MISTRUST-BASED DIGITAL RIGHTS MANAGEMENT

RANDAL C. PICKER[*]

INTRODUCTION 48
I. WHY DIGITAL RIGHTS MANAGEMENT? 51
A. Copy-Control DRM 51
B. Bundled Uses and Per-Use Pricing 52
C. Patent-Royalty Collection 53
D. DRM and Shaping Competition 54
II. THE PROBLEM OF THE CD: SONY BMG AND ADD-ON DRM 55
A. Staring at the Jewel Box: Neil Diamond's 12 Songs. 56
B. Inside XCP and MediaMax 57
C. Four Problems for Add-On DRM 60
III. IDENTITY-BASED DRM: SWITCHING FROM PRODUCTS TO SERVICES 62
A. Google Video 63
B. Amazon Upgrade 65
C. iTunes 66
D. Implementing Identity-Based DRM 68
CONCLUSION 70

[*] Copyright © 2006, Randal C. Picker. All Rights Reserved. Paul and Theo Leffmann Professor of Commercial Law, The University of Chicago Law School and Senior Fellow, The Computation Institute of the University of Chicago and Argonne National Laboratory. I thank my fellow panelists at the Digital Broadband Migration Conference, February 19-20, 2006 at Silicon Flatirons at the University of Colorado School of Law for comments; participants in the April 7, 2006 UCLA School of Law Media, Entertainment and Culture Workshop; Ed Felten; the Russell Baker Scholars Fund and the John M. Olin Program in Law and Economics; and through the Olin Program, Microsoft Corporation, Verizon, and Visa U.S.A., Inc., for generous research support. I posted a short-version of this work on the University of Chicago Law School Faculty Blog, http://uchicagolaw.typepad.com/faculty/2006/02/adding_mistrust.html, and benefited from the ensuing comments and online discussion.

INTRODUCTION

Consider this hypothetical: You buy a music CD and pop it into your computer. Before you can rip the CD to your computer, a registration window opens. That window takes your name and credit card information. Once registered, you can rip the CD and play the music to your heart's content. You can add the songs to your central media servers at home or put the songs on your iPod and the iPod of each member of your family. You can do a mash-up if you want: take the first 20 seconds of each song and make a new one. And if you want to upload the CD to a peer-to-peer network, go ahead.

What's the catch? The catch is that your identity travels with the songs—more precisely, not your full identity but an ID tag that can be matched with your stored account information—and someone in possession of the tag can access part of your account, turn in the tag, and get $10 charged to the account holder's credit card. Think of this as identity-based digital rights management (DRM) with incentives or—more sharply—mistrust-based DRM. How would this approach differ from current DRM schemes and why might this one have a better chance of succeeding?

As I explain below, it would be difficult to implement this sort of scheme for standard music CDs or DVDs. But just as the VCR has gone the way of the dodo, physical media are dying as mechanisms for delivering content. Edison's wax cylinders have had a great run, but online distribution of content will supplant physical media in the next decade. We are replacing products with services.

The scheme I describe above is precisely the one that is being implemented in online distribution today, at least in part. This is still at an early stage, but Apple's iTunes, Google's new video service, and Amazon's forthcoming Amazon Upgrade give us a sense of how online DRM will be implemented, not as a kludgy add-on as is being done for music CDs, but as part of the original design. Mistrust-based DRM will be a key part of this, precisely because of the way that it leverages the content purchaser's incentives to protect identity and, in so doing, protect content.

DRM is both important and controversial. From the copyright holder's perspective, DRM is first and foremost about making meaningful the legal rights assigned to the copyright holder under copyright law, especially the right to control the making of copies.[1] The right to control

[1] *See* 17 U.S.C. § 106 (1) (2000) ("Subject to sections 107 through 121, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords; . . ."); Council Directive 2001/29, art. 2, 2001 O.J. (L 167) 16 (EC) ("Member States shall provide for the exclusive

copying of a work isn't self executing. Copying has been controlled through the technology of copying, where until the last thirty years or so, copying was expensive and asymmetric. By expensive, I mean that it was relatively difficult to make the second copy of a work. By asymmetric, I mean that it was typically substantially cheaper to make the second copy as part of making a unified run of copies of the work than it was for a third-party to make a second copy from a first physical copy of the work.

This has changed over the last thirty years. With the rise of the cassette tape recorder, photocopying equipment, the VCR, and, more recently, of peer-to-peer networks, copying costs have dropped and third-parties are as well-situated as the copyright holder to make additional copies. Copying costs have become symmetric, and technology, once the barrier to copying, has become the means of copying. Legal rights previously enforced through technological barriers are now much harder to enforce, at least not without new technological barriers, hence the rise of digital rights management. The promise is meaningful enforcement of the rights that exist on the statute books; the fear is a shift in control in favor of copyright holders and away from the public, perhaps through limits on fair use of works.

With add-on DRM of the sort we have seen for music CDs, the CD owner and a dedicated decryptor have a shared interest in evading use restrictions. The CD owner is eager to enlist the help of the decryptor and has little concern about the wide spread over the network of the music on the CDs, and one p2p user has little to fear from a fellow user of the network. In contrast, identity-based DRM—when a valuable ID tag travels with the content (or with access to the content)—will drive an incentives wedge between the CD owner and the decryptor and between members of the p2p network. The CD owner will fear that in removing the use restrictions, the decryptor will acquire the account information and that information could be put to ill use or that the content will seep out into the p2p network still bearing the ID tag.

The darknet critique of DRM says that it only takes one: just one person to get around the DRM and put the content out into the clear free of the wrapper.[2] Mistrust-based DRM embraces that idea: if it only takes one person to claim the bounty ID tag, the content owner may choose not to share the content. The interesting, almost sociological, question is how

right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part: (a) for authors, of their works; . . . ").

[2] *See* Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 641 (2004) (citing Peter Biddle et al., *The Darknet and the Future of Content Distribution*, http://crypto.stanford.edu/DRM2002/darknet5.doc (last visited Sept. 26, 2006)); posting of Ed Felton to Freedom to Tinker blog, *DarkNet*, http://www.freedom-to-tinker.com/index.php?p=206 (Nov. 25, 2002, 11:47 EST).

much suspicion do you need to introduce into a file-sharing system for content owners to refuse to share with anonymous recipients over peer-to-peer networks? And if the small-worlds phenomenon tells us that we are just six links from everyone else on the planet, how many of my friends will I trust with access to my account, given that they may give it to their friends, who may gave it to their friends, etc.? Small-group sharing plus six degrees of separation equals sharing with the entire world, and, unfortunately, not everyone in the world can be trusted.

I should be more precise about the mechanics of implementing identity-based DRM. The core notion is that an identification tag is attached to each song, presumably at the point of downloading. Given concerns about privacy, it is highly unlikely that this tag would be transparent, that is, that it would be readable by any recipient. An encrypted tag but one that uniquely identifies the original recipient of the content suffices.

We should build this system up one brick at a time. With ID tags embedded in songs, the download service could scour p2p networks for tagged content and could implement a penalty when tagged content was found. Very little limits that penalty structure. The download service could revoke the right to use that service and could couple that with a monetary fine.

This is ID tagging plus centralized enforcement. We could decentralize enforcement, and that would probably require some sort of bounty system to induce users of p2p networks to turn in songs to collect the bounty. Note that this does not mean that identity needs to be transparent; all that is required is that the—you choose: snitch/tattletale/whistleblower—has knowledge of the existence of the tag and seeks to collect the bounty by turning in a tagged song.

Identity tags plus bounties gets us to mistrust-based DRM. We need decentralization of enforcement to create mistrust and to break the alignment of incentives that otherwise exists in p2p systems. Mistrust enters at two points, as to both software (code) and peers. If shared songs carry with them valuable ID tags, you will be willing to share tagged songs only with trustworthy peers. You almost certainly will not want to share those songs with anonymous users of p2p networks. The second possible point of mistrust is the software that gets songs from your PC to the p2p network. There have often been alignment issues with this software, perhaps most notoriously with KaZaa. The existence of valuable ID tags takes this another step, as the tags may create the fear that the software itself will try to access the value embedded in the tags.[3]

[3] Whether this system can be implemented is in dispute. For critical commentary, *see* posting of Ed Felten to Freedom to Tinker blog, *Mistrust-Based DRM*, http://www.freedom-to-tinker.com/?p=980, (Feb. 22, 2006, 13:54 EST); posting of Ed Felten to Freedom to Tinker blog, *How Watermarks Fail*, http://www.freedom-to-tinker.com/?p=981 (Feb. 24, 2006, 9:07

Section I addresses four ways in which DRM is currently used, namely, copy-control; per-use pricing; closed-system definition and patent-royalty collection; and competition structuring. Section II looks at one attempt at copy-control DRM, namely, Sony BMG's distribution of copy-protected music CDs. It would be a mistake for us to generalize from the real difficulties associated with adding DRM to a preexisting product. The world of online content services is fundamentally different. In Section III, I discuss Google Video, Amazon Upgrade, and Apple's iTunes. These are three leading examples of services that are embracing, at least in part, identity-based DRM.

I. WHY DIGITAL RIGHTS MANAGEMENT?

We should consider what digital rights management is seeking to accomplish. Four roles come to mind: (1) copy control to avoid SOFE (sold once, free everywhere); (2) per-use pricing, making possible greater pricing granularity, so as to charge consumers different prices for different uses of the same work; (3) patent-royalty collection across devices and media; and (4) competition structuring, so as to control how competition evolves with linked devices and content.

A. Copy-Control DRM

A standard use for DRM is copy control: use software to limit the number of copies that can be made. Sony BMG's infamous attempt to add DRM to music CDs—discussed in detail in Section II—imposed a number of limits on making copies of the songs on the CD. Sony BMG wasn't trying to charge more for consumers who wanted to use the CDs in a standard CD player and on a computer. The content creator is perfectly happy to have the actual purchaser use the content in any time, place, and manner that the purchaser so desires, but the producer of the content wants to prevent the purchaser from making copies to give to friends or to upload to peer-to-peer networks.

Whether this stands any chance of working is contested. Playing a song so that I can hear it—I am listening to Chick Corea as I type—means that I can record it and the DRM scheme may not survive the recording process. The quality of that copy may be degraded, but it may be good enough. And a professional decryptor—is that the right phrase to use instead of hacker?—might strip away the DRM, and put an unencrypted copy onto a peer-to-peer network. Both of these possibilities work against effective DRM designed to control copies.

With music CDs, we are trying to retrofit DRM onto an existing

EST).

platform. The analysis in Section II should make clear the enormous difficulties associated with this sort of add-on DRM. But we won't be doing too much retrofitting going forward. As discussed below, DVDs came with encryption, and the battle over the broadcast flag for digital television (and high-definition radio, too) is precisely about whether these new formats will come with built-in copy and use controls. For digital television and radio, these are public battles, where we will fight about the scope of the authority given—or to be given—to the Federal Communications Commission and about the virtues and vices of government technology mandates. In contrast, the private online content services to be discussed in Section III—Google Video, Apple's iTunes, and Amazon Upgrade—will implement DRM without any need to consult with the FCC and will do so by choice and in competition with others and as part of the DNA of the platform.

But the success or failure of copy-control DRM is not just about retrofitting of the sort that we have seen with music CDs. The core need to have the content in the clear, as it were, for the standard non-computer CD players creates the problems we will see in the Sony BMG episode. But there is a more basic problem with locked-down DRM: the content purchaser and the professional decryptor have a shared interest in evading the copy control. That will be true even if the copy control is built in originally. Unless the copy-control is identity-based, we won't give the content purchaser a reason to stay away from professional decryptors and their tools. That means that there is good reason to think that the broadcast flag regime is likely to struggle too.

B. Bundled Uses and Per-Use Pricing

I buy a DVD. Most users play DVDs on their home DVD players, but I want to watch my DVDs on my video iPod. The copyright holder wants to charge me extra for my non-standard use and uses DRM to restrict my ability to move the DVDs to the iPod. DRM might facilitate per-use charging, as might take place if the DVD producer assessed a fee to unlock the DVD content for the iPod.

I don't want to try to assess the virtues and vices here of per-use pricing. I think that this is tricky. Absent DRM, using the DVD on the video iPod is a use that comes bundled with the DVD itself. That means that each DVD purchaser has to buy the entire bundle—the standard DVD player use and the video iPod use—even when she might just want to buy the standard use. The bundled uses might come at a higher price than the standard use.

The only point to note here is how per-use pricing DRM influences the willingness of the content purchaser to try to crack the DRM scheme. Restrictions on use—as opposed to restrictions on sharing—will push the content purchaser towards figuring out how to evade the DRM scheme. The core theme of this paper is that we want to try to separate content purchasers from professional DRM evaders. Encoding identity into content will help do that, but restricting use will create more reasons to put identity at risk so as to circumvent use restrictions.

C. Patent-Royalty Collection

DVDs are encrypted with the content scramble system (CSS).[4] Encryption has the consequence of linking DVD discs and DVD players together in a closed system. Absent hacking, a DVD disc will play only on an authorized player. And the fact that licenses are required for the right to use CSS means that other controls can be implemented consistently across the DVD platform. For example, the DVD Copy Control Association required CSS licensees to implement DVD drives that respected a regional encoding scheme.[5] Pick a recent DVD and shop for it first at Amazon.com and then at Amazon's United Kingdom site, www.amazon.co.uk. The U.S. website sells DVDs with region 1 encoding (for the U.S. and Canada) while the UK website sells region 2 DVDs (Europe, Japan, South Africa and the Middle East, including Egypt according to Amazon).

So far this sounds like a series of use controls perhaps directed at making price discrimination possible, as more surfing at Amazon suggests that UK DVDs are more expensive than those in the U.S. But more is at stake than just price discrimination. Dates of movie theater releases vary across countries. Part of this is presumably related to the inability of stars and directors to be in Paris and Los Angeles at the same time. If stars are important for launching a movie, you will want to open the movie on different dates in different countries.

But note what that means for the release of the DVD. If the right delay window is three months—release the DVD three months after the theatrical run has ended—the DVDs will need to be released in a staggered fashion as well. But if all DVDs play anywhere, the staggering doesn't work. Regional encoding makes that possible, and, as we have seen, the need to license CSS provides a lever to enforce regional encoding in DVD players.

But as if this were not enough complexity, there is more at stake. The DVD standard is based on more than a hundred patents. Royalties on those patents are recovered through the sale of DVD discs and players. Many of those patents are in the two main DVD patent pools, the 6C

[4] *See generally* DVD Copy Control Association, Content Scramble System, http://www.dvdcca.org/css/ (last visited July 8, 2006).

[5] *See* DVD Copy Control Association, Regional Playback Control, http://www.dvdcca.org/rpc.html (last visited July 8, 2006).

pool[6]—originally comprised of patents from six companies and now with eight participants—and a second pool involving patents from Philips, Sony, and Pioneer.[7]

Patent pools have a long history.[8] One of the key virtues of patent pools is to reduce the transactions costs associated with licensing required technology. With 100 plus patents implicated in DVDs, individual negotiations for the right to use those patents could be horrifically time-consuming, plus a licensor would fear the hold-out problem, where the holder of the last needed patent seeks a disproportionate payment. The patent pool reduces both of those costs.

How will the pools collect royalties? Toshiba was to act as the administrator for the 6C pool and would initially charge royalties of $.075 per DVD disc and 4% of the net sales price of DVD players and DVD decoders, with a minimum of $4.00 per player or decoder.[9] The closed system makes it possible to obtain royalties on both the player and the discs. We are now talking about how to run a tax system. If we are going to collect royalties on the patents, should we collect them on just the players? Just the discs? On both? There is conventional economic theory—Ramsey pricing—which attempts to provide a guide on that, but the bottom line is that we shouldn't just assume that we—society, not the patent holders—are necessarily better off if we force the patent holders to open the system and just charge royalties on the players. DRM is the lock that makes this closed system possible.

D. DRM and Shaping Competition

The Apple iPod and iTunes have emerged as the leading wave of the move to online digital entertainment. The iPod has led to a huge run-up in Apple's stock price,[10] and the iPod is so successful that it now defines its own economic ecosystem with a large market in add-on devices. And indeed, Apple is profiting from these sales, often obtaining 10% of the wholesale price of a product.[11]

[6] *See* DVD 6C Licensing Agency, DVD 6C Patent Pool, http://www.dvd6cla.com (last visited July 8, 2006).

[7] *See* Philips, DVD Format and Logo Licensing, http://www.licensing.philips.com/information/dvd/documents206.html (last visited July 8, 2006).

[8] *See generally* FLOYD L. VAUGHAN, THE UNITED STATES PATENT SYSTEM 39-67 (1956).

[9] *See* Letter from Joel I. Klein, Assistant Attorney General, to Carey R. Ramos, Paul, Weiss, Rifkind, Wharton & Garrison (June 10, 1999), *available at* http://www.usdoj.gov/atr/public/busreview/2485.htm (citing the Authorization Agreement § 5.1 in footnotes 32 and 33).

[10] *See* John Authers, *iPod Provides Apple with a Record Breaking Run*, FIN. TIMES (London), Dec. 30, 2005, at 21.

[11] *See* Ina Fried, *Apple Seeks 'Tax' on iPod Accessories*, CNET NEWS.COM, Mar. 16,

An empty iPod isn't very interesting. How do you get content into the iPod? The iPod plays MP3 content. That means that you can take a music CD, rip those files into MP3 files, and move the content to the iPod. I use a text-to-speech program to listen to text files on my iPod Nano, and those files are written as MP3s. You can also buy MP3s online at sites like emusic.com. Note that none of this content is sold particularly for the iPod and none of it is subject to DRM. This is all content that could easily be moved around p2p networks.

iTunes—and, here is the key point, *only* iTunes—sells non-MP3 online content for the iPod. This content is encoded in the AAC format (Advance Audio Coding) and is wrapped in Apple's FairPlay DRM scheme. Apple has refused to open the iPod to other sellers, such as by licensing FairPlay to them.[12] Indeed, when RealNetworks figured out a way around the DRM limitation so that it could sell online music for iPods, Apple intimated that RealNetworks might have violated the Digital Millennium Copyright Act or engaged in contractually-barred reverse engineering. In any event, Apple updated the iPod software—not just for new iPods but for all existing iPods—and reestablished incompatibility.[13]

Systems competition is complicated, so it would be a mistake to assume that Apple has acted in a way that should trouble us or that should be found to violate U.S. antitrust law. But the inherent difficulty of regulating systems competition means we are likely to see a variety of policy responses to this particular use of DRM. France has already threatened to force greater interoperability for the iPod and iTunes.[14]

II. THE PROBLEM OF THE CD: SONY BMG AND ADD-ON DRM

The producers of music CDs fear that they have entered a SOFE world: sold once, free everywhere. If a person can buy a CD, rip it, and upload it to a peer-to-peer network, the copyright holder may only sell one copy of a CD. Of course, that isn't the real world, but it is close enough to understand the urge to add digital rights management to music

2005, http://news.com.com/2100-1041_3-5620959.html.

[12] This isn't to say that users aren't looking for ways around FairPlay. *See, e.g.*, Kirk McElhearn, *Classical Music on the iPod and iTunes*, PLAYLIST MAG., Mar. 11, 2005, http://playlistmag.com/features/2005/03/classicalipod/index.php.

[13] For a discussion of formatting *see* BERKMAN CENTER FOR INTERNET & SOCIETY, ITUNES 11-12 (2005), http://cyber.law.harvard.edu/media/uploads/81/iTunesWhitePaper0604.pdf. For a discussion of Real Networks *see* John Borland, *RealNetworks Breaks Apple's Hold on iPod*, CNET NEWS.COM, July 26, 2005, http://news.com.com/2102-1027_3-5282063.html; John Borland, *Apple Fights RealNetworks' 'Hacker Tactics'*, CNET NEWS.COM, Dec. 14, 2004, http://news.com.com/2100-1027_3-5490604.html.

[14] *See French Measure Is Criticized As Encouraging Music Piracy*, WALL ST. J., Mar. 23, 2006, at B6.

CDs.

But we run into a disabling problem immediately: music CDs need to play in CD players. For decades, CDs have played in CD players and a new CD needs to be able to do that as well. So somehow an ordinary CD player needs to play the CD flawlessly, yet when that same CD is inserted into the CD drive built into your computer, it needs to work differently. Otherwise if the computer is given unfettered access to the music, it's rip, upload, and off to the p2p networks.

This is a real problem: make sure that the product can be used in its traditional, standard uses and yet limit new uses. That isn't a statement about the merits of that approach, just the difficulties of implementing it. It is as if the CD needs to play in the CD player and yet somehow be prevented from being inserted into a toaster when the purchaser really wants to pop it in.

A. Staring at the Jewel Box: Neil Diamond's 12 Songs.

Enter Sony BMG and two different encryption schemes, XCP and MediaMax. Sony BMG has released a number of music CDs using the two schemes.[15] To take one example, Neil Diamond's *12 Songs* is encrypted with the XCP copy protection scheme. A careful examination of the front spine of the CD reveals a logo coupled with the phrase "CONTENT PROTECTED" and, beneath that, in small letters, a suggestion to see the reverse side for what are optimistically described as "features."

On the back, along with the usual list of songs, near the bottom, we see blocks of information relating to copyright. That includes the FBI anti-piracy warning symbol;[16] a statement that "unauthorized copying is punishable under federal law;" and a "compatible with" block. The latter addresses playback, ripping, and the use of portable devices. The block indicates that limited copies are possible; that the website cp.sonybmg.com/xcp should be consulted for additional information; and a footnote indicating that "certain computers may not be able to access the digital file portion of this desk. Use subject to applicable end user license agreement."

And, were that not enough, all of that is followed with yet smaller print indicating a variety of copyrights, trademarks, and a final statement: "WARNING. All Rights Reserved. Unauthorized duplication is a violation of applicable laws." A music CD that only a lawyer could love.

[15] For a list of relevant CDs, *see* Sony BMG Music Entertainment, http://www.sonybmgcdtechsettlement.com/CDList.htm (last visited July 9, 2006).

[16] For details, *see* Press Release, Federal Bureau of Investigation, Pirates in Cyberspace: Not Exactly Fun and Games (Feb. 19, 2004) *available at* http://www.fbi.gov/pressrel/pressrel04/piracy021904.htm.

Some of what appears on *12 Songs* is completely generic, such as the FBI anti-piracy warning and the indication of copyright and restrictions on duplication. It is the detailed copyright-control information that is distinctive.

Remove the plastic shrinkwrap and examine the CD. It is stamped with the FBI anti-piracy warning logo and the FBI anti-piracy warning itself along with further indications of copyright and trademarks. We learn—for I did not know it before opening the CD—that the logo on the spine of the CD is the "copy control logo," which is a trademark of International Federation of the Phonographic Industry (IFPI)[17] and used under license on the CD.[18]

The CD liner contains pictures of Neil Diamond making music; a brief amount of text; and the usual production information. We are told once again about copyrights and trademarks, and a final warning about reserved rights and unlawful duplication. The only new copyright item of interest is that all of the songs—words and music by Neil Diamond—are published by DiamondSongs and are available through SESAC, rather than ASCAP or BMI. The liner tells us nothing about the copy-control scheme.

What happens next? That depends on what you do with the CD. If you insert the CD into a standard CD player—say a Sony Discman or a CD player in your car—the music plays, just like it has since Thomas Edison built his phonograph. That almost comes as a surprise: you half expect the CD to start smoking and self-destruct, just like in *Mission Impossible*, but, nope, it plays music. Diamond describes the music as "a stripped-down acoustic sound." That seems right; the orchestration is notable for its sparseness and simplicity. The complicated part of the CD isn't the music, it's the copy-control scheme.

But a CD player is a relatively locked-down device. Not fully so, as there needs to be a port for headphones to get the music out to our ears, and you can instead use that port to hook the music up to your computer to record—or at least so my 16-year old son tells me—so we can expect leakage even from CD players. But the target of the XCP encryption scheme isn't the CD player and its port for headphones but instead your personal computer.

B. Inside XCP and MediaMax

Typically, when I purchase a CD, I immediately rip it using the Windows Media Player (WMP). Just to get the mechanics right, I will

[17] IFPI, http://www.ifpi.org/ (last visited Oct. 11, 2006).

[18] *See* Press Release, IFPI, IFPI Announces New Optional Copy Control Symbol for CDs (Sept. 17, 2002), *available at* http://www.ifpi.org/site-content/press/20020917.html.

first open WMP and then will insert the CD into my computer. With an unencrypted CD, I select the rip tab in WMP and the music is then stored on my computer. The current version of WMP allows me to determine whether or not the copy on my computer is subject to a copy protection scheme implemented by the WMP itself.

What happens instead if I insert a CD copy-protected by either XCP or MediaMax? I have not done that but Ed Felten, a computer scientist at Princeton, and his graduate student, Alex Halderman, have done so and have reported the results, initially on the "Freedom to Tinker" blog and subsequently in an academic paper.[19] There are lots of details, but I will lay out a simple version.

XCP and MediaMax are what Felton and Halderman have termed active protection systems. Both copy-protection schemes take advantage of the autorun feature built into the Windows operating system.[20] The point of autorun is to simplify installation of new software. Absent autorun, the consumer needs to figure out what program should be started from any CD to install new software. Autorun takes that process out of the consumer's hands and reduces the possibility that a consumer won't understand how to install new software.

With autorun on, the insertion of a copy-protected CD causes software embedded on the CD to be invoked. The precise details are different for XCP and MediaMax, and those differences might matter, but not for my purposes here. The key idea is that the automatically-invoked software can block normal copying of the CD and can impose an end-user license agreement that limits access by the computer to the CD.[21]

To make all of this work, autorun installs software on the user's computer and then takes the additional step of installing additional software to hide the newly-installed DRM software.[22] I am not sure how to describe this behavior, but as Felten and Halderman make clear, uninvited installation coupled with cloaking is exactly the behavior that we

[19] *See* J. Alex Halderman & Edward W. Felton, *Lessons from the Sony DRM Episode* (Ctr. for Info. Tech., Princeton Univ., Dep't of Computer Sci., Working Paper, 2006) *available at* http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf; Freedom to Tinker, http://www.freedom-to-tinker.com (blog entries describing their work with the Sony DRM).

[20] Microsoft, HOW TO: Create an Autorun CD-ROM for Applications That You Create by Using Microsoft Visual Studio .NET, http://support.microsoft.com/default.aspx?scid=kb;en-us;818804 (last visited July 9, 2006) (provides a more detailed explanation). Autorun is a Windows feature; if the CD is inserted into a computer running Linux or the Macintosh operating system, users won't invoke the DRM.

[21] For a discussion, *see* J. Alex Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System* (Princeton University Computer Science Technical Report TR-679-03, 2003) *available at* http://www.cs.princeton.edu/~jhalderm/cd3/; *see also* Posting of J. Alex Halderman to Freedom to Tinker, *CD DRM Makes Computers Less Secure*, http://www.freedom-to-tinker.com/?p=919 (Nov. 1, 2005, 11:35).

[22] *Id.*

expect and fear from spyware and other forms of malware, and in particular, a class of malware known as "rootkits."[23] These are programs that hide on PCs and allow outsiders to exercise some control over the machines (frequently making the machines zombie PCs and creating a parade of harms to the network).[24]

So Sony BMG installs software and then hides the software to make it more difficult for consumers to remove it. Sony BMG discloses the existence of the software in the End-User License Agreement (EULA), but if you didn't read that carefully, you might not notice that software was being installed.[25] And the EULA says very little about how the software is installed, making it quite hard for consumers to remove the now-hidden software later. Of course, that is the point. If the DRM software is actually going to control access to content, the software needs to be there. It can't be the case that the consumer can remove the software at will, at least if doing so won't also end the right to access the associated content sitting on the computer.

But the particular cloaking approach used by Sony BMG also made it possible for outsiders to hide their software in the same hidden area of the consumer's computer. Of course, a malware author might very well bundle his own cloaking device with the malware, and, indeed, this is a standard complaint about rootkits.[26] The real question is whether the existence of the Sony BMG cloak made it possible for a malware author to hide his malware when he couldn't have done so on his own. Whatever mechanism is used to bring in the malware in the first place should also be available to install the malware cloak, though part of this depends on exactly what level of access—administrator, user, or something else—that the user makes available, intentionally or not, to the intruder. And the fact that we actually observed a malware author taking advantage of the Sony BMG cloak tells us very little. My guess is that malware authors are high on the list of DRM haters, so we could readily predict that the Sony BMG cloak would be exploited. What we can't know is whether the malware was simply written to make Sony BMG look bad or

[23] Posting of Ed Felten to Freedom to Tinker, *SonyBMG "Protection" is Spyware*, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 8:23 EST); Posting of J. Alex Halderman to Freedom to Tinker, *MediaMax Permanently Installs and Runs Unwanted Software Even if User Declines EULA*, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005 14:23 EST). For a general discussion, *see* GREG HOGLUND & JAMES BUTLER, ROOTKITS: SUBVERTING THE WINDOWS KERNEL 4 (2006) ("In other words, a rootkit is a set of programs and code that allows a permanent or consistent, undetectable presence on a computer." (emphasis omitted)).

[24] *See generally* Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky*, in THE LAW AND ECONOMICS OF CYBERSECURITY 115 (2006).

[25] For what purports to be the Sony BMG EULA, *see* http://www.sysinternals.com/blog/sony-eula.htm (last visited July 6, 2006).

[26] *See* Halderman, *supra* note 21.

whether absent the Sony BMG cloak the malware author would have written his own cloak.

Felten and Halderman make clear that a savvy computer user will be able to avoid the XCP and MediaMax encryption schemes.[27] Turning off autorun means that the user affirmatively has to invoke the software, and the consumer has no incentive to do so. Indeed many computer security experts recommend turning off autorun as the insertion of the CD can otherwise have unexpected consequences.

C. Four Problems for Add-On DRM

We should take stock of the situation faced by content producers such as Sony BMG. First, the analysis by Felten and Halderman make clear that add-on DRM is likely to be ineffective. Smart consumers will sidestep the DRM limitations by turning off autorun and that will give them access to the standard audio files that are on the CDs. From there it is just a hop, skip, and a jump to wide distribution on p2p networks.

Second, add-on DRM faces stiff consumer resistance. I first encountered *12 Songs* in my native capacity as consumer. Amazon did a good job of emphasizing that the CD was copy-protected and I quickly clicked elsewhere. Some consumers have attempted to organize boycotts of companies that sell copy-protected CDs. I suspect that none of this is lost on content sellers, and that influences how much—or how little—they emphasize that the CDs are copy-protected. My detailed description of *12 Songs* was meant to highlight that it would be easy for a consumer to miss the copy protection. Yes, there was a lot there, but much of it is in small print; if you weren't looking for it as I was, it might be easy to skip right over it. And the appearance of an End-User License Agreement might not be enough either, as for better or worse, consumers routinely click through these agreements.

Third, add-on DRM will need to navigate a thicket of federal and state laws. The class-action lawsuit filed by the Electronic Frontier Foundation alleged claims under the California Consumer Legal Remedies Act; for unfair, unlawful and fraudulent business practices in violation of California Business and Professions Code Section 17200; for breach of the implied covenant of good faith and fair dealing; and for false or misleading statements under California Business and Professions Code 17500.[28]

State Attorneys General in Massachusetts and New York launched

[27] Posting of Ed Felten to Freedom to Tinker, *What Does MediaMax Accomplish?*, http://www.freedom-to-tinker.com/?p=935 (Nov. 23, 2005, 8:54 EST).

[28] For background on the case, including the complaint, *see* Electronic Frontier Foundation, Sony BMG Litigation Info, http://www.eff.org/IP/DRM/Sony-BMG (last visited July 6, 2006).

investigations out of Sony BMG sales, and the Texas Attorney General brought suit under the Texas Consumer Protection Against Computer Spyware Act of 2005, a new law that became effective on September 1, 2005.[29] And blog commentary has raised questions about the applicability of the federal Computer Fraud and Abuse Act, which criminalizes under certain conditions unauthorized access of a computer.[30]

The point here is not to address the legal sufficiency of these claims. For example, I think that we will be cautious in taking the Computer Fraud and Abuse Act into these situations. That act focuses on outside break-ins, rather than those who proceed under permission of the sort set forth in Sony BMG's XCP EULA. We will not quickly move from possible contract violations—and indeed I am not sure that there are any of those here—to criminal liability.[31] That does mean, as Felten has pointed out, that installing software without a contract in place will pose greater risks, as Felten and Halderman suggest occurs with MediaMax DRM. Instead, the point is to note that a business strategy that engenders multiple class actions and investigations and lawsuits by state Attorneys Generals is likely to be short-lived.

Fourth, I should also say that while I do not expect us to jump quickly from contract to criminal violations, I also think that in the longer-run we will probably not allow content providers to simply enforce one-sided EULAs. We face a basic conflict over control: computer owners want to control their PCs, content sellers want to control what happens to their content.[32] I don't think that there are many absolutes in this argument. The fact that I paid for my laptop doesn't mean that I can't agree with Sony BMG or some other content provider that there are limits on what I can do with my computer, limitations that I might want to agree to to get access to content. And content owners start with terms

[29] Arik Hesseldahl, *Spitzer Gets on Sony BMG's Case*, BUS. WK., Nov. 29, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051128_573560.htm (last visited July 7, 2006); Press Release, Mass. Attorney Gen., Recalled Sony BMG CDs with Potential Risk to Computer Viruses Are Still Available in Boston (Nov. 30, 2005), *available at* http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1540; Press Release, Attorney Gen. of Tex., Attorney General Abbott Brings First Enforcement Action In Nation Against SonyBMG for Spyware Violations (Nov. 21, 2005), *available at* http://www.oag.state.tx.us/oagNews/release.php?id=1266.

[30] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000). For commentary, *see* Posting of Ed Felten to Freedom to Tinker, *Sony CDs and the Computer Fraud and Abuse Act*, http://www.freedom-to-tinker.com/?p=949 (Dec. 21, 2005, 8:44 EST); *see also* Posting of Eric Goldman to Technology and Marketing Law Blog, *Is Sony's DRM Spyware*, http://blog.ericgoldman.org/archives/2005/11/is_sonys_drm_sp.htm (Nov. 7, 2005, 10:10 EST).

[31] *See* Secureinfo Corp. v. Telos Corp., 387 F.Supp. 2d 593 (E.D. Va. 2005).

[32] *See* John Borland, *Who has the right to control your PC?*, CNET NEWS.COM, Nov. 21, 2005, http://news.com.com/2100-1029_3-5961609.html; *see* Bruce Sterling, *The Rootkit of All Evil*, WIRED MAG., Feb. 2006, at 94.

set by copyright. Some of those terms clearly benefit copyright holders, but others, such as fair use and the first-sale doctrine, benefit content users.

These contracts—whether written on paper or implemented through agreement and technological limits—sit out there as part of the legal landscape. Computer users should be able to cede control over their machines if they choose to do so. We see this frequently with software that updates itself remotely, such as Google Desktop Search, or as Sony BMG contemplated updates would occur.[33] And it is far from clear to me that consumers can't waive fair use rights under the Copyright Act.

We are entering an era in which consumer commitments about how they will receive, manage and use content will matter. Content owners want to know that content is entering a protected environment, meaning an environment that may control use, copying, and distribution of copyrighted works. If consumers can't make meaningful commitments, content providers won't be able to make meaningful distinctions between consumers.

That said, whatever one concludes about the angels-dancing-on-the-head-of-pins question about the limits of contract, my guess is that click-through agreements implementing unreasonable rules regarding third-party access to consumer computers will not be sustainable politically, either before juries or in Congress. If that is right, contract won't be the main device by which we will validate DRM, but we instead may require additional legislation with accompanying safe harbors, where some will favor strong protections for consumers—possibly as to uses and probably as to privacy—and others will favor content producers.

If you sell music CDs, this is a bleak story. Add-on DRM hasn't worked, isn't wanted by consumers, and leads to lawsuits. In settling the EFF lawsuit, Sony BMG has agreed to stop selling music CDs with MediaMax or XCP.[34] Given the reaction so far, Sony BMG almost must be delighted that it is now legally barred from doing something that it should no longer want to do anyhow.

III. IDENTITY-BASED DRM: SWITCHING FROM PRODUCTS TO SERVICES

Return to the hypo at the beginning of the paper. Buy a CD, slide it

[33] For a discussion of Google Desktop Search, *see* Randal C. Picker, *Rewinding Sony: The Evolving Product, Phoning Home and the Duty of Ongoing Design*, 55 CASE W. RES. L. REV. 749, 757 (2005); *see* Sony BMG EULA, *supra*, at 25 (Article 8 reads "The SONY BMG PARTIES may from time to time provide you with updates of the SOFTWARE in a manner that the SONY BMG PARTIES deem to be appropriate.").

[34] *See* Information Web Site for the Sony BMG Music Entertainment, Sony BMG CD Technologies Settlement, http://www.sonybmgcdtechsettlement.com (last visited July 7, 2006).

into your computer for ripping, and up pops a registration window. After registering with a credit card, you have full access to the content, and that content is tagged with your identity. Share the content on a peer-to-peer network and you share your identity, including account information allowing future purchases, with the world.

As Section II of the paper should make clear, it will be very hard to implement this with CDs. The core problem with add-on DRM is that the CD content needs to be available in the clear to standard CD players. Consumers will have every incentive to elide pop-up windows requiring registration. But this is the standard method of doing business for online content services: create an account first, with credit card and other ID information, and buy second. Identity-based DRM is possible and the only question is how we will implement it. Look at three versions of this: Google Video, Amazon Upgrade, and Apple's iTunes.

A. Google Video

Go to Google Video (video.google.com) and look around. Thought that Super Bowl XL was dull? Maybe you would prefer to watch the commercials instead. Google Video has them, including the dreadful Burger King Whopperettes; the official version of the approved GoDaddy.com ad (it took them fourteen tries to get past the censors, and Google Video has four of the rejects); and my personal favorite, Richard Dean Anderson reprising his role as MacGyver for debit MasterCard, where he buys a bunch of miscellaneous household junk, including a $4 tube sock, which he uses to escape from his evil captors. (Lest there be confusion, the ad tells us: "Dramatization. Do not attempt.")

The commercials are free, but Google Video is also in the business of selling content—mainstream professional content, such as sporting events, as well as standard TV content both old—*I Love Lucy* and *The Brady Bunch*—and new, including *CSI* and *Survivor: Panamá*. And unlike iTunes with its one-price-fits-all policy, prices at Google Video move around. Single episodes of television shows are $1.99, just like at iTunes. But if you want to see Kobe Bryant knock down 81 points against the Toronto Raptors, it will set you back $3.95. *Charlie Rose* is a comparative bargain: almost a full hour of current TV for $0.99.

Google Video shows an acceptable but low-quality brief preview of the show alongside a chance to buy the higher-quality full version. Enter the usual credit card information—Google stores this for future purchases—and before you know it you are downloading. My first download was of an episode of *Star Trek Voyager* in which Captain Janeway and the crew find Amelia Earhart (her plane wasn't lost in 1937; she was abducted by aliens and put into cryostasis for 400 years, obviously).

Downloading what exactly? You initially see a downloaded video file of 708 bytes, but, assuming that you didn't select streaming, Google eventually stores the entire video file on your hard drive (177 megabytes for *Voyager*). You playback the download in Google's Video Player. You can try to open the file in the Windows Media Player, but it can't decode it. Google's FAQ notes that downloaded videos must be played in the Google Video player because some of the videos are copy-protected.

Files in hand—both the small files and the large content files—what can you do? That seems to depend on the settings of the file. The *Voyager* file is more controlled. When you click on it to see what happens—either the small file or the video contents file itself—you see a series of messages in the Google video player: connecting and creating the video file, buffering, determining file ownership, authenticating. If you have not stored a Google account cookie on your computer, you will be asked to log on to your Google account. If you have a cookie, Google will use the cookie to confirm your right to play the file. Either way, you need to establish a live Internet connection to play the video.[35] This means no video iPod. In contrast, you seem to establish rights to *Charlie Rose* once—single validation rather than per-use validation. You can watch it again if you must without being connected to the Internet.

What does that mean for file sharing? The small video files don't bring the content with them. If you move a small file to another computer and click on the file there, it will seek to make contact with the Google mothership. The file seems to remember your gmail address, but you have to insert your password. As to the video files, the *Charlie Rose* file plays in full without contact or a password (though in a degraded form, but that may been a result of burning the file to a CD and moving that file physically to a second computer). The *Voyager* video file phones home and needs password access to the account before playing.

This is one version of identity-based DRM, in many ways, a natural, conservative implementation of identity-based DRM. Absent the ability to strip the DRM from the downloaded file, anyone using the file needs access to the password to the Google account. But the downloaded video files are a natural target for unwrapping, and the purchaser of the file has no reason not to share the files with others. If the files came with access to the Google account—email and password—the file downloader would have a much stronger incentive to not share the file.

[35] *See* Google, Google Video Player Privacy Notice, http://video.google.com/support/bin/answer.py?answer=32170 (last visited July, 7, 2006).

B. Amazon Upgrade

Switch from video to text, and, in particular, the digitized book market. Google Book Search has received most of the attention—in the market and in the courts—but Amazon has announced two interesting programs: Amazon Pages and Amazon Upgrade.[36] Pages is a pay-per-page model. Want to read only the juicy parts of the latest tell-all? You could go to the bookstore and stand there flipping through the book with a clerk looking over your shoulder, but now, with Pages you can go legit: you can just search for "Monica Lewinsky," pay for the two pages you really want to see, and be done with it.

Amazon Upgrade is something else entirely: digital access to books purchased through Amazon. This is a really clever move by Amazon. They are changing the basic scope of the book business, which will put even more pressure on independent book sellers and even large operators like Barnes & Noble and Borders. And they have come up with a structure that should put meaningful limits on the sharing of digital texts.

Many readers—including me—want it both ways: the joy of reading books on paper and the search capability of books online. If I am actually going to take the time to read the whole book, I want to be able to maximize my use of it. A paper copy and a searchable digital copy will do just that. Amazon Upgrade does just that. The details are a little murky, but the core idea is buy the book, get the search service.

Buy a book from Amazon—one click shipped to you—and Amazon will sell you the right to search that book online at Amazon. Sell when? Just when I buy the book, as a bundle? Can I buy online access later? At the same price I could have paid at the time of purchase? Pay an annual fee and get access for all of my purchases through Amazon? None of that is particularly clear, and each approach might have different competitive consequences.

But focus instead on copyright and digital copies. Amazon doesn't seem to be selling digital offline copies with the paper copies. Instead, Amazon is selling a search service. Everything suggests that Amazon intends to do this with the consent of copyright holders, presumably for a split of the revenues.

The difference between service and product is substantial. If I downloaded a copy of the digital book, Amazon (and the copyright holder) would have to worry about what I do with the copy. Do I try to make other copies? If it is wrapped in some encryption via DRM software, do I strip off the wrapper and put the content into the open? Again

[36] *See* Press Release, Amazon.com, Inc., Amazon.com Announces Plans for Innovative Digital Book Programs That Will Enable Customers to Purchase Online Access to Any Page, Section, or Chapter of a Book, as Well as the Book in its Entirety (Nov. 3, 2005), *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=778248.

the darknet critique: It only takes one sophisticated person to break the encryption, and then the content can circulate freely. And the "size" of access required for digital text is quite different from that of video or music. You want all of the video or music, not frames or notes here and there. In contrast, a search service for digital text with access to chunks in response to search terms might suffice.

The service model limits that possibility considerably. Presumably, I will need to log on to Amazon with my account information to use the digital books that I have "purchased." For me to share my access with anyone else, I will have to give them full access to my Amazon account. I will probably do that with family members, and maybe a friend or two, but I won't do it with my 10,000 closest friends halfway around the world.

That was Napster and Grokster, but the Amazon service model gives me a strong incentive to control access to the copy. By linking access to the digital object to access to other attributes that I care about—my account information and the ability to ship books via one-click around the globe—the service model turns me into an honest trading partner. I don't have that same strong incentive with a digital book product.

C. iTunes

iTunes, a separate download available on Apple's website, is the key software for the iPod universe.[37] It is the software interface to the iPod through which content is put on the iPod. iTunes is also an online content store, originally music and now music and video. Let's go shopping. As I open the iTunes Music Store, I see at the top a list of featured albums. Click on one—*Unwritten* by Natasha Bedingfield—and iTunes switches to a new window. We see the album cover, basic release info (an album with 14 songs released on August 2, 2005), and a series of buttons—"Gift This Music," "Artist Alert," and "Tell a friend"—plus, most importantly, a button to buy the album for $9.99. But iTunes also sells each of the separate 14 tracks as singles for 99 cents each. Want just the title track? Click, pay—through previously provided account info—and download and you "own" the *Unwritten* single that you just made.

As good shoppers, we should comparison shop at Amazon. A search on music on "unwritten Natasha Bedingfield" pulls up 14 items, plus sponsored links for ringtones. It isn't immediately obvious what the 14 different items are, but two jump out at you. The last one on the list is the Sony XCP copy-protected version of the CD, listed as currently unavail-

[37] *See* Apple, iTunes 7, http://www.apple.com/itunes/overview/ (last visited Sept. 26, 2006).

able. The first one looks like the album cover that we saw at iTunes, so click there. And that version is the August 2, 2005 release, 13 tracks, for a price of $12.98, marked down $6.01 from the list price of $18.98. Amazon also offers a link to used versions of the CD, starting at a low price of $7.99. (A bit of a mystery: Amazon lists 13 tracks, iTunes 14 with the fourteenth being a song listed as a hidden track.)

Two points should jump out immediately. First, online delivery changes the cost structure of delivering content. No CDs, no jewel boxes, no stacks of inventory sitting around. Although estimates of savings differ, many believe that the drop in the costs of delivering content are substantial. The prices reflect this: $9.99 at iTunes vs. $12.98 at Amazon, plus shipping. Second, we can unbundle the album and sell songs song by song. This allows consumers to choose only the songs that they want. Even when singles were popular, only a limited number of singles were produced. Now on iTunes, every album brings with it its own singles. That gives rise to some tricky pricing issues, but I won't explore those here (so what price would you need to set for the singles such that the anticipated revenue sales for the album and the singles is not less than would have been earned had the album been sold only bundled). Unbundling also means that songs can be released faster and an artist need not wait until 14 songs have been amassed to release any one of them.

iTunes also sells video for playback on the video iPod or on a computer. For video, single items sell for a $1.99; be it a 21-minute episode of NBC's *Scrubs*, 43 minutes of *Desperate Housewives* or a 4-minute Pixar short. iTunes also sells a season pass to a particular show—good for all episodes of a particular season—for $34.99. There is a lot that is strategically interesting about the video on iTunes and we should examine that briefly to understand what is at stake for digital rights management on iTunes.

Start with cable bypass. The over-the-air broadcast networks would love to restore a direct relationship with their viewers. Right now, between cable TV and satellite, roughly 85% of U.S. viewers receive broadcast TV through an intermediary. Cable bypass means that the broadcasters have figured out a way to cut out the cable and satellite companies. iTunes is one path to bypass, though, of course, serious use of iTunes means a broadband connection, and for now at least, broadband comes from the cable company or as DSL from the local phone company.

For premium cable networks, online video makes it possible to unbundle the channel and make it easy for viewers to sample hot premium cable shows. Showtime is making some of its content available on iTunes. Premium cable channels are typically purchased by the month, and you pay a flat amount regardless of how many shows you want. On iTunes, if you just want to watch Kirstie Alley in *Fat Actress*, you can buy it episode by episode.

The irony is that while the Federal Communications Commission has been pushing cable networks to create family-friendly cable tiers or else[38]—the else is mandatory à la carte pricing—per-show pricing has come to iTunes. iTunes sells content from both the Disney Channel and MTV, but you can spend your money on Disney and never spend a dime on MTV.

We should now head inside iTunes and consider briefly how Apple has approached DRM.[39] Apple's DRM is called "FairPlay" and it is identity-based. Purchased songs can be copied to an unlimited number of computers, but only five computers at a time can play the songs. This is unlimited copying, limited use, and is implemented through an authorization process that amounts to assigning an identity to particular computers. Authorization is simple: "To authorize a computer, simply play a purchased song on your computer. The first time you authorize your computer, you'll need to enter your iTunes account name and password."[40] So the songs are freely sharable, but only someone with access to your account information can actually play the songs, and you can only authorize five computers. Again, like Google Video, a content purchaser isn't affirmatively discouraged from sharing the content—there is no DRM bounty—so songs can be shared and subject to unwrapping by clever decryptors.

D. Implementing Identity-Based DRM

Focusing on the choices that we need to make in implementing identity-based digital rights management one choice is local storage (downloading) vs. remote storage (streaming). That choice will take into account the relative costs of storage and bandwidth. A download model means that the content is delivered once and is stored on the central server and on each consumer's computer. A streaming model means that bandwidth is used each time the content is used. Listen to the song once, use bandwidth; listen to it 100 times, use 100 times the bandwidth.

Another question is frequency of validation. A streaming model presumably does one-to-one validation, meaning that your right to use the song is confirmed with each use. It would be difficult to give you access to the song without knowing who you were. Note, of course, that validation doesn't mean that we can tell that you are you: it just means

[38] *See* Press Release, Chairman Kevin J. Martin's Statement on the Announcement That Cable Companies May Voluntarily Offer Family Tiers (Dec. 12, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-262676A1.pdf.

[39] *See generally* BERKMAN CENTER FOR INTERNET & SOCIETY, *supra* note 13.

[40] Apple, iTunes Music Store Customer Service: Authorizing Your Computer, http://www.apple.com/support/itunes/musicstore/authorization/ (last visited Sept. 26, 2006).

that the remote computer seeking to access the song is presenting authentication information that matches with the access rights to the content.

In a downloading model, validation is a choice. An online seller could require validation each time the downloaded content is used. For example, for some content, Google Video downloads the content to the consumer's computer but still confirms that access is allowed with each use. In contrast, Apple's iTunes contemplates that content will be downloaded to a computer and then loaded on an iPod. The iPod cannot make contact to the Internet on its own—it isn't a networked device—and so content is used without per-use validation.

We can start to see the stresses in this system. Per-use validation of the sort seen in Google Video limits use of the content to networked devices, meaning no video iPod. Per-use validation will raise privacy issues,[41] but per-use validation means that the person using the content has to have access to the account information. Access and identity travel together. In contrast, if content can be downloaded and used without validation—meaning without use of the account information—then we quickly come back to the world of locked-down DRM. This isn't music CDs where it will be hard to get consumers to implement the DRM in the first place. But it does mean that if the consumer can strip off the DRM, the content will move into the clear and can be used by anyone, even someone without the account information.

But, you should say, haven't we just changed the amount of stripping that needs to be done? If content from iTunes comes with DRM designed to prevent p2p distribution and content from Google Video comes with DRM designed to require per-use validation, don't we still face the core problem that professional DRM breakers will strip both of these? That will unwrap the content from the DRM and allow it to enter p2p networks free of the DRM restrictions.

That is why we need to switch approaches by embedding identity with the content. Content producers want to raise the cost of uploading content to p2p networks. They have tried to do that with locked-down DRM and have largely failed, and they have tried to raise costs through lawsuits. But we should instead try to harness the incentives of the content purchasers. We should want to make them as careful with content as they would be with their own identities.

Switch to identity-based DRM with incentives. Recall the idea: content is tagged with a version of my identity and a bounty. Turn in the bounty, collect a reward. The point isn't that this information couldn't be stripped by the dedicated decryptor but rather that the content purchaser should fear that the decryptor will not have the incentive to remove the

[41] Posting of Ed Felten to Freedom to Tinker blog, *Google Video and Privacy*, http://www.freedom-to-tinker.com/?p=956 (Jan. 20, 2006, 9:34 EST).

bounty but will instead use it. Plant fear, uncertainty, and doubt—introduce suspicion into p2p networks—and see what happens. Mistrust-based DRM would change the incentives to upload and share with strangers. You might be perfectly happy to give copies of songs tagged with the bounty ID to family members and close friends, but almost certainly not the strangers.

Here is where the ID bounty model makes a difference. With locked-down DRM, the content purchaser and the computer hacker have symmetric interests in wanting to see the encryption scheme broken. The DRM scheme limits uses that the consumer might wish to make. Remove the restrictions and the consumer can do more, and if at the same time that means that the song is available throughout the world on a p2p network, who cares?

In contrast, with ID-bounty DRM, the interests of the CD purchaser and those of the professional decryptor and the peers in the p2p network may diverge. The CD purchaser may not be confident that a decryptor will want to be as careful with the bounty as the purchaser would be. The uncertainty about whether the bounty has been stripped from the file might introduce a substantial cost to uploading. We have all learned that when we delete a file on our computer it's really still there; actually removing it is much more work. In similar fashion, professional decryption software might leave a residue of the bounty, which another smart professional decryptor might recover and collect on.

CONCLUSION

The powerful shift in copying technology over the last thirty years has destabilized how we produce copies and the economic arrangements associated with prior technologies. These technological changes have created a broad shift in the ability to make copies, moving control away from producers towards consumers. As a consequence, these technologies have altered the practical enforceability of the rights that law assigns to copyright owners.

Digital rights management technologies are an effort to make meaningful the legal rights of copyright owners. DRM faces severe obstacles. For preexisting products like the music CD, it has proven to be very difficult to add DRM after the fact. CDs need to work in standard CD players, and that limits DRM. The firestorm over Sony BMG's effort to produce CDs subject to DRM suggests that we are unlikely to see meaningful DRM for music CDs soon.

But we are switching how we deliver content from products to services. Music CDs and eventually DVDs will be replaced by online services such as Apple's iTunes and Google Video. Both of these come with DRM built-in and both rely on identity-based DRM. Identity-based

DRM ties identity to content. Content can be shared widely, but absent access to identity, the content is worthless.

This is a substantial step forward for DRM, but may still be a step short of where we need to be. Content purchasers still have no reason to protect purchased content. Identity-based DRM coupled with bounty tags will create an incentives wedge between content purchasers and stripping/p2p software and with peers in a p2p network. We should want a system where content purchasers are as careful with content as they would be with identity, and mistrust-based DRM may be that system.