

A Framework for Evaluating Digital Rights Management Proposals

Rachna Dhamija
UC Berkeley, SIMS
rachna@sims.berkeley.edu

Fredrik Wallenberg
UC Berkeley, SIMS
fredrik@sims.berkeley.edu

Abstract

In this paper, we analyze the strengths and weaknesses of the various solutions to compensate intellectual property rights holders. Specifically we look at digital rights management (DRM) based systems, extensions to DRM to support fair uses, monitor-and-charge schemes, compulsory licensing schemes and alternative business models.

Our main contribution is to provide a framework from which current and future proposals may be evaluated. In order to realistically evaluate any compensation scheme, we suggest that the following questions are important to ask:

- *Is the proposal technically feasible?*
- *What are the incentives to circumvent legal and technical protections for all parties in the transaction?*
- *What is the burden of monitoring for compliance in the system, and on which parties does this burden fall?*
- *What is the efficiency of the collection and distribution of funds from consumers to rights holders?*
- *What are the impacts on user privacy and fair use?*
- *What is the feasibility of legal enforcement, both domestically and internationally?*

1. Introduction

Over the last few years the debate over protection, or lack thereof, of copyrighted works has flourished. Proposals on how to reimburse the creators of these works range from strict proprietary encryption locks to new business models that rely on revenue streams from ancillary products. Each new proposal points out the shortcomings of previous schemes and highlights the benefits of its own solution. However, no consistent framework exists for analyzing the different solutions.

In this paper, we analyze the strengths and weaknesses of the various solutions. Specifically, we look at DRM based systems, extensions to DRM to support fair uses, monitor-and-charge schemes, compulsory licensing schemes and alternative business models. From this comparison, we extract important dimensions such as technical feasibility, incentives to cheat, burden of monitoring, privacy, and the feasi-

bility of legal enforcement. Our main contribution is to provide a framework from which current and future proposal may be evaluated.

Digital Information as a “Public Good” Economists sometimes refer to certain goods as *public*. This does not imply that they are in the public domain as defined by intellectual property law. Rather, a public good is a product or service that has two properties. First, it is *non-rival*, which simply means that consumption by one person doesn’t limit consumption of the next. Second, it is *non-excludable*, implying that once the product exists, the benefit cannot be limited to those that have paid for it.

Ideas and information captured in physical media traditionally fall into some middle ground. While the information itself certainly has the characteristics of a public good, the physical media that it is tied to is rival and excludable. This gives rise to business models involving the sale of physical artifacts whose only value is the embedded information such as books, CDs and DVDs. These business models have taken a serious blow with the introduction of information in digital form combined with communications media such as the Internet. The question at hand is whether or not it is possible to devise a scheme under which money can be transferred from those consuming information goods to the providers of the same.

We use the characteristics of a public good to distinguish between the following classes of proposals to compensate intellectual property rights holders:

- The first approach is to make the product rival. Solutions in this category use DRM copy protection to make sharing of information goods hard (or impossible).
- The second approach is to make the product excludable. This includes watermarking schemes that allow owners to monitor who is using the product in order to charge for its use and to pursue those who don’t pay.
- A final approach is to accept that a product is a public good that is non-rival and non-excludable. This cate-

gory of solutions relies on financing through a general collection system (such as levy or tax schemes) or on revenues from alternative business models and voluntary contributions.

The three classes of solutions present different challenges from the standpoint of incentive compatibility. They also differ with respect to cost and enforceability, and who bears the burden of each.

For example, DRM systems that artificially make a product either excludable or rival invite circumvention activities by end users (who realize that, if they could remove the technical barriers, the product is neither excludable nor rival). In compulsory licensing schemes, which tax users independently of their actual consumption, there is less incentive for users to cheat. However this scheme invites another problem. If the disbursement of funds to rights holders is based on the observed consumption of their products, rights holders now have a strong incentive to bias the observed traffic in their favor. With either solution, there is one party that will have to be monitored for cheating unless technical barriers are put in place that cannot be circumvented, an unrealistic assumption.

In section 2, we summarize the general and specific proposals that have been made for compensating rights holders. In section 3, we analyze how the different solutions fare in areas such as technical feasibility, incentives to cheat, burden of monitoring, efficiency, privacy and fair use. Finally, we present our conclusions in section 4.

2. Proposed Solutions

2.1. Creating Rival Goods

Traditional DRM Digital rights management (DRM) systems aim at protecting ownership and copyright of electronic content by restricting what actions an authorized recipient may take with respect to that content. In traditional DRM systems, content is distributed in protected form and relies on a compliant device or secure execution environment to allow the user to make use of the work. In these schemes, the content may be protected through encryption (as is the case with the DVD Copy Control Association Content Scrambling System¹ and cable and satellite transmissions) or through labeling (as is the case with Macrovision²) and the Digital Television Broadcast flag [1]. In permissions-based systems, the encrypted content is delivered with a machine-readable license, which specifies the license terms and specific permissions for which a user is au-

¹<http://www.dvdcca.org/css/>

²<http://www.macrovision.com/>

thorized to make use of the work (as is the case with eBooks and many audio and video players). For examples, see the Windows Media DRM³, the RealNetwork Helix DRM⁴ and the Apple FairPlay DRM⁵.

DRM Extension Proposals One of the strongest criticisms of DRM systems has been their inflexibility in allowing end users to make *fair uses* of works. U.S. Copyright laws give copyright owners the right to prohibit others from making some uses of the work, such as copying, distributing or making a derivative work. However, there are many exceptions to this rule that allow users to legally make further uses of the work, even when such uses are not authorized by the copyright owner (for example, the ability to make private backups, or the ability to make excerpts for commentary or criticism). The term fair use strictly refers to the four factor test given in 17 U.S.C. §107. Here, we use the term more loosely to refer to other exceptions that apply to copyright, e.g., Special Rules for Libraries and Archives (17 U.S.C. §108), narrow exemptions (17 U.S.C. §110), first sale rights, term expiration, public domain, privileges for reverse engineering and backup of computer programs.

In their “Fair Use Infrastructure” proposal, Burk and Cohen examine how fair use can be retained under a DRM system that provides strict access control [2]. The proposal has two components. First they suggest that there is a subset of all possible cases of fair uses that can be well-described and encoded as automatic defaults into DRM systems. For the cases of fair use that cannot be easily encoded in this way, the authors propose that users could make a request for access to the work with a trusted third party. The third party is responsible for determining if the requested use falls under fair use, and if so, it is able to grant access to the encrypted work via a key escrow system (in which keys to decrypt works are deposited by copyright holders).

Mulligan and Burstein propose modifications to Rights Expression Languages (REL), i.e., XrML, in order to better support fair uses [3]. They argue that REL syntax and vocabulary should enable rights holders to express license terms in a way that more closely matches copyright law. Specifically, rights holders should be able to express fair use exceptions, as clearly and easily as they are able to express restrictions on the use of a work. Furthermore, they propose that DRM systems should be designed so that all parties in a rights transaction (both the rights holders and end users, for example) can express their rights through REL. Erick-

³<http://www.microsoft.com/windows/windowsmedia/drm.aspx>

⁴<http://www.realnetworks.com/products/drm/>

⁵http://www.info.apple.com/usen/musicstore/musicstore.html?topic=music_authorization

son proposes a DRM architecture in the same vein [4]. In his model, users can make rights requests (such as a fair use request) to a third-party licensing authority. Like the other proposals in this section, he argues that a third party licensing authority will be more impartial than the rights holders in deciding whether to grant a use request. Also, like Burk & Cohen, his solution to achieve a closer approximation to fair use depends upon giving users the opportunity to engage in a rights negotiation with rights holders.

2.2. Creating Excludable Goods

In order to provide monitoring and tracking, some DRM schemes rely on watermarking, which embeds a visible or invisible mark in content such as audio, images and computer software. Fingerprinting is similar in concept and usually refers to embedding a unique serial number in content (as opposed to general copyright information). Fingerprinting can also involve the extraction of unique features from a particular piece of work in order to identify it.

There are a number of examples of the use of ex-post monitoring by copyright holders to detect unauthorized uses of their work. For example, some companies have proposed an automatic system to detect unauthorized distribution of images that consists of a watermarking scheme and a web crawler that downloads pictures to check if they contain the watermark (for example see Digimarc MarcSpider⁶ image tracking). In their attempts to stifle piracy, the music and motion picture industries are using the services of third parties such as BayTSP⁷ and Ranger Online⁸ to track down infringing copies without the need for a-priori watermarking. BayTSP claims to have detected 10,000 infringements with a 95% compliance and removal rate resulting from take-down notifications.

In his “ISPs as Digital Retailers” scheme, Sobel proposes to use watermarking and fingerprinting techniques, not only to find copies of work but also to charge consumers directly. In Sobel’s proposal, ISPs can license content from copyright holders at wholesale prices and then re-sell the content to their customers, with whom they have an established billing relationship [5]. He suggests that digital fingerprinting (and/or watermarking) could be used by the ISPs to monitor the flow of copyrighted materials over their networks. In order to ensure that the transaction costs associated with negotiation are minimized, the author proposes a statutory license that forces the copyright owner to provide a license, however, it does not regulate the prices that copyright holders may charge.

⁶<http://www.digimarc.com>

⁷<http://www.baytsp.com>

⁸<http://www.rangerinc.com>

2.3. Public Goods

Even among those who agree that digital information should be treated as a public good, there is a wide discrepancy in the solutions proposed with respect to government regulation. At one end of the spectrum, we have proposals that rely on legal intervention, typically in the form of compulsory licensing schemes. At the other end, we have abolitionists who suggest that doing away with intellectual property rights will best allow market solutions to flourish.

Compulsory Licensing One conclusion of accepting that digital information goods have the characteristics of public goods is that creation needs to be subsidized through compulsory licensing policies. In this case, the rights holders are required to license their works at a set rate and under certain conditions. One way to characterize the problem is how to “collect a pool of money from Internet users, and agree on a fair way to divide it among the artists and copyright owners” [6]. In this paper, we use the term “compulsory licensing” as von Lohmann does, to refer to the taxation model that is commonly used for public goods. However, other compulsory licensing models are possible, see for example the Music Online Competition Act of 2001⁹ and U.S. Copyright Office’s Copyright Arbitration Royalty Panel¹⁰.

Specific compulsory licensing proposals, such as those by Netanel and Fisher, suggest that the money should be collected based on consumption of devices (such as CD and DVD burners), media (blank CDs and DVDs) and services (such as ISP access) [7, 8]. The efficiency of any collection scheme will depend on how close the consumption of products and services that are taxed is to that of the digital goods that are consumed. Funds raised in this manner would then have to be disbursed to the rights holders based on some approximation of the use of their respective products.

Netanel’s Non-Commercial Use Levy (NUL) proposal builds upon the basic concept of compulsory licensing by specifying that the license should only be for non-commercial use and should not include all forms of digital goods [7]. Specifically he intends the model to cover “literary works” that are not primarily tools. That is, he expects creative content such as music, movies, text and graphics to be covered, but not computer programs.

To refine the collection mechanism, he proposes that the levy should be imposed upon “commercial providers of all consumer products and services the value of which . . . P2P file sharing substantially enhances” [7, page 32]. He further proposes that the NUL should strive to raise as much money as the sales supplanted by P2P sharing.

⁹<http://www.house.gov/boucher/moca-page.htm>

¹⁰<http://www.copyright.gov/carp/>

While the remuneration should ideally be tied closely with the users' aggregate private value of the goods, Netanel acknowledges that such monitoring would imply high transaction costs and privacy costs. He suggests that metering of downloads, streams and uses should be done both at the ISP level and, in some cases, on user devices and be supported by digital fingerprinting and sampling techniques.

Fisher proposes that we replace the current copyright model with a government administered reward system [8]. In order for creators to collect revenue under this system, they are required to register with the copyright office and will receive a unique filename in return (that would allow the work to be tracked). Similar to Netanel, Fisher proposes that the government put a tax on devices and services that are used to access digital entertainment.

The distribution would be determined through the analysis of a number of metrics including surveys and usage data provided by file sharing systems, such as KaZaa. Fisher also recognizes that the amount of compensation needs to differ depending on the type of good, thus the fact that both a new Britney Spears song and the recent Spielberg movie have the same "market share" doesn't mean that they should receive the same remuneration.

Alternate Business Models Boldrin and Levine, among others, believe that copyright (or other intellectual property rights) is unnecessary in order to stimulate the creation of information goods [9]. There have been many calls for the development of new business models that don't require control of the content per se, but where the revenue comes from excludable actions such as showing a movie in a full size theatre or giving live concerts. Further, just as the content drives demand for "performances", it may also provide room for merchandising. However, a number of artists have expressed skepticism about such ancillary revenue streams [10].

Finally there are those that suggest that voluntary payments may work. There are plenty of examples within the shareware industry of products that are made available for free (without any limitations on functionality) and of "contributions" that are sufficient enough to support the developers. Yet, there are examples where the "tips" were insufficient to pay for the development of the product. For example, Stephen King's novel *The Plant* was originally offered under the "tip model" but the model failed to raise sufficient revenue and the book was withdrawn [11].

As an enabler for alternative business models, Creative Commons licenses can be used by authors to indicate that their copyrighted works can be copied and distributed, usually under certain conditions (for example, only with attribution, or only for non-commercial use). Related efforts are

The Free Software Foundation's General Public License for software licenses and the Electronic Frontier Foundation's Open Audio License for digital sound recordings.

3. Discussion

In this section, we compare and contrast the proposals for compensating rights holders along the following dimensions: technical feasibility, incentives to cheat, burden of monitoring, efficiency of collection and distribution of funds, privacy, fair use, feasibility of legal enforcement and flexibility.

Technical Feasibility A number of security researchers have commented on the technical futility of copy protection and DRM [12, 13, 14]. One cryptographer has stated that DRM approaches will never be successful because "all digital copy protection schemes can be broken and, once they are the breaks will be distributed" [12]. Other security researchers are more optimistic that DRM models can have more success by focusing on risk management and the ability to adapt to security compromises [15].

All of the attacks that traditional DRM system are vulnerable to also apply to the DRM extension proposals. While the DRM extension proposals aim to provide better support for fair use, they acknowledge that it is impossible to create a DRM system that will allow all fair uses. A fundamental technical challenge is how to create exceptions that are flexible enough to allow legitimate fair uses, but not so flexible that they can be exploited as loopholes by infringers.

The centralized key escrow scheme proposed by Burk & Cohen would be an enormous technical undertaking. Many of the technical criticisms of key escrow systems in general also apply to this proposal [16]. For example, a centralized key repository creates a very high value target and introduces many new vulnerabilities and threats regarding the improper disclosure of keys. Due to the large number of users and copyrighted works, such a system would be extraordinarily complex to administer and extremely costly to implement.

Sobel's monitoring and charging scheme is also infeasible to implement securely. It is simply too easy for users to alter digital fingerprints and watermarks, especially given that they have a strong incentive to do so. For example, users may easily be able to remove the mark, or to place a watermark from one work into another [17, 18, 19]. Another simple attack is for users to encrypt their files to prevent detection of the watermark. It would be difficult (or impossible) for the ISP to differentiate between legitimately encrypted content and encrypted copyrighted content without banning

encryption entirely.

The main technical challenge in the compulsory licensing schemes is how to track digital copies of content. Fisher suggests two approaches to tackle this problem [8, Ch. 6, p.6]. The first is for the creators to imbed digital watermarks into copies of their work, which could then be tracked and replicated in each copy of the original work. Unfortunately, as discussed above, the watermarking approach is subject to a number of attacks that may make such a plan infeasible.

Fisher's second approach relies upon the existence of a centralized registration system, which would require artists to register their work in exchange for a unique serial number for that work. Again, Fisher does not provide any details for how the serial number would be tracked. One possibility is to embed the serial number as a watermark, but this is subject to the problems discussed above. Any centralized registration service of this type will be an enormous technical undertaking.

Even if watermarking systems were impossible to defeat, both the monitor-and-charge schemes and the compulsory licensing schemes are subject to "distributed" cheating attacks, where the consumption of a good is artificially inflated across a large number of (real or illegitimate) users. These types of attacks are challenging to detect, and any usage monitoring or sampling scheme must be designed with this in mind.

Incentives to Cheat DRM schemes that tie payment directly to consumption inherently give users a larger incentive to circumvent copy-protection or monitoring devices in order to avoid payment. Also, onerous security restrictions on DRM-wrapped content make compliance less attractive, given the availability of unrestricted content [20]. DRM schemes that allow a certain threshold of private use copying may be perceived as more "fair" and may therefore enjoy wider adoption and higher compliance rates. Apple's recently announced Fairplay DRM allows more private use copies to be made compared to other DRM schemes [21].

DRM extension proposals, such as those proposed by Mulligan & Burstein and Erickson, may increase user compliance, because users are now able to engage in fair use without circumvention. In the Burk & Cohen model, the incentive for the users to comply is that those who fail to obtain access via the escrow agent would be subject to prosecution for circumventing technical measures. Under Burk & Cohen the incentive for rights holders to deposit keys with the escrow agent is that they would otherwise be unable to invoke legal protection against circumvention. If they choose not to escrow their works, users would be given a "right to hack" as a substitute for access to the work via escrow keys. One problem with these proposals is that rights

holders currently have no economic incentive to express fair use terms or to allow user negotiation in DRM enforced licenses, as proposed by Mulligan & Burstein and Erickson, absent a change in the law [22].

In a monitor-and-charge model, such as that proposed by Sobel, users have the incentive to under-report consumption to avoid payment. Irreputable rights holders also have an incentive to push unrequested information to the user to increase their revenue. In fact, spammers could potentially construe their spam as copyrighted material and be paid for it.

In compulsory licensing schemes, which tax users independently of their actual consumption, there is less incentive for users to cheat (users may still have an incentive to skew the reporting, either because they would like to favor certain artists or because they are concerned about the tracking of their specific consumption.) This is one of the prime motivators for any compulsory licensing scheme as outlined in section 2.3. Fisher recognizes that, under these types of schemes, it is now rights holders that have the incentive to cheat, or engage in "ballot stuffing." This ballot stuffing is very similar to the spamming problem that monitor-and-charge schemes are subject to. However, in the compulsory license case, cheating will be more challenging to detect since end users are not being directly charged and therefore have less incentive to complain about products they have not consumed. As discussed above, cheating that artificially inflates the consumption of a good over a large number of (real or illegitimate) users, will be hard to detect in both schemes.

Burden of Monitoring Under DRM-based systems, the burden of monitoring user compliance falls on the rights holders.

In the monitor-and-charge environment, as proposed by Sobel, the monitoring burden falls on the ISP. The Sobel proposal correctly identifies that the ISP is in the best position to monitor individual users [23]. What the author fails to acknowledge is that the ability to successfully monitor depends on the effectiveness of the tracking mechanism (which isn't very effective) and the user's incentive to circumvent the protection (which is high). The security responsibility for the former falls entirely on the shoulders of the rights holders who insert the watermarks. The incentive for users to cheat will depend on price and usage restrictions, both of which are also determined by the rights holder. With that in mind it isn't surprising that the ISPs are less than thrilled about the proposal. Furthermore, while ISPs do bill their individual users, the complexity implied by this system (where everyone can be a copyright holder and consumer) would result in "the worlds most complicated billing sys-

tem” (Sarah Deutsch, council for Verizon, at the UC Berkeley Law and Technology of DRM conference in February 2003).¹¹

In compulsory licensing schemes, the burden of monitoring falls on the government to ensure that rights holders do not “game” the system. One concern is that this vests a large amount of power and discretion over creative culture with a government agency. In this case, public monitoring will be critical to ensure that the rules established are fair. For example, what criteria will be used to determine who is authorized to register as a legitimate artist with the copyright office? How do we ensure that organizations, such as RIAA and MPAA, who have large lobbying power, will not tilt such a system to their advantage and to the disadvantage of smaller independent artists? How will the agency respond to the opposition that is sure to arise over the funding of politically unpopular art? For example, The South Carolina House of Representatives passed a bill to renounce the Dixie Chicks for their “unpatriotic” criticism of President G.W. Bush prior to the second Gulf War [24]. As another example, we cite the legal battles that arose over “standards of decency” in government funding of artists by the U.S. National Endowment for the Arts [25].

Efficiency of Collection and Distribution of Funds In the case of DRM-based solutions, the revenue received by the rights holders is a direct function of the value assigned by the users (specifically, we know that the user’s value is at least as high as the price). In the case of a monitor-and-charge system like Sobel’s, the fact that the payment is made well after the decision to consume tends to have an impact on purchasing behavior.

Under compulsory licensing schemes, direct ties between funds collected and true consumption cannot, per definition, be established. The precision of the estimate of what is consumed can be improved by tying the collection of funds to the consumption of (non-public) goods that have a high correlation with the public information good. In this context, Netanel’s proposal fares better than most compulsory licensing schemes, because funds are raised based on levies on (non-public) goods whose values are tightly linked to the digital work.

A further effect of decoupling collection and consumption is that “sales” can no longer be used to determine how funds are disbursed. Rather, some metric must be used to estimate the aggregate value of the consumption of a particular work. When users no longer “vote with their wallets”, even perfect observation of every copy acquired (through downloading or otherwise) is unlikely to yield a perfect es-

timate, because consumption patterns are changed. That is, when the marginal cost is lowered (to near-zero), not only will the users consume more, but the mix will most likely change since the user will consume goods with a value to them lower than the previous cost but higher than the new marginal cost. The further away from the individual actions that the sampling is done (by, for example, monitoring the traffic on the backbone), the worse the precision becomes.

Privacy There is an inherent tension between the goals of DRM copyright-enforcement and the privacy goals of end users. Rights enforcement technologies may compromise user privacy through the restrictions they place on users, by tracking and monitoring users and their usage patterns, and also through the data that is collected by network operators [26, 27, 28].

The DRM extension proposals also present a serious challenge to user privacy by creating a centralized database of user requests for access. The most privacy-optimal solution would fulfill fair use requests (or under Burk & Cohen, release escrow keys to applicants) without retaining any personally identifying records. However in order to prevent abuse and prevent would-be infringers from exploiting such a system, it is likely that records will be kept. The danger is that copyright industries will demand the ability to match keys with identities so that pirated materials can be linked to the suspected infringers. In their proposal, Burk & Cohen recommend that identifying information be released only pursuant to a court order and only on a showing of actual piracy. This issue is currently being tested in U.S. courts. As of this writing, ISPs are required to turn over subscriber information to copyright holders upon “reasonable suspicion of a violation”, a much lower standard than that suggested by the authors. See The U.S. District Court (DC) opinion in RIAA v. Verizon, holding that the issuance of a subpoena by a Clerk of the District Court to obtain the identity of an anonymous peer to peer infringer from his ISP does not violate either the First Amendment of the Constitution, or the justiciability requirements of Article III [29]. Furthermore, Burk & Cohen acknowledge that in any scheme where users must request access, even the most stringent system of privacy protections for fair uses is likely to chill some lawful uses. For more treatment of the chilling effect, see [30, 26].

Under a monitor-and-charge scheme, such as that proposed by Sobel, the impact on privacy should be expected to be much higher than Sobel acknowledges since *all* copyrighted traffic to and from an *identified* user will be monitored. The observations on the chilling effects of monitoring apply here as well.

In general, compulsory licensing models would require less precise monitoring of individual activities than DRM-

¹¹http://mindjack.com/relay/archive/2003_02_01_index.shtml

based or monitor-and-charge models. Even if file usage is monitored at the same level, metering for the purpose of redistribution of funds does not require identification of the end user. Neither Netanel nor Fisher provide any details of their watermarking schemes, if they will embed any personally identifying information, for example. But presumably, such a scheme could depend on aggregate sampling and would not require ISPs or P2P operators to record how much any particular individual has downloaded or uploaded a particular file (however, ISPs and P2P operators could choose to record this data, as it would be commercially valuable). Netanel's approach is more problematic than Fisher's from the perspective of privacy since he, in an effort to improve precision, suggests that usage should be tracked not only on the network (down to the individual user level) but also on the user's devices.

Fair Use The legal definition of what constitutes a fair use is ambiguous in U.S. copyright law, and only a court can determine with authority whether a particular use is a fair use. It is unlikely, therefore, that we will be able to build DRM systems that can reason about what uses are fair in the foreseeable future.

One solution to resolve the tension between rights holders desires for copy controls and users desires to make fair uses is to encode special exception cases of fair use into the DRM system. The exceptions must be broad enough to be useful, but cannot be so broad as to allow infringement to occur. Regardless of how broad the encoded exceptions are, there is always the spectre of future fair uses that have yet to be thought of [31].

All of the DRM extension proposals in section 2.1 enable the introduction of a third party decision maker. The aim is to approximate case-by-case determinations, which cannot be emulated by fair use defaults alone. In particular, the proposal by Burk & Cohen strives to encode some flexibility to handle borderline cases as well as new uses.

Solutions that rely on ex-post monitoring have an inherently better chance of supporting fair uses. The difficulty inherent in Sobel's monitor-and-charge model is that the ISPs must determine which uses are fair use. The likely result would be a very strict interpretation by the ISPs resulting in severe limitations on fair use, because the ISPs would face legal liability for infringing uses and they do not benefit financially from fair use copies.

Compulsory licensing schemes will also inherently more easily allow fair uses to be made. However, one criticism of the compulsory licensing schemes is that the cost that is borne by users will account for all uses, whether they are licensed and authorized uses or whether they are unauthorized fair uses.

Feasibility of Legal Enforcement Even if we can track and identify infringers from a technical standpoint we still have to worry about whether or not we can enforce laws effectively.

Currently, with DRM based systems, there is a very large set of possible entities that the rights holders may pursue when infringement is discovered, including individual users, providers of circumvention tools, operators of file sharing networks and ISPs. Little changes under the monitor-and-charge proposal. However, the rights holder can now prosecute one entity, the ISPs, for failing to enforce copyright laws, and it will be up to the ISPs to pursue everyone else.

The major difference is seen under a compulsory licensing scheme. In this case, the rights holders only have to concern themselves a smaller subset of users that infringe the license, such as unauthorized commercial users under Netanel's NUL. The entity in charge of disbursement of royalties will have to monitor the rights holders, but it benefits from having the means to punish them by virtue of withholding funds [8, Ch.6, p.29]. Penalizing individual users who do not explicitly act on behalf of a rights holder, but are simply trying to distort the system, will be much harder.

Another obvious problem stems from international users (and content). DRM-based systems can function well internationally, however, prosecuting infringing uses in other countries presents a challenge. For example, in the DeCSS case, Jon Johansen was acquitted by Norwegian courts [32]. Similarly, the monitor-and-charge and compulsory licensing schemes only contemplate raising money from U.S. users, without any concern for how foreign users would be induced to pay or how the U.S. would handle payments to foreign entities.

Currently, rights holders are seeking broader legal anti-circumvention legislation in the U.S., European Union and other countries to protect DRM-based business models [33]. It remains to be seen whether rights holders would also seek legislative protection in the case of compulsory licensing (for example, in the form of prohibiting users and network operators from circumventing watermarking schemes).

Flexibility There is another important consideration when choosing a mix of market based solutions and government intervention. In general, government mandated solutions foreclose development of many new solutions. Adopting a compulsory licensing solution will lock us into a specific solution and may halt the evolution of new business models for distributing digital goods.

4. Conclusions

Based on the analysis in the previous section, it is quite clear that there are many tradeoffs to consider when evaluating proposals to compensate intellectual property rights holders. In order to realistically evaluate any compensation scheme, we suggest that the following framework of questions be applied:

- Is the proposal technically feasible? No proposed technical protection measures are strong enough to sustain a determined attack. Only in combination with models where the incentives to circumvent are limited, can technical solutions succeed.
- What is the feasibility of legal enforcement, both domestically and internationally? It is easy for researchers and market actors to forget that a solution that requires significant government intervention and enforcement is inherently bound to the confines of country boundaries and international treaties. Reducing the reliability on legal enforcement may improve the chance of international effectiveness.
- What are the incentives to circumvent legal and technical protection for all parties in the transaction? The incentives for users to cheat will depend on the price per copy of digital works and the restrictions that are placed on usage. Decoupling revenue collection from the act of copying may reduce incentives for the user to cheat. Privacy concerns may also affect these incentives.
- How efficient is the proposed solution? Efficiency is a concern in the collection and disbursement of funds from consumers to rights holders. It is also a concern when analyzing the burden of monitoring for compliance and where that responsibility is placed.
- What are the impacts on user privacy and fair use? Privacy concerns frequently run counter to desires for economic efficiency. Therefore, any proposed solutions must acknowledge that there is a trade-off to be made. Fair use is important on its social merits alone, however, a broader adoption of fair and private uses will also serve to reduce user incentives to circumvent.
- How flexible is the solution? Some proposals will, if adopted, foreclose other types of solutions. It could be that it is better to support an inferior solution now, but one that leaves us with an opportunity to adapt other, better solutions in the future.

References

- [1] "Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group," June 3 2002. [Online]. Available: <http://www.cptwg.org>
- [2] D. L. Burk and J. E. Cohen, "Fair Use Infrastructure For Copyright Management Systems," *Harvard Journal of Law & Technology*, vol. 15, no. 1, Fall 2001. [Online]. Available: <http://jolt.law.harvard.edu/articles/pdf/15HarvJLTech041.pdf>
- [3] D. K. Mulligan and A. Burstein, "Implementing Copyright Limitations in Rights Expression Languages," in *2002 ACM Workshop on Digital Rights Management*, Washington DC, November 18 2002. [Online]. Available: http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc
- [4] J. S. Erickson, "Fair use, DRM, and trusted computing," *Communications of the ACM*, vol. 46, no. 4, pp. 34–39, April 2003.
- [5] L. S. Sobel, "DRM as an Enabler of Business Models: ISPs as Digital Retailers," *18 Berkeley Technology Law Journal*, forthcoming 2003. [Online]. Available: <https://www.law.berkeley.edu/institutes/bclt/drm/papers/sobel-drm-btlj2%003.pdf>
- [6] F. von Lohmann, *The Daily Princetonian*, April 14 2003. [Online]. Available: <http://www.dailyprincetonian.com/archives/2003/04/14/opinion/7930.shtml>
- [7] N. W. Netanel, "Impose a Noncommercial Use Levy to Allow Free P2P File Sharing," *U of Texas Law, Public Law Research Paper*, no. 44, November 15 2002. [Online]. Available: http://www.utexas.edu/law/faculty/netanel/Levies_chapter.pdf
- [8] W. Fisher, "PROMISES TO KEEP: Technology, Law, and the Future of Entertainment," available at <http://cyber.law.harvard.edu/people/ffisher/PTKprivate.htm>, last revised: March 22 2003. [Online]. Available: <http://cyber.law.harvard.edu/people/ffisher/PTKprivate.htm>
- [9] M. Boldrin and D. K. Levine, "The Case Against Intellectual Property," *American Economic Review*, no. 92, pp. 209–212, 2002. [Online]. Available: <http://www.dklevine.com/papers/intellectual.pdf>
- [10] J. Toomey and K. Thomson, "Virtual Tip Jar or Charity Case?" available at <http://www.futureofmusic.org/articles/arsfinal.cfm>, Future of Music Coalition, last revised: May 20 2000. [Online]. Available: <http://www.futureofmusic.org/articles/arsfinal.cfm>
- [11] *Associated Press*, December 8 2000. [Online]. Available: <http://www.cnn.com/2000/books/news/12/08/stephen.king.ap/>
- [12] B. Schnier, "The futility of copy prevention," *Cryptogram*, May 15 2001.
- [13] P. Biddle, P. England, M. Peinado, and B. Willman, "The Darknet and the Future of Content Distribution," in *2002 ACM Workshop on Digital Rights Management*, Washington DC, 18 november 2002. [Online]. Available: <http://www.cse.ogi.edu/~krasic/cse585/darknet.pdf>
- [14] E. W. Felten, "A Skeptical View of DRM and Fair Use," *Communications of the ACM*, vol. 46, no. 4, pp. 57–59, April 2003.

- [15] P. Kocher, J. Jaffe, B. Jun, C. Laren, and N. Lawson, "Self protecting digital content," CRI Content Security Research Initiative, Tech. Rep., 2003.
- [16] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier, "The risks of key recovery, key escrow, and trusted third-party encryption," Counterpane Labs, Tech. Rep., 1998. [Online]. Available: <http://www.counterpane.com/key-escrow.html>
- [17] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proceedings of Information Hiding Workshop*, 1998.
- [18] S. A. Craver, A. Perrig, and F. A. P. Petitcolas, "Robustness of copyright marking systems," in *Information hiding techniques for steganography and digital watermarking*, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Artech House Books, January 2000, ch. 7.
- [19] S. A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. S. Wallach, D. Dean, and E. W. Felten, "Reading Between the Lines: Lessons from the SDMI Challenge," in *Proc. of 10th USENIX Security Symposium*, Washington, D.C., August 13–17 2001. [Online]. Available: <http://www.usenix.org/events/sec01/craver.pdf>
- [20] F. Hill Slowinski, "What Consumers Want in Digital Rights Management," AAP and ALA, Tech. Rep., March 2003. [Online]. Available: <http://www.publishers.org/press/pdf/DRMWhitePaper.pdf>
- [21] "Apple Computer pressrelease," June 23 2003. [Online]. Available: <http://www.apple.com/pr/library/2003/jun/23itunes.html>
- [22] B. L. Fox and B. A. LaMacchia, "Encouraging recognition of fair uses in DRM systems," *Communications of the ACM*, vol. 46, no. 4, pp. 61–63, April 2003.
- [23] R. Andersson, "Why information security is hard," University of Cambridge Computer Laboratory, Tech. Rep., 2001. [Online]. Available: <http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf>
- [24] "House resolution 3818," South Carolina General Assembly 115th Session, 2003–2004, Sponsors: Rep. Ceips, Adopted March 19 2003. [Online]. Available: http://www.lpittr.state.sc.us/sess115_2003-2004/bills/3818.htm
- [25] "NATIONAL ENDOWMENT FOR THE ARTS v. Karen FINLEY," No. 97–371. Supreme Court of the United States, Argued March 31, 1998. Decided June 25, 1998. (524 U.S. 569).
- [26] J. E. Cohen, "DRM and Privacy," *Communications of the ACM*, vol. 46, no. 4, pp. 47–49, April 2003. [Online]. Available: <http://www.law.georgetown.edu/faculty/jec/CommACMdrm.pdf>
- [27] J. Cohen, "A right to read anonymously: A closer look at 'copyright management' in cyberspace," *28 Connecticut Law Review*, no. 981, 1996.
- [28] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack, "Privacy engineering for digital rights management systems," *Digital Rights Management Workshop 2001*, pp. 76–105, 2001.
- [29] "RECORDING INDUSTRY ASSOCIATION OF AMERICA v. VERIZON INTERNET SERVICES," Case 03-ms-0040, (D.D.C. 2003), Memorandum Opinion issued April 24, 2003. [Online]. Available: <http://www.dcd.uscourts.gov/03-ms-0040.pdf>
- [30] "EFF Open Letter to Universities," Electronic Frontier Foundation, November 6 2002. [Online]. Available: <http://www.epic.org/privacy/student/p2pletter.html>
- [31] F. von Lohmann, "Reconciling DRM and Fair Use: Preserving Future Fair Uses?" in *"Fair Use by Design?" Workshop*. 12th Computers, Freedom & Privacy Conference, April 16 2002. [Online]. Available: <http://www.cfp2002.org/fairuse/lohmann.pdf>
- [32] "Den offentlige påtalemyndighet mot Jon Lech Johansen," OSLO TINGRETT, January 7 2003. [Online]. Available: <http://www.domstol.no/archive/OsloTingrett/Nye%20avgjorelser/DVD-jon.doc>
- [33] P. Samuelson, "Digital Rights Management {and, or, vs.} the Law," *Communications of the ACM*, vol. 46, no. 4, pp. 41–45, April 2003.