g Co.*, 158 F.3d 693, 706 (2d Cir. 1998)).

54. *Id.* at 44.

55. DVR companies, however, can monitor recording habits of its subscribers and can find out what type of programming DVR users record when their DVR dials into the system. Much publicized of late, TiVo has announced that it collects anonymous viewing patterns based on area code. The company's privacy policy states that the user must call customer service if she chooses to not have such data collected from her device. It can use this data to determine general viewing habits and better target advertising. Selling such information to advertisers could become a valuable resource for these companies that have yet to turn a profit based on subscription sales. *See* Cave, Damien, "When Big Brother Knows you watch 'Big Brother'",

http://www.salonmag.com/tech/view/2000/09/11/tivo(visited 1/27/01.)

56. For free standing units, the subscription provides all the program information. However, for the UltimateTV and TiVo units that are integrated within a DirectTV receiver, a user might still be able to get such information from the DirectTV service provider.

57. See http://avsforum.com/ubbtivo(visited 6/7/01).

58. *See* http://www.avsforum.com/ubbtivo/Forum6/HTML/005438.html(visited 6/7/01).

59. *See* http://www.9thtee.com/tivoupgrades.htm, (visited 4/13/01) and http://www.9thtee.com/extractstream.html(visited 6/7/01).

60. *Napster* at 38.

61. *Id.* at 39.

62. *See id.*

63. *Id.* (discussing *Netcom*, 907 F. Supp. at 1371.)

64. See *Netcom* at 1374.

65. *Fonovisa*, 76 F.3d at 262. (*quoting Gershwin*, 443 F.2d at 1162.)

66. *See id.*

67. *See id.*

68. *See Netcom*, 907 F. Supp. at 1361.

69. *See Napster* at 49-50.

70. While DVR services allow the units to dial into a central server run by the DVR company to access program information, they do not act as internet service providers. Hackers who want to connect their DVR to a network or the Internet must use their own service provider. Thus, when a hacker posts an infringing copy of a TV program on the Internet, it has gone through the service provider's system and not that of the DVR company.

71. *See Fonovisa* at 263-64.

72. *See Netcom* at 1377.

73. *See Napster* at 47.

74. *See* Chen, Christine Y., "TiVo is Smart TV," Fortune, March 12, 2001, p. 124.

75. To increase revenue until it has enough subscribers, TiVo is currently looking into other business models, such as selling data on viewing habits and entering into partnerships with advertisers, product companies and networks, such as Miller Brewing, PGA, NBC and HBO. TiVo units come preloaded with content and feature their products and programming within the DVR software and program guides. UltimateTV features ads within its programming guides as well. *See* "TiVo makes strides with marketers," Broadcasting and Cable, Feb. 5, 2001, p. 43. *See* also Footnote 61.

76. As of the beginning of 2001, TiVo had a total subscriber base of 153,000 and expects to add 180,000 to 220,000 subscribers this year. *See* "TiVo shifts marketing, unveils AOL deal," Reuters Company News Jan. 30, 2001. (Available at http://www.hoovershbn.hoovers.com/bin/story?StoryId=CoNzkub9DtJmWmtaZnJm5&FQ=c%, visited 2/19/01). Forrester Research predicts that DVR sales will reach 53 million by 2005. *See* Shim, Richard, "TiVo adds new features to TV recorder service," CNET News.com Jan. 6, 2001. (http://www.news.cnet.com/news/0-1006-200-4393048.html?tag=st.ne.1430735..nt, visited 2/19/01.)

77. *See* Footnote 15.

78. *See* Footnote 11.

79. *See* Fried, Ian, "Hackers don't upset TiVo - yet," CNET News.com.

80. *See Sony* at 440.

81. Major networks, studios and entertainment groups, such as AOL Time Warner, recognize the future of such technology, by holding equity stakes in DVR companies such as TiVo. *See* Chen, Christine, "TiVo is Smart TV."