How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use"

Deirdre K. Mulligan
Acting Clinical Professor and Director Samuelson Law, Technology & Public Policy Clinic
Boalt Hall, School of Law
University of California
Berkeley, CA 94720
dmulligan@law.berkeley.edu

John Han
M.S. Candidate
Class of 2004
School of Info Management & Sys
University of California
Berkeley, CA 94720
john_han@sims.berkeley.edu

Aaron J. Burstein
J.D. Candidate
Class of 2004
Boalt Hall, School of Law
University of California
Berkeley, CA 94720
burstein@boalthall.berkeley.edu

ABSTRACT

We set out to examine whether current, DRM-based online offerings of music and movies accord with consumers' current expectations regarding the personal use of copyrighted works by studying the behavior of six music, and two film online distribution services. We find that, for the most part, the services examined do not accord with expectations of personal use. The DRM-based services studied restrict personal use in a manner inconsistent with the norms and expectations governing the purchase and rental of traditional physical CDs, DVDs, and videocassettes. If adopted by consumers the DRM systems stand to alter the norms governing personal use of copyrighted content and create pitfalls of legal liability for unsuspecting consumers. In conclusion, we present technological and legal considerations which may help current and future DRM system designers better accommodate consumers' expectations of personal use.

Categories and Subject Descriptors

K.5.0 [**Legal Aspects of Computing**]: Hardware/Software Protection

General Terms

Legal Aspects

Keywords

Digital Rights Management, Content Distribution, Access Control, Personal Use, Fair Use, Copyright, Privacy

1. INTRODUCTION

In a previous paper, two of the present authors detailed the failure of current rights expression languages (RELs), generally modeled on access control languages, to support the exceptions and limits on exclusivity found in copyright policy [33]. The authors found that existing RELs expanded copyright holders' exclusive rights and made it nearly impossible to either express or engage in the legal and unregulated personal uses individuals expect from content. As we concluded in that paper, REL-based DRM-systems are incapable of capturing, or even approximating, the myriad limitations on exclusive rights as well as the contextual considerations that underlie much of how copyright works in practice. We concluded that DRM systems that enforce unconditional access control rules distort copyright law.[1]

Given the documented constraints of current RELs, we decided to examine whether currently popular DRM applications are meeting consumers' expectations of personal use. We undertook an empirical study to examine the extent to which representative services offering DRM-based delivery of music and movies support consumer expectations of personal use. We examined the behavior of the services as well as their terms of service agreements. To provide the basis for our assessment, we have defined a baseline set of "personal uses"[2] that individuals expect to have. Where appropriate, we tie these

DRM '03, October 27, 2003, Washington, DC, USA.

[1] Private contracts present a similar opportunity to displace or distort copyright policy. For that reason, we examined the terms of services as well as the behavior of the services. However, as others have noted, because contracts require a separate enforcement action to be brought and a decision by a court to enforce they are less able to eat away at individuals' expectations in an unchecked manner [27][28].

[2] At the outset we need to clarify one point. Too much of the discussion regarding DRM and the law has revolved around the term "fair use." (Fair use is defined in Section 107 of Title 17 (Copyright) of the United States Code. The statute lists four broad, non-exclusive factors for courts to consider whether the copying of a work, otherwise within the exclusive rights of the copyright holder, is "fair" and therefore may be carried out without compensating or obtaining permission from the copyright holder.) As most computer scientists, and even some lawyers, are eager to note, a computer cannot be instructed to implement fair use. Vague factors rather than concrete uses define fair use, which means that determining whether a use is fair often requires litigation, rather than the algorithmic evaluation of an action.

expectations to both statutory and case law from the United States. For the purpose of our evaluation we extracted several classes of functions that a DRM system capable of supporting expectations of personal use would necessarily provide -- portability, excerpting, and limited relationship between users and copyright holders. Although some of the services that we examined offer substantial innovations in the way that individuals can gain access to and experience copyrighted works, none support the range of personal uses of copyrighted works that individuals expect. We conclude with some suggestions as to how current DRM technologies could be designed to better support personal use.

2. DEFINING PERSONAL USE

2.1 Topology of Uses of Copyrighted Works

Copyright law enumerates a subset of possible uses over which authors or principals of works are granted exclusive rights (reproduction, preparation of derivative works, distribution, public performance, public display). In general, any activity that implicates one of these rights requires permission from the copyright owner, though numerous exceptions apply. Congress grants these exclusive rights to provide creators with an incentive to make their works available to the public, and to spur further creation and dissemination of creative works.

Copyright holders while given excusive control over this set of rights are given no authority to control many other uses of their copyrighted works. This means that legal possessors of content have broad latitude under the law to use those works in ways which they choose.

Copyright law is silent on a host of uses of copyrighted works; we call these uses *unregulated*. These unregulated uses occupy a curious place in copyright law. They are defined by their absence from the regulatory structure, rather than their affirmation or explicit allocation to the public. These unregulated uses are those that typically require no reproduction, [3] preparation of derivative works, distribution, public performance, or public display of the copyrighted work. Consider the possible uses of a novel. Opening and closing the book, reading it from cover to cover, repeatedly reading some sections while skipping others, annotating its pages with notes, physically removing pages, or reading the book in a foreign country are examples of uses which copyright statutes simply do not address. Similarly with a CD, purchasers may listen to the recording in their car, at their home, at their office, or in their friend's car. Purchasers may play selections for their family and friends. They may lend the CD to other people, even to a complete stranger, to use in any number of places. Today all of these actions are widespread and few individuals would question their legality.

Fair uses are protected and loosely defined by Section 107 of the Copyright Act.[4] It states that "the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." In contrast to unregulated uses, "fair uses" typically arise, and are defined, in the context of a defense to allegations of copyright infringement.[5] While fair uses of copyrighted works involve uses that are within the exclusive rights of the copyright holder, they are "not an infringement of copyright." A fair use is by definition, an unauthorized reproduction, derivative work, distribution, public performance, or public display of a copyrighted work that is viewed under the law as non-infringing and requires no compensation to the copyright holder. Several important personal uses have been held to be fair use, including the home recording television programs for later viewing and personal copying of digital files to use them at a different location [38][43].

In this paper we focus on "personal use." As a mixture of unregulated and fair uses personal use is not subject to a clear definition [29][30][46]. Personal use encompasses many uses that we have previously described as "unregulated uses" – uses which typically do not infringe on the exclusive rights reserved to authors and on which the copyright law is largely silent. Many of the unregulated uses are routinely exercised by individuals in their capacity as private citizens. Personal use also encompasses uses that have not been litigated because they have been difficult to monitor or are viewed as having a de minimis economic effect, but which might be found to be infringing [46]. The term "personal use" also includes some rights that have been declared "fair use" by the courts. While this subset of personal uses tread on the exclusive rights of copyright holders they have been authorized or permitted under the fair use doctrine. Personal use for the purpose of this paper is comprised of both legally defined "personal use rights" and "personal use expectations." Figure 1 depicts the topology of "personal use".

[3] Engaging in a range of these activities on the Internet may require the creation of a temporary digital copy. Under current case law these copies themselves may be considered infringing. However, the purpose of making the copy is to support an activity individuals expect to be able to engage in because of their experience with copyrighted works distributed on other media.

[4] To determine whether a use is fair one must evaluate a list of four non-exclusive factors:

a) the purpose and character of the use;

b) the nature of the copyrighted work

c) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

d) the effect of the use upon the potential market for or value of the copyrighted work.

[5] The question of whether "fair use" is strictly a defense or serves to affirmatively define rights of the public is open to debate. Even if "fair use" is conceived of as a defense, its use to define fair use exceptions to the exclusive rights leads to the creation of what can be considered for all practical purposes a set of "fair use" rights [16]

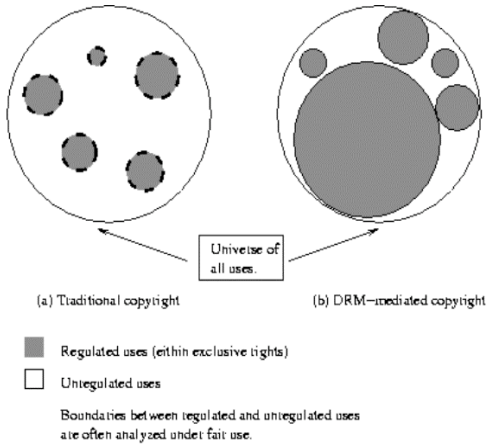

Figure 1: A figurative depiction of how DRM alters the assignment of rights under copyright.

While a simple definition of personal use is elusive, several efforts have been made to articulate a set of uses or rights of copyrighted content that should be reserved for individuals. The DigitalConsumer's Bill of Rights is one example. It states that individuals have the right to: time shift; space shift; make backup copies; choose platforms; translate between formats; and, to use technology to effectuate these rights [17]. For a DRM system to support any one of the "rights" articulated in the DigitalConsumer's Bill of Rights, or another articulation, it must provide some baseline functionality. Rather than focus at the level of "rights" we decided to examine whether the DRM enabled applications provided the functionality necessary to engage in these personal uses.

The three functional aspects that we explored are:

Portability: the ability to use acquired content on any suitable device, regardless of ownership interest in the device or its physical surroundings. Portability also refers to the ability to shift the format of a copy.

Excerpting: the ability to excerpt from, modify, and in other ways tinker with content.

Limited relationship and interaction with copyright holders: This criterion refers to the extent to which services relationship and interaction with individuals reflect expectations set in other media. It considers the extent to which services require ongoing relationships from their users, and the breadth of those relationships in terms of time commitment and content usage rules and requirements. One aspect examined of the nature of these relationships is the complexity of information transaction required to acquire content; in other words the number of entities collecting and using service user's personal information, the independence of those entities' respective privacy policies, and the complexity of relationships for information exchange between those entities.

2.2 The Market, Personal Use, and DRM content distribution systems

Individual expectations concerning normative uses of music and film have proved resilient to personal-use limiting digital content distribution models. In other words, customers have largely rejected restrictive DRM systems rather than change the uses they expect to be able to make with content they own [26]. Pressplay, MusicNet, and Rhapsody, all prevented CD burning, transfer to portable player, and download to personal computers upon their respective debuts in the Fall of 2001. The product use policies were profound failures. Individuals didn't find compelling reason to switch to their new models, which priced content similarly to CDs, but crippled prominent uses beyond the point of sale. In late 2002, along a somewhat mutual learning curve, each of these firms redesigned their respective service policies to accommodate CD burning, downloading, and device transfer [34][37][39][41]. Despite these "concessions", the most successful music subscription service in April 2003 only slight surpassed 100,000 subscribers [26], a number dwarfed by the more than 60 million file traders active today [52].

One lesson learned from the experiences of early versions of these online music distribution services might be that if consumers are to adopt digital distribution as a preferred mode of content acquisition, copyright interests must be reconciled with what users expect to be able to do with purchased content. Scholars have described this relationship between copyright and what consumers expect as a "fundamental trade-off between control and customer value." [50] Less restricted products are more valuable to the customers who purchase them. This means that less restricted products should attract more customers and justify higher prices than otherwise. The trade-off, then, is that allowing very liberal use of products may enable the production of substitute copies that harm sales of original works. The challenge for content distributors is to maximize sales of works by finding the right balance of permissible uses to satisfy customer norms while not facilitating piracy.

Customer rejection of the overly restrictive policies used by early music service iterations suggests that preventing CD creation and device transfer misses this optimization point. On the other extreme, it seems likely that unrestricted content file sharing is bad for content sales. In striking a proper balance, copyright owners have worked from a default of total restriction with some uses permitted. Although steps have been taken to liberalize the use of DRM protected media, the restrictions remain substantial. The continued struggle of most online music services to attract mass markets and convert peer-to-peer file sharers might indicate that consumers find current usage restrictions unacceptably restrictive.

Some music distribution services accept the perseverance of consumer expectation. From those firms there appears to be a growing market-motivated tendency to accommodate more precisely what individuals expect of and law designates as personal use. This trend is well illustrated through Apple's promotion of the release of iTunes music store under the slogan "Rip, Mix and Burn" to indicate that service's

comparatively liberal usage policies. Considering and accommodating what individuals expect may be important if DRM systems and the new business models that they enable are to attract mainstream customers.

3. THE PRESENT CLASH BETWEEN DRM-BASED SERVICES AND PERSONAL USE

3.1 Study Methodology[6]

With each service we examined registration, logging-in and logging-out, downloading, service and content upgrades, service cancellation, and content rendering, in addition to the contractual terms of service. Of rendering we examined playback on a second computer and portable CD player, as well as copying, format conversion, and excerpting. To examine content editing capability, we tested files from each music service using two media editing suites: SoundForge and GoldWave. We monitored network transmissions and file accesses originating from each service and its respective software on our workstation. For network transmissions, we used an application called Snort [42] to record and log all incoming and outgoing packets during various stages and processes of service use. We then used Ethereal [22] to analyze TCP traffic between service proxy software and service servers. Our study, in this respect, was limited by the use of encryption and unknown communication protocols at the application layer. We monitored how each service's client accessed the local filesystem using FileMon [44]. All file reads and writes were logged but we did not record the data read or written.

3.2 Overview of Findings

Generally we found agreement between the services' stated actions as outlined in their terms of service, end user license agreements, and privacy policies and their observed behaviors. Since many privacy policies reserve expansive rights for the services to monitor their customers activities, and many terms of service restate the restrictions that the technology implemented, this finding was not surprising. The clash between these behaviors and personal use as defined by law and individual expectations, however, was substantial.

3.2.1 Portability of Content: Findings

With the music services examined,[7] portability was sold as a feature in the form of incremental permissions. iTunes was the exception to this finding, selling tracks a la carte, after which purchasers acquired unlimited burning capability per track. The music services examined can be divided into subscription[8] and non-subscription services. Four of the music services were subscription-based: Pressplay, MusicNet, Rhapsody, MusicNow. Pressplay and MusicNet each provide their users with pre-bundled sets of ten CD-burn and device-transfer credits per monthly billing cycle.[9] Rhapsody and MusicNow sell tracks individually. The two remaining music services--iTunes and Liquid Audio--did not require a subscription before content could be purchased. Liquid Audio, like iTunes, sells content rendering and portability permissions track-by-track. As shown in Appendix A, every music service examined with the exception of iTunes limits the number of times tracks licensed for portability (enhanced tracks) can be burned to disc, the number of portable devices enhanced tracks may be transferred to, and the number of additional computers that may be registered to perform downloaded tracks.[10]

With all of the DRM content services studied, transferring tracks to additional computers makes files non-functional. Content license keys are stored separately from content files on a local machine. This design makes license reacquisition necessary to regain functionality every time content is rendered on a new computer. Individual content services possess the discretion of whether to grant new licenses. This discretion acts as enforcement mechanism preventing file portability in certain cases. Pressplay, for example, only allows files downloaded from its service to be rendered on one subsequent machine. It enforces this limitation by profiling and then authenticating the hardware of computers which users use to play content. Requesting a new license from a third computer will fail to match one of the two profiles associated with a given user and a license will not be granted.

Another way that portability is limited through the services examined is license expiration. Microsoft DRM-based applications set a license expiration value which designates the life-span of granted licenses. This enforces the restriction that "rented" or "leased" works will work only for the contracted duration. Users of some of the subscription services for example, may download tracks, but must remain members of the service in order to retain use of those tracks. This requirement is enforced through the periodic grant of temporary licenses. Without service renewal, downloaded files simply deactivate.

A third source of portability restriction is license revocation. License revocation involves the termination of a license by a content service provider prior to its originally set time of

---

[6] We used an Intel-based Dell desktop(1.70GHz processor, with 256M RAM) running Microsoft Windows 2000 to examine Windows-based services. We tested iTunes using a Macintosh G4 titanium laptop running OSX (version 10.1.5).

[7] Due to their rental business model, neither of the film services that we examined allowed transfer to portable media, so there is little to discuss with this factor.

[8] The subscription services, in effect, rent copies of musical recordings. This business model, which is essentially prohibited by an exception to the first sale doctrine, and therefore off-limits to anyone but a copyright holder, does provide an inexpensive way to obtain access to a large variety of music. Since these services are authorized by copyright owners, the music rental exception to the first sale doctrine does not apply [1].

[9] After those credits are used, Pressplay offers users the option to purchase more *portability credits* in sets of five. AOL/MusicNet does not permit the purchase of additional credits past the ten it assigns each month, instead requiring users interested in burning more than ten tracks to wait until the next monthly subscription cycle.

[10] *See* Appendix A for a summary of the terms that all services offered.

cessation. None of the services examined exercised any form of license revocation.

Each of the Microsoft-based DRM services permits the conversion of enhanced content files into CDA or WAV file formats for burning to CD. Beyond this no other format conversion is allowed.[11] Windows Media-encoded content can only be rendered in WMP, which does not provide a method for file conversion. iTunes, which uses Apple's proprietary AAC encoding format, also lacks apparent methods for converting files to other formats.

In practice, most of these restrictions could be worked around by burning a file to CD and recopying it onto a computer, otherwise known as CD ripping.[12] None of the services examined restricted CD ripping. Ripping songs from CD using Windows Media Player (WMP) converts them to WMP format. During conversion users are prompted whether or not they would like the content to be marked as "protected"--protected content then being restricted from rendering on subsequent computers. Rejecting the "protected" option yields a completely portable, DRM-free copy of the file. iTunes enforces the additional limitation that ripped versions of its tracks cannot be reburned to CD by making these files non-readable using some CD burning software.[13] None of the other services enforced similar restrictions.

DRM-based online music services thus raise the cost to users of achieving the same portability that accompanies a physical CD. The cost is accounted for mostly in the time that it takes to burn copies of a track to a CD, and then rip the track back to a computer file. Users who place a sufficiently high value on the portability of musical recordings will be willing to invest this time. [14]

3.2.1.1 Potential legal risks for users who attempt to "lend," "time-shift," or "space-shift"

If portability is unsupported or limited, and by extension, the ability to share and space and time shift copies of music and movies is restricted by online services, there is a question of whether users will attempt to maintain these personal uses.

One option for sharing files is to share a subscription account. That is, one user could share his user name and password with another person. Although such account-sharing does not involve portability in the usual sense--transporting physical copies, or transmitting digital ones--the effect of sharing subscription information is rather similar. This act could involve defeating a combination of technical and contractual access control measures. The same act could also involve bypassing access controls on both local machines and remote servers. Similarly, a user could attempt to "time" or "space" shift files by defeating the technical features that tether files to a specific device. This would involve violating the terms of services as well.

These activities may expose users to liability under the Digital Millennium Copyright Act (DMCA), the Computer Fraud and Abuse Act (CFAA), and the state-defined crime of theft of services. Although the DMCA provides, by far, the most plausible theory with which to enjoin account sharing or attempts at "time" and "space" shifting the other statues mentioned may become more applicable in other plausible circumstances.

A brief review of some common technical restrictions and contractual restrictions and there relation to account sharing will help bring the legal issues into sharper focus. "Tethering" a copy, or limiting the number of machines to which a usable copy of a work can be transferred is a common technical restriction.[15] Many of the services added contractual terms that further defined the boundaries of individual subscribers' permissible uses. For example, Pressplay's Terms of Service (TOS) provides that the second copy of a download may only be transferred "to an additional computer (desktops or laptops) *that you own*." [36] Pressplay's TOS also states that each subscriber "agree[s] . . . not to allow others to use [his] member name, password and/or account." [36]

To draw out more fully some of the potential legal issues implicated by account-based, subscription services, we consider an example of "account misuse." Let us consider, as a term of the fictitious music service Music, Inc., a prohibition on account sharing identical to the Pressplay term cited above. For simplicity, assume that Music, Inc. only offers streaming audio tracks. Access to Music, Inc.'s streaming media servers is controlled by user name and password-based access controls, and the audio streams are encrypted until they reach Music, Inc.'s software client. Suppose that Jill, who is not a Music, Inc. subscriber, uses the account information of her husband to access Music, Inc.'s streaming audio. It is important to note that the source of music in this example is a

---

[11] As with portability, ripping tracks from burned CDs produces DRM-free versions of the content copied. These files may then be converted into any of a number of additional formats without restriction using available software. However, because WM formats are proprietary, the programs capable of their conversion are not free or ubiquitously installed [35].

[12] "Ripping" refers to the process of copying a music track contained on an audio CD into computer memory as a file.

[13] We tried Roxio and NeroBurn.

[14] The question of what kinds of copyright infringement liability might attach to the act of burning a CD via an online music service, then ripping and distributing copies from this CD, is an interesting one but we do not explore it here. For a strong suggestion that placing files obtained in this fashion on a peer-to-peer network is an act of direct copyright infringement see [31].

[15] An important question for users is whether they can make backup copies of tethered downloads. Nothing prevents this; the Windows Media Audio format prevents the copies from being used on other devices. A tethered download can be *synced* to a different computer-after the consumer's original computer is replaced, for example--but such a restored track may not be transferred to a second device.

remote server; the content does not reside on the user's home computer.[16]

Music, Inc. could make a plausible claim against Jill for a violation of the "access control" provisions of the DMCA. Alleging a violation of the DMCA's "access control" provisions requires alleging that a person "circumvent[ed] a technological measure that effectively controls access to a [copyrighted] work." [2] "Effectively controlling access," in turn, means that a technological system requires the "application of information . . . with the authority of the copyright owner." [3] The threshold legal question is whether the user name and password, which can be stored in the Music, Inc. client application, comprise "information" within the meaning of the statute. If so, then it appears likely that sending this information to Music, Inc.'s streaming audio server is the "application" of information that results in access to copyrighted works. In further support of its access control violation claim against Jill, Music, Inc. could argue that she has applied her husband's account information in violation of Music, Inc.'s express authorization because Music, Inc.'s Terms of Service do not extend to her permission to use her husband's account. Whether a court would interpret the DMCA and the Terms of Service in this way is uncertain, and there are not yet cases discussing this point. This hypothetical violation is, admittedly, a rather formal one, and it is difficult to see how the music service would be able to detect the difference in the physical identity of the user. Still, even a formally plausible claim of a DMCA violation for sharing a music service account draws attention to the potential liability that could arise from customary behavior.

A separate, if somewhat more tenuous, claim could arise under the CFAA. Part of the CFAA provides that "[whoever] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value" violates the CFAA. Although the CFAA has gained most notice for its use in criminal prosecutions,[17] it also authorizes civil suits by "[a]ny person who suffers damage or loss by reason of a violation of" the CFAA [5].

Nonetheless, Music, Inc. would shoulder a heavy burden in pursuing a CFAA-based claim against Jill for the conduct described in this section. First, plaintiffs pursuing a civil claim under the CFAA must allege damage or loss of $5000 or more in a one-year period [4]. Given that most online music services charge about $10 per month for unlimited access to streaming audio, it is difficult to see how Music, Inc. could show that it suffered a $5000 loss. Second, Music, Inc. would have to prove that Jill both "exceeded authorized access" on Music, Inc.'s remote streaming audio server and had the "intent to defraud" Music, Inc. in doing so. Courts have interpreted the CFAA's authorization condition to include both access control methods, such as passwords [18], and contractual conditions [19],[18] so it is possible that Jill has "exceeded authorized access" on the remote server. However, her rather innocent (mis)use of an account is unlikely to reflect an intent to defraud.

To incur liability under the CFAA, Jill (or her husband) would have to share their account with sufficient numbers of persons to meet the $5000 damage threshold, and would have to do so with the intent to deprive Music, Inc. of that compensation. If we assume a value of $120 per subscription per year, a person would have to share an account with 42 other persons in order to inflict a $5000 loss upon the service. In practice, an online music service would probably invoke contractually reserved self-help measures before account sharing reached this level. For example, Pressplay reserves a right to suspend or terminate an account if it "reasonabl[y] suspects" that a subscriber has violated an applicable intellectual property right [36].

Finally, we consider whether Jill's actions could run afoul of state law. Although it is difficult to generalize about state laws, most states define a "theft of services" offense. These statutes are frequently open-ended, defining an offense for obtaining performance of a "service" by deception [45]. Jill's conduct in our rather homely example probably does not rise to the level of "deception," but the possibility remains open that similar conduct in different contexts could meet this standard.

The point of this example is not to suggest that copyright holders or DRM application vendors are likely to pursue these actions against users, but to highlight the fact that the structure of DRM applications may drive users seeking to engage in customary personal uses of copyrighted works toward legally questionable behavior.

3.2.2 Excerpting and Modifying Content: Findings

All services contractually prohibit sampling, excerpting, and other forms of content modification. Those agreements that were explicit in this regard banned content modification, copying, and translation, among other possible uses [13][36]. Moreover, technologically DRM-encoded files are not interpretable using media editing software. SoundForge recognized files' DRM protection and aborted attempts to open them. GoldWave allowed files to be opened but, as one would expect, did not decode intelligibly.[19]

---

[16] The idea behind this example, and our justification for discussing it in connection with portability, is that sharing account information has an effect similar to one person's lending a copy of a recording to another person. In both cases the lender gives up his right to use the content while the borrower uses it. As we shall see, however, the legal consequences of sharing a recording are quite different from those of sharing an account for an online service.

[17] One of the earliest cases was the Government's prosecution of Robert Morris, who in 1988 released a worm that exploited a security hole in the Sendmail program [49].

[18] Other contractual conditions create a right for Pressplay to terminate an account if it "reasonabl[y] suspects" that a subscriber has violated an intellectual property right [36].

[19] As we noted earlier, however, the efficacy of these limitations, to the extent that they are enforced by DRM, can be overridden burning to and ripping from CD.

3.2.2.1 *Excerpting and Modifying Content: Legal Analysis*

As discussed above, individuals have been able to sample content from physical media for use in reviews, commentary, and the composition of new creative works. Directly copying content distributed by the online services that we examined is not possible, and courts thus far have found that circumventing access controls, even to make a fair use, is no defense to the DMCA's anti-circumvention provisions [40][47][48]. Although a user's right to edit content is less explicitly provided for than excerpting, there is little doubt as to its widespread exercise and its cultural value. This limitation is not provided for in the Microsoft DRM architecture that underlies most of the services that we examined.[20]

Three general outcomes seem possible, should this legal framework remain constant. First, if users begin to adopt DRM-based online services as a replacement for physical media and files on peer-to-peer networks, the excerpting norm may gradually give way. A second possibility, which is not exclusive of the first, is that users who are serious about being able to excerpt legally from recorded works will eschew DRM-protected works. (In the case of movies, of course, this would require purchasing video cassettes rather than DVDs.) Second, DRM-based services might respond to user preferences regarding excerpting in the same way that they have responded to the demand to be able to download tracks to personal computers and burn them to CD. Others have explored ways in which this might occur [11][21][24]. We defer further discussion of this point to our Suggestions.

3.2.3 *Changing Business and Privacy Relationships*

Each of the services that we studied requires the local installation of proxy software.[21] Use of MusicNet requires the additional installation of RealPlayer and America On-Line. While left active these software proxies continually reference Windows Internet Explorer (IE) index.dat files. Index.dat files serve as history logs for the folders in which they reside. One resides in each of IE's cookies, history, and temporary Internet files folders. These files are not affected when folder contents are altered or deleted, and cannot themselves be deleted. Thus, index.dat files act as a type of permanent record of the websites that users have browsed and of the files that they have downloaded from the Internet.[22]

Rhapsody's software client contacts Rhapsody's content server every 45 seconds while idle. This software reads from Window's index.dat files prior to every transmission. Since there is no clear reason why the service, while idle, would require information about cookies or browsing history, these two findings in conjunction may reflect monitoring of user browsing habits.

The two film services require their customers to transact with servers to reacquire new license files each time content is rendered.[23] Both MovieLink and CinemaNow state that they collect usage information concerning the number of times films are played for royalty purposes.[24] The "registration" with services servers each time films are played for the first time, paused and resumed, or rewound and resumed, no doubt allows the two movie services to maintain meticulous records concerning how movies files are used by individual customers. Windows Media Player may also be used to monitor how content files are used. WMP records the number of times individual tracks are rendered in order to enforce restrictions on track playback [51].

Furthermore, using the services studied initiates highly complex webs of information monitoring and exchange. For example, the number of advertising partners Pressplay engages with is unclear. However, it is clear that usage of the service involves interaction with a minimum of four separate entities with a minimum of four separate policies governing use of

---

[20] Content encoded using Microsoft DRM is usable in ways explicitly provided by the capabilities of WMP which is charged with the rendering of all DRM encoded content. This means that files may be set in order to allow or deny playback, transfer to portable rendering device, copying, or burning to CD. However, all other uses including the majority of non-regulated uses are prevented by default due to limitations in WMP capabilities. In this example, because WMP does not contain features for editing music or video, Microsoft DRM encoded files can never be edited.

[21] The Movielink proxy includes a tray application whose purpose is to remove downloaded movie files from a user's hard drive after rental periods have expired. Movielink client software also includes a background process that periodically communicates with a server for software updates. The installation and operation of these applications are not made apparent to users.

[22] Service proxies read from these index.dat files consistently during every stage of service use which we examined. During login, logout, content upgrades, and prior to content downloading and rendering, FileMon recorded read accesses to these files. We were unable to examine iTunes for consistency with this pattern. Moreover, due to encrypted transmissions, we were also unable to determine whether information about user browsing histories was being transacted with service servers. The services admit to recording what files are streamed, downloaded, and enhanced, as well as counting the number of times content is rendered [13][36].

[23] CinemaNow grossly violates user privacy by not encrypting user login information before transmitting it. This facilitates theft of login information and misuse of accounts. It also offers eavesdroppers identifiable information concerning users' browsing habits.

[24] Reissuing a license each time a movie is viewed is consistent with this royalty arrangement. The music services examined also state that their royalty obligations require them to record how many times a downloaded track is played, and whether a track is burned to CD [32][13]. CinemaNow deserves mention as one of the most obnoxius and patronizing privacy policies that we examined. Its tone stands in sharp contrast to the fire and brimstone of their *Terms of Use* and perhaps correlates with the respect that CinemaNow affords to the rights discussed in both policies.

information collected about users.[25] The other services examined all exhibit similar degrees of complexity.

3.2.3.1 The Legal Basis for an Expectation of Privacy in the Use of Copyrighted Works

The current law of the United States provides little structure for an ongoing relationship between consumers and copyright owners. Users also have legal avenues for experiencing works without engaging in any transactions to access them. One example is reception of radio broadcasts. Because radio broadcasters pay for blanket licenses to perform recorded music over the air, listeners neither need to pay nor reveal which broadcasts they have tuned into.

Often, however, acquisition of a work requires some form of transaction. These transactions may be nearly anonymous, such as when a consumer pays cash for a copy of an album or a movie. No record remains to link this individual with the purchase of this copy. Subsequent transactions involving this copy -- lending, selling, and even the copy's destruction -- also occur without any record necessarily being created. At the other extreme of transactional anonymity is video rental. The rental firm often requires credit card information before awarding membership, even if cash is used in transactions. The firm also records which rentals have been taken out by an individual, with the obvious purpose of being able to identify late returns and charge fees accordingly.

Copyright law helps to illuminate the individual expectation of privacy beyond purchasing content. Unlike users of the content services we studied, purchasers of content have traditionally entered into transactions with distributors or other intermediaries, and not copyright holders. Since copyright owners and content distributors have very different profit interests, this change of the selling party causes a subtle but important shift from the perspective of the consumer.

Whether music, movies, books, or other media are at issue, a publisher often must pay a copyright holder (or some other party entitled to receive royalties) for each copy of a work that is made. Beyond this point, their profit interest turns toward the sale of those works. Distributors may keep records of customer activity to optimize inventories and supply chains or to target advertising. However, since publishers record the number of copies they make, once a consumer purchases a copy of a work there is no longer a copyright-based reason to monitor that purchaser's activities.

Copyright holders' incentives to monitor users are certainly very different from those of the distributors whom content purchasers are accustomed to dealing with. Because copyright owners derive profit primarily from the licensing of their copyrights, they have a compelling interest to monitor how purchased works are being used for the purpose of enforcing copyrights and extracting additional revenue.

Monitoring of content users by copyright holders is a novel phenomenon. For example, traditionally, despite the paper trail that may follow from renting or purchasing works with a credit card, copyright owners neither have access to credit card transaction data nor a relationship with individual consumers to enable other forms of monitoring. The federal Video Privacy Protection Act [6] (VPPA) requires rental outlets to destroy rental records "as soon as practicable." [9] Rental firms may not share their records with anyone except in a few narrow circumstances, such as with law enforcement officials in possession of a warrant, or with parties to a civil lawsuit who show a "compelling need" for the information [8]. The combination of a federally protected privacy right and the small size of many video rental outlets (which limits the extent to which rental records could be shared within a business or corporation) has created a strong consumer expectation that their video rental records are accessible to few people.

Legal support for this consumer expectation is different online. Whether the VPPA applies to Internet distribution of digital copies of music is an open question [7]. Even if the VPPA does apply, its protections do not address the different data collection opportunities presented by Internet distribution. For example, an Internet based digital movie rental service, offers the distributor--increasingly the copyright holder--numerous opportunities to record sensitive information about intellectual consumption [14] including user browsing habits, or the frequency with which movies or sections of movies are viewed, among other activities. If the VPPA is inapplicable to such Internet based digital movie rental services, without the obligation to destroy personally identifiable information "as soon as practicable", the reservoir of information available for marketing and profiling, copyright enforcement, and subject to subpoena increases dramatically. Even if the VPPA were found to apply many of the new opportunities to collect information--browsing, collection by third parties who are not renting the videos--would remain outside the scope of protection.

Privacy-preserving means of experiencing online music are lacking. In contrast to transaction free reception of open-air radio broadcasts, the most closely analogous online service, streaming audio, requires full user registration. The broadcasting server logs which songs consumers have streamed and, possibly, for what duration. In addition to monitoring by content servers, service proxy software, service websites, and media rendering software may all comprise sources of surveillance.

---

[25] Pressplay, for example, shares non-identifying statistics with "certain strategic partners." [53] These, likely advertising, partners use the information for their own analysis governed by a separate set of privacy policies. Pressplay tracks movement within their website through a contracting service called Keylime Software which is governed by a third privacy policy. As with other services operating through their webpage, Pressplay disclaims liability for any action Keylime may perform in violation of its own privacy policy. Finally, Microsoft DRM, which Pressplay utilizes to protect content, periodically collects and transmits machine-identifying information to a Microsoft streaming media server as part of a software update process. The handling of this information is performed according to Microsoft's privacy policy [53].

The ways that information is collected and processed during use of the services examined is almost impenetrably complex. It is difficult to determine exactly what data a service collects, and merely discovering that separate monitoring entities sit behind the services requires a careful reading of the services' privacy policies. Software clients further complicate consumers' privacy policy evaluations, because each client is governed by its own privacy policy. More importantly, deciphering the terms of each separate service's privacy policy and building an accurate understanding of how each overall service uses client information is a daunting task as compared with the straightforwardness of purchasing content in traditional media.[26]

4. DRM APPLICATIONS AND PERSONAL USE

The DRM systems we studied fail to approximate personal use on several levels. We found that DRM-based restrictions on content use generally arise from a default of total restriction (unlicensed content), from which incremental permission may be granted in exchange for a fee. The collections of permission sets available to content owners reflect the design choices of DRM systems architects, though certainly with consideration for what would spur adoption by copyright holders. For example, Microsoft's rights management product furnish application developers with a set of Boolean values, which may be turned on or off to permit or restrict various uses,[27] and a set of variable counters to implement frequency limitations on exercise of those permissions. These enumerated carve-outs make it virtually impossible to emulate established personal uses. There is no context dependency or conditional prerequisite to the restrictions that might allow for consideration of factors that play into a fair use determination or that might distinguish between public and private or commercial and non-commercial use. The restrictions chosen by content principals are universally enforced in all instances and contexts of use limiting not only large-scale infringement but also many personal uses.

Also important, a host of unregulated uses are incidentally obliterated by DRM design. Since content encoded using Microsoft DRM may only be rendered using a set of products with narrow capabilities, all of the uses that rendering programs have not been designed to perform are blocked by default. License files may designate the ability or inability to perform core uses such as playback, transfer to portable device, copying, or burning to CD. However, all other uses not designed for in rendering software, including a large fraction of non-regulated uses, are restricted without consideration for purchasers' legal rights and normative expectations.

The DRM systems we studied were based on DRM software development platforms that make emulation of normative content portability difficult to implement. Rendering of traditional media requires mere possession of the copyrighted work. Irrespective of ownership of the work and ownership of the rendering device, one who has legitimate access to a physical book, CD, or DVD, is capable of and has the right to use that work within the bounds of the law. With the DRM distributed content we examined, however, the choice to separate license files from content files may in some cases prevent content from being rendered when accompanying license files are missing. In addition to producing a weak approximation of normative content portability, this design shifts authentication to determine usage rights from content itself to users or hardware owned by users. In performing user and hardware authentication, services are able to collect a host of incidental information, which may be used for profiling or other troubling purposes.

Finally, because DRM systems allow their owners to exercise nearly limitless post-distribution control over works, DRM using companies may feel compelled to extend traditional revenue streams, to create new ones, and to acclimate users to new business models [20]. For example, the music services examined impose costs [j1]not only at the time of purchase, but also at incremental points of product use. This business model, unlike traditional retail or rental business models, is enabled through DRM enforcement mechanisms [25]. The privacy implications of DRM applications, particularly given the absence of distribution intermediaries, weigh heavily against expectations of personal use.

Two consequences may precipitate from these restrictions which individuals are not used to. Content purchasers may fail to find compelling reason to buy Internet distributed music and movies. This is certainly plausible given that online music and movies are priced similarly to their physical world analogues, yet, less valuable to consumers due to unique restrictions over use. A perhaps more insidious possibility suggests that if DRM protected content distribution systems reach a threshold of ubiquity, consumer expectations of what uses they may make, and with what level of anonymity and privacy, with content will begin to change. Music and movies users may not like limitations on the portability of content they own, but if no comparable alternatives exist, those individuals may be forced to adjust their normative behaviors and expectations [40].

5. SUGGESTIONS

The DRM systems that we studied use broad restrictions to enforce copyright holders' control over content. Whether DRM systems are capable of limiting the capacity of individuals to make pirated uses of works is an open question [10]. However, through the restrictions they impose, a host of acceptable personal, non-regulated, and fair uses allotted under copyright law are crippled. We believe that all aspects of the current result are not inherent in DRM design, rather there are a profusion of decision points where DRM architects can choose to support personal use and as a result design products more responsive to the balance of copyright law.

---

[26] When purchasing content distributed using physical media, there is a single transaction point at which information about the purchaser maybe collected. When it is, the collection of that information is usually clear since it must be done in person and requires action from the purchaser. Although discovering how information collected will be used subsequently requires investigation of the collecting entity's policies, there is almost always a single policy and its terms, if understood, are generally sufficient to explain the entire context of data use.

[27] A few terms in the vocabulary include: AllowBackupRestore; AllowBurnToCD; AllowPlayOnPC; AllowSaveStreamProtected; AllowTransferToNonSDMI; and AllowTransferToSDMI.

5.1 Allow transfer of rights

The sine qua non of effective DRM technology, from a copyright owner's perspective, is control over the number of usable copies of a work. The willingness of copyright owners to offer their works over the Internet is a sign that automated DRM control over the number of copies has become acceptably reliable. One step toward better alignment with personal use expectations and copyright law might be for copyright owners to offer subscribers the ability to share a restricted copy of a work with other people. Online distribution services currently enforce continuing relationships with their clients, which could provide a basis for allowing consumers to lend a copy of a work to another person. One possible implementation would be for online music services—or even subscribers—to issue licenses to a third party (not necessarily also a subscriber) on the condition that the subscriber would be unable to use that resource while it was being borrowed. Another implementation might involve combining license with content files so that rendering permissions are inherent with possession of a file. This might be accomplished by making each content file unique and requiring registration with a content server before rendering to enforce the requirement that only one user can use each file at a time.

In addition to lending, allowing users to transfer privileges to third parties or third machines would also give owners of works and subscribers to services portable access to their own accounts. Furthermore, enabling such a use would provide individuals with better capability to share content with friends and family members according to their right of non-public, "private" performance. To maximize the relation of this "sharing" to norms of sharing, the transfer of privileges should be enabled in a manner that preserved the anonymity of the borrower.

Permitting file lending could be performed in a way consistent with DRM's piracy prevention goals. The notion of massive numbers of strangers sharing a single account or collection of files to illicitly satisfy their music needs seems implausible given that simultaneous access to accounts or files is restricted. Although allowing file sharing would require new DRM designs, allowing account sharing would be relatively easy to implement. Account sharing is technologically feasible already with each of the services that we examined. Thus a change in contractual terms of use would sufficiently enable portability resembling that of physical media in this respect.

5.2 Don't limit copying of individual tracks

Removing restrictions on the frequency of CD burning for individual tracks would also better accord with personal use. iTune's Music Store has developed an attempt at balancing personal use with piracy risks in this respect by limiting the number of times specific playlists may be burned to CD but not imposing a similar restriction upon individual music tracks. Although this still falls short of the physical world analog--individuals have personal use rights to replicate songs in set playlists without an equivalent frequency limitation--this system of piracy protection is certainly some degree closer to consumer expectation than outright deactivation of burning capability for tracks after one or two CDs have been created[28].

An alternative anti-piracy rule could limit the number of copies of individual tracks that rendering software will produce within a set period of time. Another rule could require authenticated user presence during the creation of each CD. These two requirements would recreate some of the time and energy costs associated with duplication of physical CDs and videocassettes.[29] DRM has gained popularity as a form of digital access control largely in response to reductions in barriers to content piracy. Artificially reinstalling some of those time and energy costs might alleviate piracy concerns to an extent.

5.3 Allow excerpting and modification

Content excerpting and modification are legally more complex than portability and copy restriction. Transformation and excerpting from content are fair use exceptions to copyright law and, thus, defined by a set of vague contextual factors inherently difficult to incorporate into deterministic DRM designs. Despite the lack of legal clarity concerning these uses, the extent to which allowing excerpting and modification within reasonable limits would more closely emulate what individuals are accustomed to and expect is more certain. If DRM architects and system designer choose to accommodate this expectation, they could develop APIs to help rendering software developers create applications capable of modifying and excerpting from content in a way secure for copyright holders. DRM designers could install requirements that the creation of these subsequent samples and transformations themselves be "rewrapped" in DRM encoding. Such requirements would provide a level of security for these files similar to that of the originals, and help to ensure copyright holders' continued confidence in DRM systems that allow these functions.

To the extent an excerpt is protected as fair use, there are no independent limitations on the ongoing use of the media containing the excerpt. In other words, a fair use excerpt is not subject to limitations on copying and playback. To emulate this norm, DRM designers might consider not subjecting excerpts to time, copy, and playback limitations regardless of the rules controlling the original works from which they are derived. This could be done in a way protective of content markets by defining a maximum excerpt size, limiting the rate of excerpt creation, and preventing the combination of excerpts to reform a whole. Since, DRM designers control what software may decode and render DRM protected content, they are in a position to apply novel requirements in addition to providing novel functionality. Creating maximum excerpt file sizes would prevent the creation of overly long samples which might substitute for original works. Limiting the rate of excerpt creation would make excessive piracy-motivated

---

[28] MusicNet allows two CDs. Rhapsody allows one CD. See Appendix A.

[29] Many advocates would object to the imposition of such time and energy costs, however the authors believe such a change would be qualitatively better than what is currently available to consumers and suggest it on that basis regardless of the broader concern.

excerpt creation economically unattractive. To prevent recombination of excerpts to form whole works, DRM designers could require that rendering software not play consecutive excerpts back-to-back, or only allow back-to-back rendering with a set period of intermittent delay.

In law, excerpting is deliberately regulated using the sensitive context-based requirements which define fair use. Coding maximum sizes for excerpts, limits on the rate of excerpt creation, and delays for playback of consecutive excerpts into DRM systems would mark a fundamental change from this vague and circumstance-dependant nature of excerpting created by law. Despite this, the usage rules currently enforced by DRM reconstruct a fundamentally distorted brand of personal use. Thus the rules we suggest have the potential to make the systems that adopt them more supportive of personal use, if still a crabbed approximation.

Beyond these specific personal-use respecting suggestions, DRM system service contracts are an appropriate place to clarify rights and duties that are not readily reified with machine-enforced rules, and to reinforce individual use rights and expectations. Service providers can use contracts and license agreements to build-in context sensitivity to usage scenarios. This could help reconcile the shortcomings of cookie-cutter rights architectures by providing an outlet for limitations to expressed restrictions.

5.4 Promote User Privacy

By gathering data from consumers incidental to DRM transactions, businesses interfere with the privacy norms and expectations regarding the post-purchase use of content and derive benefit that is not reciprocated. The DRM systems we examined engage in detailed surveillance of content consumption by consumers within private spaces. In most instances the systems monitor the content used, the time of use, the frequency of use, and the location of use. The services both limit what consumers can do in the confines of their own home, or the equivalent, and create detailed reports about use of digital works. In addition to monitoring and reporting by the service itself, there are multiple third parties who monitor and collect data about individuals' use of the site. These entities are not well disclosed, and discovering their identities and use of the data requires detailed reading of privacy policies.

The monitoring and data collection practices of Internet content distribution services raise troubling privacy concerns, and also create opportunities to police and limit behavior occurring in private spaces. Absent legal protections, the design of DRM and the terms of service and contract provisions crafted by Internet content services are the primary forces determining the scope of intellectual privacy available online.

As others have noted, Fair Information Practice Principles, particularly collection limitation, disaggregation of identifying and transactional data, and data destruction should inform the design and implementation of all aspects of DRM [54]. In particular, DRM system developers should eschew the collection of data that is not absolutely necessary to protect content. For example, in the services we examined data was routinely collected about the number of times purchased or licenses tracks are played; browsing behavior; burning; and where it was permitted efforts at portability. The connection of this data to copyright enforcement or copyright holder remuneration is unclear.

Where data is needed to protect content then segregating usage data from identifying or subscriber data is important – even if it can be reconnected later on. Where possible data should be fully anonomyized by default soon after collection. When the justification for collecting information no longer holds, it should be destroyed.

Additional data collection by the service and any data collection by third parties should at a minimum require the opt-in consent of consumers, not be a condition of service use, and offer more convenient and customized services, such as one-click shopping or film and music recommendations.

In all cases users should be notified that data collection is taking place, and of what uses collected data is being put to after it is gathered. Consumers are unlikely to be able to engage in anonymous transactions with DRM-based services anytime soon, but these services could go further to assure their customers that their intellectual preferences will not be recorded and therefore subject to misuse or misappropriation. Such steps would be consistent with the privacy norms and expectations surrounding intellectual preferences developed in other areas and build consumer confidence in DRM protected content distribution.

DRM systems used to protect content might be more reasonable if they are not also applied to support business model changes unrelated to copyright interests. Customers may misconceive that incremental payments for content portability and continual reacquisition of digital licenses are somehow necessary for enforcement of content rights. If content services choose to change their business models, they should not leverage any DRM enabled advantage without explaining the change to potential customers. Such openness would give consumers a fair opportunity to compare those services with their physical media counterparts and to make educated purchasing decisions.

6. CONCLUSION

The DRM protected environment for content use does not resemble that which copyright law strives to set, nor that which we as consumers have come to expect. Personal and fair uses have become handicapped. The DRM systems studied require and enforce ongoing relationships between users and service providers extracting personally identifiable information during service registration, content purchase, license upgrades, and rendering of content. The systems do not provide basic functionality necessary for users to engage in normal personal uses such as sharing and "time" and "space" shifting. Technologists, policy makers, and the public alike should note these trends, and their departure from copyright law and individuals' expectations of personal use of legally acquired copyrighted works.

6. ACKNOWLEDGMENTS

Our thanks to Professor Pamela Samuelson for insightful editing remarks and commentary.

7. REFERENCES

[1] 17 U.S.C. § 109(b)(1)(A).

[2] 17 U.S.C. § 1201(a)(1)(A) (2003).

[3] 17 U.S.C. § 1201(a)(3)(B) (2003) (defining a "technological measure" that "effectively controls access to a work").

[4] 18 U.S.C. § 1030(a)(5)(B)(i) (2003).

[5] 18 U.S.C. § 1030(g) (2003).

[6] 18 U.S.C. § 2710.

[7] 18 U.S.C. § 2710(a)(4).

[8] 18 U.S.C. § 2710(b)(2).

[9] 18 U.S.C. § 2710(e).

[10] Peter Biddle, Paul England, Marcus Peinado, Bryan Willman, *The Darknet and the Future of Content Distribution*, in PROCEEDINGS OF 2002 ACM DRM WORKSHOP. Available at < http://crypto.stanford.edu/DRM2002/darknet5.doc>.

[11] Dan L. Burk & Julie E. Cohen, Fair Use Infrastructure for Rights Management Systems, 15 HARV. J.L. & TECH. 41 (2001).

[12] CinemaNow Privacy Statement. *See* <http://www.cinemanow.com/about/privacy.asp>.

[13] CinemaNow Terms of Use. *See* <http://www.cinemanow.com/about/terms_of_use.asp>.

[14] Julie E. Cohen, *DRM and Privacy*, 46 COMMUNICATIONS OF THE ACM 47 (April 2003).

[15] Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998) (criticizing assertions of the fairness and efficiency in DRM systems).

[16] Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma: Intellectual Property in the Information Age*, National Academy of Science (2000), 133-135.

[17] Digital Consumer List of Users' Rights. *See* <http://www.digitalconsumer.org/bill.html>.

[18] *EF Cultural Travel BV v. Zefer Corp*., 318 F.3d 58, 63 (1st Cir. 2003) (suggesting that passwords

implicitly limit "authorized access" to the holder of the account to which the password is assigned).

[19] *EF Travel v. Explorica*, 274 F.3d 577 (1st Cir. 2001).

[20] Electronic Privacy Information Center, *Digital Rights Management and Privacy*. *See* <http://www.epic.org/privacy/drm/>.

[21] John S. Erickson, *Fair Use, DRM, and Trusted Computing*, 46 COMMUNICATIONS OF THE ACM 34 (April 2003).

[22] The Ethereal Network Analyzer. *See* <http://www.ethereal.com/>.

[23] Edward W. Felten, *A Skeptical View of DRM and Fair Use*, 46 COMMUNICATIONS OF THE ACM 57 (April 2003).

[24] Barbara L. Fox & Brian L. LaMacchia, *Encouraging Recognition of Fair Use in DRM Systems*, 46 COMMUNICATIONS OF THE ACM 61 (April 2003).

[25] I. Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217.

[26] Jon Healy, *Faster Than the Speed of Software; The record labels have a new idea for selling music online. The only catch: This time, they are ahead of the technology needed for it to happen*, L.A. TIMES, Part 3; Page 1 (Apr. 27, 2003).

[27] Mark A. Lemley, *"Beyond Preemption: The Law and Policy of Intellectual Property Licensing,"* 87 Cal. L. Rev. 111 (1999).

[28] Lawrence Lessig, *Code and Other Laws of Cyberspace*, 135-136, Basic Books, NY, 2000.

[29] Jessica Litman, *Symposium: Copyright Law as Communications Policy: Convergence of Paradigms and Cultures: War Stories*, 20 Cardozo Arts & Entertainment L.J. 337, 338-339 (2002) (discussing Congress' unwillingness to define personal use but willingness to protect consumers from liability for specific non-commercial uses)

[30] Michael J. Meurer, *Focus on Cyberlaw: Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works*, 45 Buffalo L. Rev. 845, 859 (1997) (noting that personal use rights are not precisely defined and that none result in competition with the copyright holder).

[31] *MGM Studios, Inc. v. Grokster, Ltd*., 259 F. Supp. 2d 1029, 1038 (C.D. Cal. 2003) ("Grokster is of course aware as a general matter that some of its users are infringing copyrights.") (internal quotation and citation omitted).

[32] Movielink Privacy Policy. *See* <http://www.movielink.com/commerce/help/privacy.jhtml>.

[33] Deirdre K. Mulligan & Aaron J. Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, in PROCEEDINGS OF 2002 ACM DRM WORKSHOP. Available at <http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc>.

[34] Ryan Naraine, *Pressplay Goes Unlimited, Rhapsody Does DirectTV*, InternetNews.com, (August 1, 2002). *See* <http://www.internetnews.com/bus-news/article.php/1437451>.

[35] Patrick Norton, *Convert Windows Media to WAV*, TechTV (November 14, 2001). *See* <http://www.techtv.com/screensavers/answerstips/story/0,24330,3337090,00.html>.

[36] Pressplay Terms of Service. *See* <http://www.pressplay.com/terms.html>.

[37] Real Networks, *Realnetworks Launches Realone Rhapsody Music Subscription Service*, 2003 Press Releases. *See* <http://www.realnetworks.com/company/press/releases/2003/rhapsody.html>.

[38] *Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.*, 180 F.3d 1072 (9th Cir. 1999) (holding that Rio, a portable digital device for playing MP3 files, makes

copies to enable portability, or “space-shift[ing] which is a paradigmatic fair use").

[39] Reuters, *New Deals from MusicNet Quintet*, November 14, 2002. *See* <http://news.com.com/2102-1023-965928.html>.

[40] Pamela Samuelson, *DRM {and, or vs.} the Law*, 46 COMMUNICATIONS OF THE ACM 41, 42 (April 2003), 44. Available at <http://www.sims.berkeley.edu/~pam/papers/acm_v46_p41.pdf>.

[41] Michael Singer, *Apple's Making Serious Music*, InternetNews.com (April 28, 2003). *See* <http://siliconvalley.internet.com/news/article.php/2197271>.

[42] Snort: The Open Source Network Intrusion Detection System. *See* <http://www.snort.org/.>.

[43] *Sony Corp. of America v. Universal City Studio*, 464 U.S. 417, 455, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984) (holding that “time-shifting” of copyrighted television shows with VCR's is fair use).

[44] System Internals Freeware, Filemon for Windows. *See* <http://www.sysinternals.com/ntw2k/source/filemon.shtml>.

[45] Texas Penal Code § 31.04(a)(1) (providing that a “person commits theft of service if, with intent to avoid payment for service that he knows is provided only for compensation . . . he intentionally or knowingly secures performance of the service by deception, threat, or false token.”).

[46] Deborah Tussey, *From Fan Site to Filesharing: Personal Use in Cyberspace*, 35 Ga. L. Rev. 1129, 1143-44 (2001) (discussing the overlap between fair use and personal use but noting that many commonly engaged in personal uses have never been labeled “fair” by the courts and may well not be if presented).

[47] *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001). (This interpretation may clash with the intent of Congress to make “circumvention of copy- and use-controls . . . lawful when performed for noninfringing purposes, such as to enable fair uses.”).

[48] *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (affirmed on appeal under the name *Universal City Studios v. Corley*)

[49] *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991).

[50] Hal Varian, Carl Shapiro, *Information Rules*, Harvard Business School Press, Boston, Massachusetts, 97-98.

[51] Windows Media Player for Windows XP Privacy Statement. *See* <http://www.microsoft.com/windows/windowsmedia/software/v8/privacy.aspx>.

[52] Todd Woody, *The Race to Kill Kazaa*, Wired Magazine Issue 11.02 (February 2003). Available at <http://www.wired.com/wired/archive/11.02/kazaa_pr.html>.

[53] Pressplay Privacy Policy. *See* <http://www.pressplay.com/privacypolicy.html>.

[54] Feigenbaum, J., Freedman, M., Sander, T., and Shostack, A., *Privacy Engineering for Digital Rights Management Systems*, In Proceedings of the 2001 ACM Workshop on Security and Privacy in Digital Rights Management. Springer-Verlag. Berlin (2002).

Appendix A: Summary of permissions granted by various services