ARTICLE

DRM INTEROPERABILITY

HIRAM MELÉNDEZ-JUARBE[*]

I. INTRODUCTION ....
II. THE IMPORTANCE OF FLEXIBLE PERSONAL USE OF CONTENT AND INTEROPERABILITY ....
A. The Case for Flexible Personal Use and Against the Limits Imposed by DRMs and the DMCA ....
B. The Value of Interoperability ....
III. STATE OF AFFAIRS ....
A. Limited Technical Overview and Technological Proposals ....
B. Incompatible Systems ....
C. Why Incompatible? ....
1. Copying, digital goods and DRMs ....
2. Network effects, interoperability and standards ....
IV. STANDARDS AND CONVERTERS ....
V. TRENDS AND CONCLUSION ....

I. INTRODUCTION

Netflix is an online DVD rental service that delivers movies to clients by mail and also allows them to watch movies directly in their computers. A client watching a streaming movie cannot edit, copy, or paste selections of the movie into other works. The client cannot download the film to watch offline nor save it to enjoy after her membership is expired. She will only be able to watch it according to the terms and interplay of Digital Rights Management ("DRM") technologies that operate in her computer, the digital movie file, and on Netflix's servers.

A client visiting Netflix using a Windows-based computer will be able to

[*] Associate Professor, University of Puerto Rico Law School. BA, University of Puerto Rico (1997); JD, University of Puerto Rico Law School (2000); LL.M., Harvard University Law School (2002); LL.M. New York University Law School (2008); JSD Student New York University Law School. I am grateful to Rochelle Dreyfuss, Katherine Strandburg and students at NYU Law School's 2008 Innovation Policy Colloquium for their insightful comments and criticism. I am also indebted to Helen Nissenbaum for helping me think about the many ways in which values are embedded in information and communication technologies. All errors are, or course, mine. I can be reached at www.elplandehiram.org.

enjoy both of the site's services: DVD renting and movie streaming. For the same monthly fee, until recently, a client with an Apple computer could only rent DVDs by mail and not benefit from movie streaming because Apple's DRM was incompatible with Netflix. If a Mac user attempted to stream a movie via Netflix, she would get the following message:

> Our apologies — instant watching is currently not supported for Macintosh.
>
> . . . We're required to use Digital Rights Management to protect movies watched instantly online, and right now we only have approval for this protection on Windows Operating systems, not the Mac.
>
> Apple does not license their DRM solution to third parties, which has made this more difficult, but we are working with the studios and content owners to gain approval for other solutions. As soon as a studio-approved DRM for the Mac is available to us, whether from Apple or another source, we will move quickly to provide a movie viewer that enables you to watch movies from Netflix instantly on your Mac. . . .[1]

While Microsoft's DRM has always been fully interoperable with Netflix-streamed content, Apple's has not. There is no real technological barrier – this is simply the result of Apple's decision not to license its technology to Netflix and Microsoft's decision to do so.[2] This scenario is just one example of the many instances of DRM incompatibility that populate the entertainment and software businesses. This lack of interoperability presents a significant concern both from the consumer's perspective and from a broader innovation policy standpoint. This article aims to examine the problem of lack of interoperability in the context of Digital Rights Management systems, and hopes to shed some light on the causes and effects of this state of affairs.

DRMs are largely used by copyright owners to control the use of digital products, such as music and video files, as well as software of any kind. As they are currently employed, DRMs limit a person's potential experience with digital products in two prominent ways.

First, DRMs limit the range of uses a person can make with digital content as a result of DRMs' *de facto* aggrandizement of copyright owners' control over content. Such control exceeds rights recognized by the copyright regime. Specifically, DRMs enable copyright owners to extend their reach to private and personal uses of digital goods to a degree not previously possible in the

[1] *See* Perfetti Media, *Netflix: Always Thinking About Their Customers – Even When They Can't Help*, http://www.perfettimedia.com/user-experience/netflix-always-thinking-about-their-customers-%E2%80%93-even-when-they-cant-help (last visited Feb. 7, 2009); Netflix Community Blog, *Instant watching on Mac, Firefox, and more*, Aug. 9, 2007, http://blog.netflix.com/2007/08/instant-watching-on-mac-firefox-and.html.

[2] On October 31, 2008, Netflix announced the availability of a Beta program for Intel-based Mac clients to watch instantly movies using Microsoft's Silverlight software. *See* Netflix Blog, *Opt-In for the Netflix Movie Player*, http://blog.netflix.com/2008/10/opt-in-for-new-netflix-movie-player.html, October 31, 2008 (last visited, Nov. 11, 2008).

analog world.

Second, because DRM technologies emerge in a network market, there is currently vigorous competition among firms to establish their technology as the dominant DRM and get the benefit of tipping effects (the "tendency of one system to pull away from its rivals in popularity once it has gained an initial edge").[3] Consequently, this network market results in a wide range of incompatible DRM technologies and, hence, a host of products that are able to interoperate with some DRM-enabled media, but that cannot interoperate with digital goods that use competing DRM standards. This lack of interoperability creates an inconvenience to users and significantly limits users' experiences with digital information goods.

Although lack of interoperability limits a user's experience, DRM interoperability is not always desirable. To the extent that interoperability increases the network of devices and content within the reach of copyright owners, a world with interoperable DRMs may consequently aggrandize content control and further expand copyright owners' *de facto* rights at the expense of otherwise legitimate personal uses. In this sense, a user must figure out how to increase interoperability between digital goods and devices while, at the same time, retain a significant measure of flexibility of personal non-commercial use of content. With this in mind, this article proceeds as follows: Part II makes the case for the dual goals of use flexibility and interoperability. Temporarily bracketing the issue of how to combine flexible use with a DRM-rich digital environment, Part II examines (a) the value of flexible use of content and how current DRMs limit user creativity and innovation and (b) the value of interoperability both from the perspective of user creativity and technological innovation.

Part III examines the current disjointed state of affairs in the DRM context. Because DRMs allow copyright owners to monetize and control the use of content, it is reasonable to think that interoperability would be in their best interests becuase it allows increased and diverse inter-platform monetizable uses. Thus, interoperability seems intuitively congruent with the business models made possible by DRMs. Yet, there has not been much progress in developing interoperable DRMs even when sufficient incentives exist. The aim of this part is to consider the technological and economic reasons that explain current low levels of DRM interoperability.

Finally, the Part IV examines different technological and policy alternatives to break this interoperability deadlock in a way that is sensitive to users' rights and expectations and points to future research avenues.

In all, the aim of this article is to bring clarity to this rather confusing area and suggest ways in which important values and innovation might be fostered in the DRM context.

[3] Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 105-06 (1994).

II. THE IMPORTANCE OF FLEXIBLE PERSONAL USE OF CONTENT AND INTEROPERABILITY

This part argues that both interoperability and a flexible realm of personal use of content are valuable policy goals that should be pursued. To what extent these two objectives can be reconciled is a more difficult question which I will address later.

A. The Case for Flexible Personal Use and Against the Limits Imposed by DRMs and the DMCA

Digital technologies allow individuals to make and distribute costless copies of information products with almost no loss in quality.[4] This is not the place to consider all the political implications of these technological advances. Suffice it to say that digitally networked technologies allow the development of what Professor Balkin of Yale Law School has called a *democratic culture* "in which individuals have a fair opportunity to participate in the forms of meaning making that constitute them as individuals."[5] This, in turn, fosters two important political values in ways that were not possible in an analog context: (1) a richer and more diverse cultural milieu;[6] and (2) the development of more autonomous individuals who are increasingly capable of becoming authors of their lives and their cultural environment.[7] As explained by William Fisher:

[4] WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW AND THE FUTURE OF ENTERTAINMENT 11-18 (2004).

[5] Jack Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 3 (2004).

[6] *See* NEIL WEINSTOCK NETANEL, COPYRIGHT'S PARADOX (2008). For related discussions on how to accommodate freedom of speech values within copyright law, *see generally*, Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561 (2000); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 389 (1999); Eugene Volokh & Brett McDonnell, *Freedom of Speech and Independent Judgment Review in Copyright Cases*, 107 YALE L.J. 2431 (1998); Eugene Volokh, *Freedom Of Speech And Intellectual Property: Some Thoughts After Eldred, 44 Liquormart, And Bartnicki*, 40 HOUS. L. REV. 697 (2003); Diane Leenheer Zimmerman, *Is There A Right To Have Something To Say? One view of the public domain*, 73 FORDHAM L. REV. 297, 363-65 (2004); Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1 (2001); Rebecca Tushnet, *Copyright as a Model for Free Speech Law: What Copyright Has In Common with Anti-Pornography Laws, Campaign Finance Reform, and Telecommunications Regulation*, 42 B.C. L. Rev. 1 (2000).

[7] *See* NEIL WEINSTOCK NETANEL, COPYRIGHT'S PARADOX (2008); C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH (1989). *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006); LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

> [O]pportunities for creativity of this sort contribute to what has been called "semiotic democracy." Over the course of the twentieth century the power to make cultural meaning in most Western countries has become ever more concentrated . . . . Reversing the concentration of semiotic power would benefit us all. People would be more engaged, less alienated, if they had more voice in the construction of their cultural environment. And the environment itself . . . would be more variegated and stimulating. The new technology makes that possible.[8]

However, the same features of digitization that allow greater human creativity threaten copyright owners' interests in their works. It is, thus, only natural for them to seek broader mechanisms, both legal and technological, to protect these interests.[9] As a consequence, content owners are today capable of controlling individual use of works well beyond their legitimate claims of copyright, affecting otherwise protected personal non-commercial use of content,[10] works in the public domain,[11] and works that could otherwise benefit from the first sale doctrine.[12]

This technological control is significantly empowered by the Digital Millennium Copyright Act ("DMCA"), which severely punishes efforts to circumvent DRMs.[13] Section 1201(a) of the DMCA prohibits the circumvention of a "technological protection measure that effectively controls *access* to a work"[14] (or the manufacture or distribution of such technology) while section 1201(b) addresses the manufacture, distribution or traffic technologies primarily designed to circumvent a Technological Protection Measure ("TPM") "that effectively *protects a right of the copyright owner*."[15]

A TPM "effectively controls access to a work" if it "requires the application of information, or a process or a treatment, . . . to gain access to the work."[16]

[8] FISHER, *supra* note 6, at 30-31.

[9] As Balkin explains: "The very same features of the digital age that empower ordinary individuals also lead business continually to expand markets for intellectual property and digital content. Yet as businesses do so, they must deal with features of the digital age that empower consumers and give them new abilities to copy, distribute, and manipulate digital content." Balkin, *supra* note 7, at 14.

[10] L. Ray Patterson and Christopher M. Thomas, *Personal Use In Copyright Law: An Unrecognized Constitutional Right*, 50 J. COPYRIGHT SOC'Y U.S.A. 475, 478-81 (2003); Pamela Samuelson, *Copyright And Freedom Of Expression In Historical Perspective*, 10 J. INTELL. PROP. L. 319, 331-32 (2003).

[11] *See generally* Timothy Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49 (2006); Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 57 (2001).

[12] 17 U.S.C. § 109(a) (2000).

[13] 17 U.S.C. § 1201.

[14] 17 U.S.C. § 1201(a).

[15] 17 U.S.C. § 1201(b) (emphasis added).

[16] 17 U.S.C. § 1201(a)(3)(B).

Hence, a person circumvents a TPM when decrypting a TPM that controls *access* to a work even when the person has a legal right to enjoy it.[17] In this sense, the DMCA prevents users from breaking those technological measures even if they have purchased a copy of the work, which essentially furnishes to copyright holders the right to control whether and under what circumstances a person can enjoy a work.

The DMCA has some exceptions that permit user circumvention in a limited set of cases. Section 1201(f) specifically allows reverse engineering of a TPM "for the sole purpose of identifying and analyzing those elements of [a computer] program that are necessary to achieve interoperability with other programs."[18] This exception, however, is only available to make interoperable two different computer programs - not a computer program with digital content such as music or video. Also, the exception is only available if (a) the elements that are discovered through reverse engineering "have not been previously readily available to the person engaging in the circumvention" and (b) to the extent that the acts of "identification and analysis do not constitute infringement."[19] As interpreted by federal courts, this exception is very limited, as circumvention is prohibited even when made for interoperability purposes if other objectives are sought concurrently.[20]

Also, even though the DMCA's provisions are presumed to not "affect

[17] Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 303-04 (SDNY 2000) (In this case the court declared that the use of a software (DeCSS) that was designed to access the content of a legitimately acquired DVD in order for the DVD to be played in a Linux OS computer was a violation of the DMCA).

[18] 17 U.S.C. § 1201(f)(1).

[19] *Id.* *See* Davidson & Assoc. v. Jung, 422 F.3d 630, 639-42 (8th Cir. 2005) (finding the exception inapplicable because the act of circumvention of technological protection measures of an online game facilitated independent infringement by third parties who were able to make unauthorized copies of the game through defendant's service). *See generally*, Aaron K. Perzanowski, *Rethinking Anticircumvention's Interoperability Policy* (September 6, 2008). UC Davis Law Review, Forthcoming. Available at SSRN: http://ssrn.com/abstract=1224742.

[20] *See* Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000) ("[I]t is important to recognize that even the creators of DeCSS cannot credibly maintain that the "sole" purpose of DeCSS was to create a Linux DVD player. DeCSS concededly was developed on and runs under Windows—a far more widely used operating system. The developers of DeCSS therefore knew that DeCSS could be used to decrypt and play DVD movies on Windows as well as Linux machines. They knew also that the decrypted files could be copied like any other unprotected computer file. Moreover, the Court does not credit Mr. Johansen's testimony that he created DeCSS solely for the purpose of building a Linux player. Mr. Johansen is a very talented young man and a member of a well known hacker group who viewed "cracking" CSS as an end it itself and a means of demonstrating his talent and who fully expected that the use of DeCSS would not be confined to Linux machines. Hence, the Court finds that Mr. Johansen and the others who actually did develop DeCSS did not do so solely for the purpose of making a Linux DVD player if, indeed, developing a Linux-based DVD player was among their purposes.").

rights, remedies, limitations, or defenses to copyright infringement, including fair use"[21] some courts have found that the DMCA is independent from the fair use defense, finding circumvention liability even in the face of a potential fair use.[22] Furthermore, state contract law acts as an extra layer of legal protection for DRMs, as terms of use agreements restrict consumers' ability to experiment with such technologies. Standardized contracts of this sort have been upheld as a matter of state law by some courts.[23] They are not considered to be preempted by federal law, and are thus enforceable,[24] despite their similarity to a private system of copyright legislation.[25] Therefore, even in the absence of the DMCA, private contractual agreements prohibiting circumvention of TPMs are largely enforceable in state courts.

These legal and technological developments have created a new regime of rights that go beyond those rights listed in the Copyright Act.[26] As Professor Ginsburg has explained, the DMCA has created a new right to control *access* to works.

> Every act of perception or of materialization of a digital copy requires a prior act of access. And if the copyright owner can control access, she can condition how a user apprehends the work, and whether a user may make a further copy.[27]

Because of this legal regime, DRMs allow content owners to control activities that were not possible to regulate in an analog world, such as whether, when, and for how long an individual can open, play, view, or edit a work in private.[28] Therefore, DRMs allow copyright owners to monetize uses

[21] 17 U.S.C. § 1201(c) (2000).

[22] *See* Universal City Studios v. Reimerdes, 111 F.Supp2d 294, 321-24 (S.D.N.Y. 2000); Realnetworks, Inc. v. Streambox, Inc., 2000 WL 127311, at *8 (W.D. Wash. 2000). *But see* Lexmark v. Static Control Components, 387 F.3d 522, 533-53 (6th Cir. 2004); Chamberlain Group, Inc. v. Skylink Tech. Inc., 381 F.3d 1178, 1202-03 (Fed. Cir. 2004) (requiring that the protection against circumvention technology under § 1201(a) be related to copyrighted work).

[23] Davidson & Assoc. v. Internet Gateway, 334 F.Supp. 2d 1164, 1176-78 (E.D. Mo. 2004). *But see* Speecht v. Netscape, 306 F.3d 17, 35 n. 18 (2d Cir. 2002).

[24] ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454-55 (7th Cir. 1996).

[25] *See generally* Julie Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998). As the Progressives demonstrated in the heyday of *Laissez Faire* fever, private rules of governance are no less public than legislated rules when private arrangements depend on state enforcement of property and contractual entitlements. *Id. See generally* Robert L. Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. QUARTERLY 470, 470 (1923).

[26] 17 U.S.C. § 106 (2000).

[27] Jane Ginsburg, *From Having Copies to Experiencing Works: The Development on an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC'Y USA 113, 115 (2003).

[28] *Id.* at 120-21. *See also* Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 355-58 (2004) (describing the development of a

of content in ways not possible in an analog world and intrude upon what Professor Litman calls "copyright liberties,"[29] curtailing essential flexible personal non-commercial use (which includes "[r]eading, listening, viewing, and their modern cousins watching, playing, running, and building").[30] These personal use liberties are necessary for individual experimentation and innovation in the cultural realm.

B. The Value of Interoperability

The purpose of this section is to make the case for interoperability in the DRM context as a general policy matter. However, because the value of interoperability will become more clear upon examination of the current state of affairs, I will only generally outline this theme to gain some perspective.

In general terms, Information and Communications Technology ("ICT") interoperability means "the ability to transfer and render useful data and other information across systems . . . applications, or components."[31] But general definitions that try to embrace too much, as is usually the case, end up conveying too little. As one technical paper accurately describes, "[i]t seems that everyone has a notion of what interoperability means, which generally revolves around the idea of 'things' working together."[32] While it is possible to talk about interoperability in broad terms, this concept means different things to different stakeholders in different contexts.[33] As recognized by a recent Berkman Center study on ICT interoperability, any general definition "needs to be 'enriched' by adding context-specific definitional elements and is given life by the viewpoint of a variety of stakeholders. . . "[34] Furthermore, "various stakeholders often have different perspectives on and divergent

copyright system of privatized property rights); *and* Zohar Efroni, *A Momentary Lapse of Reason: Digital Copyright, the DMCA and a Dose of Common Sense*, 28 COLUM. J.L. & ARTS 249, 273-79 (2005).

[29] Jessica Litman, *Lawful Personal Use*, 85 TEXAS L. REV. 1871 (2007).

[30] *Id.* at 1893.

[31] Urs Gasser & John Palfrey, *Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation*, BERKMAN PUBLICATION SERIES (Nov. 2007), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-breaking-barriers_1.pdf.

[32] Gregory L. Heileman & Pramod A. Jamkhedkar, *DRM Interoperability from the Perspective of a Layered Framework*, DRM 2005: PROCEEDINGS OF THE 5TH ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT, at 20 (2005).

[33] For technical perspectives on interoperability *see* Gelareh Taban, Alvaro A. Cárdenas & Virgil D. Gligor, *Towards a Secure and Interoperable DRM Architecture*, DRM '06: PROCEEDINGS OF THE ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2006); Rob H. Koenen, Jack Lacy, Michael MacKay & Steve Mitchell, *The Long March to Interoperable Digital Rights Management*, PROCEEDINGS OF THE IEEE (2004), *available at* http://www.intertrust.com/main/research/whitepapers/Interoperable_DRM.pdf.

[34] Gasser & Palfrey, *supra* note 33, at 4.

incentives with regard to interoperability."[35]

In the specific context of DRMs, interoperability means "the relative ability of different systems, applications, or components - usually provided by multiple vendors - to work together in a way that is satisfactory to the relevant users of the system, application, or component."[36] Simply put, DRM interoperability gives a user flexibility to use DRM-protected content with different applications and devices.[37]

Because a technological problem "is only defined as such when there is a social group for which it constitutes a 'problem,'"[38] DRM interoperability has different meanings and implications depending on the relevant stakeholders.[39] For *users*, interoperability implies the flexibility to "choose among different services that offer DRM-protected content, which in turn can be used with different applications or on different devices."[40] From the perspective of the *content provider* it means that "content and rights can be 'cleared' once and distributed over the most efficient distribution channel, without being locked into a gatekeeper-like distribution channel."[41] For the *distributor* of content, "DRM interoperability ensures that its technology choice doesn't affect the utility of its service to users, as the delivered content might be played by any application and device."[42] And for the device *vendor* it means "that her products work with different services, or (more generally) that one system's component can be replaced by a component from another vendor."[43] Thus, for example, in the case of Netflix's movie streaming service, interoperability has meaning and value to the user who desires use flexibility and semiotic democracy, as well as to Netflix which is looking to increase consumer base and services. These meanings and values are different from those of the computer vendor who may[44] or may not[45] desire its machine to interoperate

[35] *Id.* at 5.

[36] Urs Gasser & John Palfrey, *DRM-protected Music Interoperability and eInnovation*, Berkman Publication Series 6 (Nov. 2007), http://cyber.law.harvard.edu/interop/pdfs/interop-drm-music.pdf.

[37] *Id.* at 6-7.

[38] Trevor J. Pinch & Wiebe E. Bijker, *The Social Construction of Facts & Artefacts: or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*, 14 Social Studies of Science 399, 414 (1984) ("In deciding which problems are relevant, a crucial role is played by the social groups concerned with the artefact, and by the meanings which those groups give the artefact.").

[39] Gasser & Palfrey, *supra* note 38, at 7.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] As is the case of Microsoft's Windows Media DRM Technology, *see* Microsoft, *Licensing Windows Media DRM Technologies*, http://www.microsoft.com/windows/windowsmedia/licensing/drmlicensing.aspx (last visited Jan. 31, 2009).

with the competition and the content provider who may want to ensure that all DRM-enabled devices comply with certain security standards.

Because these perspectives are not necessarily aligned (and may sometimes be completely at odds), it is difficult to assess the general value of interoperability in the abstract. There are, however, several benchmarks against which one can generally evaluate its significance. Following the Berman Center's study, one can consider the importance of interoperability according to the following three sets of values: (1) autonomy, choice and flexibility; (2) cultural diversity; and (3) competition and innovation.[46]

The first two values have already been mentioned in the previous section and it is clear that they may be served by interoperability. Low levels of interoperability tend to reduce users' choices in the selection of content, services and devices: "If DRM systems and applications are not interoperable, . . . users cannot freely choose among competitive and efficient options with regard to components that may be tested, mixed, and matched for specific purposes."[47] On the other hand, to the extent that lack of interoperability increases users' transaction costs when experimenting with digital products, the development of digital content may be hampered, which may have a negative effect on cultural diversity.

The impact of DRM's interoperability on the values of innovation and competition is harder to gauge and will be the subject of a subsequent section.[48] It is difficult to determine *ex ante* and without regard to the particular context whether DRM interoperability spurs innovation. For now, it is sufficient to generally state that because DRM technologies emerge in a network market, there is intense competition between firms to furnish the dominant DRM standard. While this may foster innovation and competition *for* the DRM market prior to tipping, it also increases the variety of incompatible DRM systems. Hence, vendors and users of one type of DRM-related products may be locked into products that are incompatible with competing products. This may impact user creativity and innovation. On the other hand, if there are high levels of DRM interoperability, competition (and hence innovation) might be encouraged between products *within* the market and not *for* the market.

Nevertheless, when interoperability is accomplished by tipping in a network market, the winner would probably seek "to charge other market players to interoperate or even to re-use basic ideas involved, based upon sheer market strength,"[49] creating burdensome entry barriers to the market. This situation

[45] *See Instant Watching on Mac, Firefox, and more* (Aug. 9, 2007), http://blog.netflix.com/2007/08/instant-wathcing-on-mac-firefox—and.html (referencing Apple's approach to video DRM interoperability).

[46] Gasser & Palfrey, *supra* note 38, at 24-29.

[47] *Id.* at 28.

[48] *See infra* Part III.C.

[49] John Palfrey, *Holding Out for an Interoperable DRM Standard, in* DIGITAL RIGHTS

may also leave stranded those consumers of smaller competitors whose products are not interoperable with the dominant firm.[50] However, the adoption of DRM standards available under reasonable and non-discriminatory licenses might ease these anti-competitive concerns.[51]

In all, regardless of our normative appreciation of DRMs as a policy matter, I agree with the Berkman Center that interoperability is a sound policy goal especially when considering how it impacts users' flexibility, choice and creativity as well as competition and innovation.[52] But one must be careful not to endorse DRM interoperability in the abstract. As this article demonstrates, DRM systems – interoperable or not – may be encoded with more or less permissive usage rules, and therefore be more or less protective of fair use and other personal freedoms. As a result, one must not unqualifiedly cheer for interoperability in the abstract, but for interoperability of a certain type of DRMs.

Having established the desirability of both DRM interoperability and user flexibility as public policy goals, this article turns to analyzing the current state of affairs in the DRM context. Its aim is to consider the technological and economic reasons that explain low levels of interoperability.

III. STATE OF AFFAIRS

This Part begins with a general overview of how Digital Rights Management systems operate, their components and technical goals. This technical explanation also considers some of the limitations of DRMs in encoding user flexibility as well as technical and policy solutions offered by some scholars. This background is useful to understanding the current state of affairs in the DRM world and the practical alternatives that combine the dual goals of DRM interoperability and personal flexible use of content.

A. *Limited Technical Overview and Technological Proposals*

Digital Rights Management systems and Technological Protection Measures have much in common, but are not the same. Ian Kerr defines TPMs as "technological method[s] intended to promote the authorized use of digital

MANAGEMENT: THE END OF COLLECTING SOCIETIES? 21 (Christoph Beat Graber et al., eds., 2005).

[50] *See generally,* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSPECTIVES, 93, 93-115 (2004).

[51] *See* Dan L. Burk, *Legal And Technical Standards In Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 569-70 (2005) ("Analyses of standard setting that rely upon open adoption of standards likewise assume that firms in the marketplace will be able to comprehend and mimic the standard through examination or reverse engineering of the products incorporating the standard. Under such conditions, the anticompetitive effects of network 'lock-in' will be at least somewhat ameliorated by the threat of new entry, so long as new entrants can adopt or adapt the standard.").

[52] Gasser & Palfrey, *supra* note 38, at 33-34.

works. This is accomplished by controlling access to such works or various uses of such works, including copying, distribution, performance and display."[53] DRMs, on the other hand, are "technology systems facilitating the trusted, dynamic management of rights in any kind of digital information, throughout its lifecycle and wherever and however it is distributed."[54] Thus, TPMs are about the *authorized* use of digital works, while DRMs are about the *management of asserted rights.* One example of a TPM is cryptography, which includes a means to control access to digital works without necessarily implying a particular assertion of rights or the management of legal rights.[55] DRMs, on the other hand, may or may not include TPMs. A digital system to manage rights over content does not necessarily control access. This is the case, for example, of the Copyright Clearance Center, where individuals purchase licenses via an online service.[56]

Other DRMs, however, extensively employ TPMs to manage asserted rights by controlling the use or access to content. These are, what Kerr calls, "TPM-Enabled DRMs."[57] The DRM literature usually is referring to TPM-Enabled DRMs when discussing DRMs. In this article I too use DRM to refer to TPM-Enabled DRMs.[58]

There have been many efforts to classify DRMs into different categories.[59] One observer divides DRM technologies into the following general categories:

[53] Ian Kerr, Alana Maurushat & Christian Tacit, *Technological Protection Measures: Tilting at Copyright's Windmill*, 34 OTTAWA L. REV. 7, 13 (2002-2003).

[54] *Id.* at 25.

[55] *Id.* at 25 n.70. *See also* JOAN VAN TASSEL, DIGITAL RIGHTS MANAGEMENT: PROTECTING AND MONETIZING CONTENT 77 (2006) (referring to Content Protection Technologies).

[56] Kerr et al., *supra* note 53, at 26 ("Many [Copyright Management Organizations] provide Internet and other online technologies to mediate the clearing of rights, establishment of license terms and payment of fees for the use of a work."); Copyright Clearance Center, http://www.copyright.com (last visited Feb. 1, 2009).

[57] Kerr et al. *supra* note 55, at 26.

[58] *Id.* There may be normative objections to the DRM rubric. To the extent that it may embody a normative claim of rights over the content and, to the extent that such claims are usually controversial, the DRM concept is value-laden. Accordingly, some refer to these technologies as "Digital Restrictions Management" or "Digital Restrictions Malware." *See* Richard Stallman, *Some Confusing or Loaded Words and Phrases that are Worth Avoiding*, http://www.gnu.org/philosophy/words-to-avoid.html#DigitalRightsManagement (last visited Feb. 1, 2009).

[59] *See, e.g.* VAN TASSEL, *supra* note 57; Niels Rump, *Digital Rights Management: Technological Aspects, in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 3 (Eberhard Becker, et al. eds., 2003); Kerr et al., *supra* note 55; Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 326-27 (2004); Center for Democracy and Technology, *Evaluating DRM: Building a Marketplace for the Convergent World* (Sept. 2006), http://www.cdt.org/copyright/20060907drm.pdf.

1. Ancillary DRM technologies
2. Technologies that protect *access* to the content
3. Technologies that limit the *copying* of content
4. Technologies that limit *transporting* the content from one device to another.

I have labeled as *ancillary* DRMs those technologies that play a role in a DRM system by lending support to other technologies that control access, copying or movement of digital goods. One example of an ancillary DRM is *identification technology*. With these DRMs copyright owners can mark content in order to identify it and thereby track its distribution. They can be used to mark the original copy as well as subsequent reproductions with the same marking or to uniquely mark each copy distributed with *unique identifiers* that are included in the digital work's metadata (which includes information on the time, place, date of creation, and specific authorized user).[60] Unique identifiers can, in turn, be integrated with another kind of identification technology: watermarking.

Watermarking and its related technology, fingerprinting, are at the cutting edge of DRM technology.[61] *Digital watermarking* technologies "are composed of scattered bits of 'noise' that are permanently embedded in each audio or video frame."[62] This allows tracing of marked copies back to the original purchaser of the copy.[63] Markings should survive even after the

[60] The Society of Motion Pictures and Television Engineers (SMPTE) has adopted one of these identifier systems as a standard (the Unique Material Identifier, SMPTE 330M) for the identification of audio-visual content)..Center for Democracy and Technology, *Evaluating DRM: Building a Marketplace for the Convergent World* (Sept. 2006), at 80, http://www.cdt.org/copyright/20060907drm.pdf.

[61] The leading industry blog on DRMs opened on October 24, 2007 and included an entire section dedicated to watermarking and fingerprinting technologies: "Watermarking and fingerprinting are distinct yet synergistic technologies. Their importance in the world of digital content rights is growing rapidly; in time, they may become more important than encryption-based DRM technology in certain media market segments. That's why we are now devoting a section of DRM Watch to this fascinating topic as we continue to broaden our coverage beyond the narrower definitions of DRM." Bill Rosenblatt, *New DRM Watch Section on Watermarking and Fingerprinting*, (Oct. 24, 2007), http://www.drmwatch.com/watermarking/article.php/3706996. *See also*, Patrick Wolf, *Complementing DRM with Digital Watermarking: mark, search, retrieve*, 31 Online Info. Rev. 10, (2007); Marcel Fernández, Josep Cotrina-Navau & Miguel Serrano, *A Class on non-linear asymptotic fingerprinting codes with ε-error*, 31 Online Info. Rev. 22 (2007); Fabien Peticolas, *Digital Watermarking, in* Digital Rights Management: Technological, Economic, Legal and Political Aspects, 81 (Eberhard Becker, et al. eds., 2003); Jurgen Herre, *Content Based Identification (Fingerprinting), in* Digital Rights Management: Technological, Economic, Legal and Political Aspects, 93 (Eberhard Becker, et al. eds., 2003).

[62] Van Tassel, *supra* note 57, at 83.

[63] Patrick Wolf, *supra* note 65, at 12.

digital copy is recorded by analog means.[64] *Digital fingerprinting*, on the other hand, embeds nothing into the content.[65] Instead, fingerprinting identifies works by analyzing their characteristic features. Because of this feature, fingerprinting is theoretically able to survive conversion into analog format; plugging the so-called "analog hole,"[66] which explains the current popularity of this technology in the industry.[67]

In the *ancillary* DRM technologies category I also include a crucial technology for interoperability: Rights Expression Languages ("RELs").[68] RELs are technical languages that have specific syntax (grammar) and semantic (vocabulary) rules for expressing a range of permitted and non-permitted uses.[69] Current RELs are capable of expressing many fields of permissions for any given content. These include the kind of uses allowed (copy, print, play), if the content can be reused or transferred, who the allowed users are, the types of devices allowed to play or exhibit the work, and when the content can be used (e.g., a time frame), among other things.[70]

[64] VAN TASSEL, *supra* note 57, at 83.

[65] Rosenblatt, *supra* note 65 ("Fingerprinting is a set of techniques for analyzing content, reducing its unique characteristics to a set of one or more numbers that serve as 'fingerprints,' and looking those fingerprints up in a database to determine the identity of the content.").

[66] The "analog hole" concept describes the fact that digital content must be presented to users in an analog form since humans do not perceive images and sounds digitally (yet!). Patrick Wolf, *Complementing DRM with Digital Watermarking: mark, search, retrieve*, 31 ONLINE INFO. REV. 10, 11 (2007).

[67] The content industry has invested considerable resources in these technologies, particularly digital fingerprinting for video content, and has pressured user-generated sites such as You Tube, MySpace and Veoh to incorporate them. Bill Rosenblatt, *Video Content Owners and User Generated Content Sites Agree on Filtering Principles*, Oct. 25, 2007, http://www.drmwatch.com/watermarking/article.php/3707261 (last visited Feb. 1, 2009) ("A group of content owners and operators of user-generated content sites last Thursday issued a set of User Generated Content (UGC) Principles designed to promote a way to regulate the use of copyrighted material on UGC networks."); Jon Healey, *The Content-recognition bakeoff*, LA Times Blog, Sept. 21, 2007, http://opinion.latimes.com/bitplayer/2007/09/the-content-rec.html; Juan Carlos Perez, *Google Plans YouTube Antipiracy Tool for September*, July 27, 2007, http://www.pcworld.com/article/id,135197/article.html.

[68] *See* Susanne Guth, *Right Expression Languages*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS, 101 (Eberhard Becker, et al. eds., 2003); Ernesto Damiani & Cristiano Fugazza, *Toward semantics-aware management of intellectual property rights*, 31 ONLINE INFO. REV. 59, 59-72 (2007); Gasser & Palfrey, *supra* note 33, at 13; VAN TASSEL, *supra* note 57, at 120.

[69] Guth, *supra* note 72, at 103; Damiani, *supra* note 72, at 60.

[70] VAN TASSEL, *supra* note 57, at 122. According to one definition, "a rights expression language provides a means of expressing use and access rights to assets. It should be sufficiently rich to formulate business models and to express terms and conditions for digital publications, audio and video files, images, games, software and other digital assets,

RELs are essential for interoperability since the idea of having multiple devices talking to each other depends on the availability of a common Rights Expression Language.[71] There are a wide variety of RELs today, making this the technological locus for interoperability debates. Currently, the dominant contender in the race for REL leadership is the eXtensible Rights Markup Language (XrML), which is based on the Extensible Markup Language (XML).[72] One example of an open REL standard is that promoted by the Open Digital Rights Language (ODRL) Initiative,[73] and another is the rights expression language that indicates usage rules governing Creative Commons-marked digital files.[74] The Creative Commons example underscores a point that should be evident: RELs are not restrictive *per se* and they can be employed restrictively or not. If current RELs' syntax and semantics are flexible enough to incorporate content owners' detailed permission structures, then they should equally be able to reflect user interests.[75]

The second category of DRMs is *access* control technologies. These "block access to content unless the user is authorized to consume it or the machine is authorized to play or display it."[76] They include, for instance, identification and password technologies, DVD regional coding, and Conditional Access cable set-top-boxes.[77] Access control technologies also include the Content Scramble System (CSS) and the Advanced Access Content System (AACS), which regulate access to DVDs only from compliant DVD players.[78]

The third set of DRM technologies, *copy* protection technologies, includes technologies designed to control the copying of works. One of them, Analog Copy Protection (Macrovision), manipulates the output component of a DVD player so that a VHS copy made from a Macrovision-enabled DVD player is distorted.[79] Another technology designed to control the copying of works is the Copy Generation Management System (CGMS), which allows only a

regardless of whether a monetary consideration is part of the transaction." Guth, *supra* note 72, at 102.

[71] Urs Gasser and John Palfrey, *Breaking Down Digital Barriers: A Case Study: DRM-protected Music Interoperability and eInnovation*, *in* BERKMAN PUBLICATION SERIES 13 (November 2007), *available at* http://cyber.law.harvard.edu/interop/pdfs/interop-drm-music.pdf.

[72] *Id.* at 14.

[73] The ODRL Initiative, http://odrl.net (last visited Feb. 1, 2009).

[74] *See* Hal Abelson, Ben Adida, Mike Linksvayer & Nathan Yergler, *ccREL: The Creative Commons Rights Expression Language*, http://wiki.creativecommons.org/images/d/d6/Ccrel-1.0.pdf (last visited Feb. 1, 2009).

[75] Stefan Bechtold, *Value Centered Design of Digital Rights Management: Perspectives on an Emerging Scholarship*, INDICARE MONITOR, Sept., 2004, at 10, 11, *available at* http://www.indicare.org/tiki-read_article.php?articleId=39.

[76] VAN TASSEL, *supra* note 57, at 92.

[77] *Id.* at 92-102.

[78] *Id.* at 88; Kerr et al., *supra* note 55, at 17.

[79] VAN TASSEL, *supra* note 57, at 105; Kerr et al., *supra* note 55, at 20.

limited number of copies to be made according to the "generation" of the copy.[80]

Finally, the fourth category of DRMs comprises *transfer* protection technologies. These limit the movement of content between devices. This category includes Digital Transmission Content Protection (DTCP) and High-bandwidth Digital Content Protection (HDCP). Devices enabled with these technologies (such as DVDs, digital TVs, digital VHS) are allowed to exchange content through secure channels accessed through the devices' digital sockets.[81]

A DRM *system* incorporates many of these individual technologies. DRM systems are highly complex and involve several components. Some DRM systems operate solely within the user's device (for example, DVD regional encoding), but in practice DRM systems have a distributed architecture with several layers: (1) content protection software (i.e., the particular technology for controlling access, copy or transfer, as well as ancillary technologies); (2) a content server that holds and delivers the work to the user; (3) a separate license server, that independently issues the relevant permissions to the user; and (4) the end-user devices.[82] Also, there is usually a payment-processing component. [83]

In a DRM process, content providers protect and identify digital works using the technologies already mentioned. Also, usage rules are described through Rights Expression Languages. Then, the content is distributed to the user either by physical distribution media (such as CDs and DVDs) or online distribution. Acquiring the digital file, however, means very little if the user has no permission to use it. Therefore, the user needs usage rights. These permissions might come bundled in physical media (e.g. a DVD) or can be distributed online through a separate license server using a rights expression language such as XrML. The amount and kind of permissions described in the REL will determine the price for usage of content. Finally, usage rights may be linked to particular DRM-compliant devices.[84] A typical system looks something like this:

[80] A CGMS can be designed so that, for example, a user could make unlimited copies from the original, but no copies from "second generation" copies. Van Tassel, *supra* note 57, at 105-06; Kerr et al., *supra* note 55, at 20.

[81] Patrick Turner, *Digital Video Copyright Protection with File-Based Content*, 16 Media L. & Pol'y 165, 199 (2007); Van Tassel, *supra* note 57, at 116-17.

[82] Marina Bosi, *Digital Rights Management Systems*, *in* Multimedia Security Technologies for Digital Rights Management 23, 25 (Wenjun Zeng, Heather Yu & Ching-Yung Lin eds., 2006). *See also* Sonera Plaza Ltd. & MediaLab, *Digital Rights Management White Paper*, Feb. 3, 2003, http://www.medialab.sonera.fi/workspace/DRMWhitePaper.pdf.

[83] Van Tassel, *supra* note 57, at 135.

[84] Bosi, *supra* note 87. *See also* Sonera Plaza Ltd. & MediaLab, *supra* note 87.

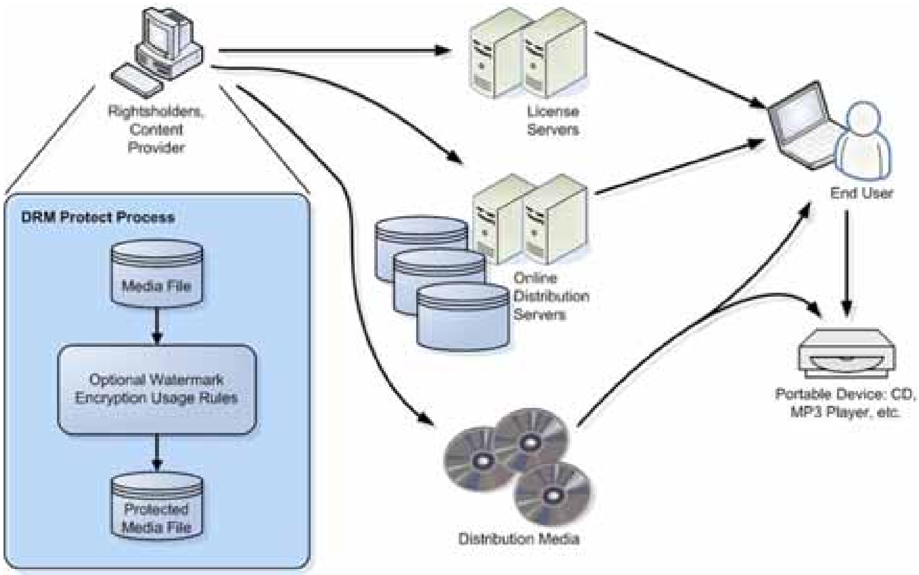
Rightsholders, Content Provider
License Servers
End User
DRM Protect Process
Media File
Optional Watermark Encryption Usage Rules
Protected Media File
Online Distribution Servers
Portable Device: CD, MP3 Player, etc.
Distribution Media

Figure 1: Basic DRM System[85]

As already mentioned, one significant problem with DRM technologies is that, as currently employed and designed, they tend to expand content owners' control over personal use at the expense of traditional copyright liberties, such as fair use. Unfortunately, encoding fair use or similar liberties into DRM systems is extremely complicated, if not impossible.

The fair use doctrine is anything but clear. When addressing a fair use claim, courts are required to consider four factors on a case-by-case basis.[86] This flexible approach is designed to avoid petrifying the statute into rigid categories and allows courts to make nuanced judgments on the balance between control and access interests in light of the policies that support copyright law.[87] Some have suggested that the fair use doctrine is so indeterminate that,

> Courts tend first to make a judgment that the ultimate disposition is fair use or unfair use, and then align the four factors to fit that result as best they can. At base, therefore, the four factors fail to drive the analysis, but rather serve as convenient pegs on which to hang antecedent

[85] Diagram by Rafael Pagán Colón derived from Sonera Plaza Ltd. & MediaLab, *Digital Rights Management White Paper*, Feb. 3, 2003, http://www.medialab.sonera.fi/workspace/DRMWhitePaper.pdf.

[86] These factors are: (1) the nature and character of the use; (2) the nature of the original work; (3) the portion of the original work used; (4) and the effect of the use on the potential market. Campbell v. Acuff Rose Music Inc., 510 U.S. 569, 577 (1994).

[87] *Id.*

conclusions.[88]

For these reasons, many are skeptical about the possibility of encoding fair use into DRMs. According to Edward Felten, "in some respects, the fair use test seems designed to frustrate attempts to computerize it. . . . In practice, an appropriate algorithm would have to ignore these factors or replace them with crude proxies."[89] Even the more nuanced Rights Expression Language XrML seems unsuited for this task.[90]

In the tradition of thought that recognizes the prospect of encoding social norms into technological artifacts[91] – a possibility only recently recognized by legal scholars[92] – several strategies have been proposed to accommodate fair use-like liberties within DRM technologies. Fox and LaMacchia, for instance, recommend a system of negotiated "safe-harbors" or defaults that can be expressed in RELs for clear cases.[93] But as Burk and Cohen argue, this approach is problematic because it will likely create a system that assumes such defaults as maximum allowed uses (ceilings) and not presumptive floors.[94] Additionally, these defaults would suffer from the same problems pointed to by Felten to the extent that many gray areas would be left uncovered.[95]

"Safe harbor" proposals can take the form of a "local solution." That is, a system where the permission structure resides with the end-user and the devices under her control. But as we saw earlier, DRM systems are highly complex and in many cases depend on distributed mechanisms where the content resides in one server that distributes the content while usage

[88] David Nimmer, *The Public Domain: "Fairest of Them All" and Other Fairy Tales of Fair Use*, 66 LAW & CONTEMP. PROB. 263, 281 (2003).

[89] Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMMUNICATIONS OF THE ACM, April, 2003, at 57, 58.

[90] *See* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH 49, 82 (2006).

[91] *See* Lewis Mumford, *Authoritarian and Democratic Technics*, 5 TECH. AND CULTURE 1 (1964); Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121 (1980); Bryan Pfaffenberger, *Technological Dramas*, 17 SCI., TECH., & HUMAN VALUES 282 (1992); WIEBE E. BIJKER & JOHN LAW, SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE (MIT Press, 1992); Lucas Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 THE INFO. SOC'Y 1, 1-17 (2000); DONALD NORMAN, THE DESIGN OF EVERYDAY THINGS (Basic Books 2002); BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY (2005).

[92] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319 (2005).

[93] Barbara L. Fox & Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, COMM'NS OF THE ACM, Apr. 2003, at 61.

[94] Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 57 (2001).

[95] *Id.* at 58.

permissions are administered by a separate License Server.[96]

Such a structure for “remote authorization” can serve as the basis for an alternative solution,[97] such as the one proposed by Dan Burk and Julie Cohen where the permission architecture is distributed between local and remote sites. Brutally simplified, the structure has three parts. A first and *local* layer would operate like the Fox and LaMacchia proposal for the encoding of safe-harbors. That is, it would have “automatic fair use defaults based on customary norms of personal noncommercial use.”[98] To avoid the problems of this limited strategy, a second level would kick-in when the local defaults do not allow a desired use. This second stage operates at a remote server controlled by a trusted third party, like the Library of Congress, and not by content owners.[99] This third party would hold keys for accessing digital works in escrow, granting permission upon a user’s request. In practice, this trusted third party would not “attempt to make a determination as to the bona fides of the access application . . . [and] simply issue keys to applicants via a simple online procedure.”[100] Then, if actual infringement is found, or if the application included false statements, the remote licensing party could hand-over the user identity pursuant to a court order issued under the most stringent standards.[101]

Very recently, Sun Microsystems Laboratories announced a DRM architecture similar to the above proposal.[102] Under Sun’s system, a user that has legally acquired content (i.e. by purchasing it) but is unable to access it because of DRM restrictions, may be able to assert fair use and gain access to it by anonymously informing a third party Service Provider of her intentions via an automated process. By identifying the content with technologies such as watermarks and fingerprints, a content owner can track a digital file on the internet without knowing the user’s identity and only after the content is determined to have been used illegally would the Service Provider reveal the user’s identity.[103]

A third and important feature of the Burk and Cohen proposal has to do with the legal protection against DRM circumvention. If the content owner deposits access keys in escrow, anti-circumvention laws would be available to her to enforce against people who crack DRMs, subject to the user’s end-use (that is, if circumvention occurs to engage in a protected use, no liability arises). On the other hand, if the content owner does not deposit the key in escrow, no

[96] *See* DRM flowchart image, *supra* note 85.

[97] *See* Armstrong, *supra* note 90, at 74-75.

[98] Burk & Cohen, *supra* note 94, at 65.

[99] *Id.* at 63, 65-66.

[100] *Id.*

[101] *Id.* at 64.

[102] Sun Microsystems Laboratories, *Support for Fair Use with Project DReaM*, Feb. 2008, http://www.openmediacommons.org/collateral/DReaM-MMI-Fair-Use-v1.0-CClicensed.pdf.

[103] *Id.*

anti-circumvention law would be available and users would be able to hack freely.[104] Under this regime, individuals would be able to hack DRM systems without fear of prosecution only when content owners fail to submit the appropriate key to be managed by the system.

This proposal has met some criticism, and understandably so. The basic critique is that, all things considered, it is still a permission structure.[105] With analog media, people can make certain uses that may *later* be determined fair or not. One important consequence of unauthorized use is that a significant amount of uses of doubtful legality fall through the cracks, thus going unpunished even if theoretically illegal. This imperfection of analog media is essential in preserving a fair amount of spontaneity in personal expression. Permission structures create transaction costs to that expression and, thus, have chilling effects.[106]

Another approach to combine flexibility with DRMs focuses on geography rather than uses. This is the path followed by certain industry sectors with Home Entertainment Networks. A Home Entertainment Network is a complex DRM system that builds on Mark Stefik's vision of a "Trusted System."[107] From an industry perspective, the idea is that "consumers can obtain content legitimately and then use it anywhere in their homes (or in their cars or in their personal portable devices), while at the same time rights holders can remain confident that all of the devices and the links among them will remain impervious to piracy."[108] From this point of view, Home Networks fulfill two basic goals: (1) the prevention of revenue-loss due to unauthorized use and (2) the enabling of a business model for the monetization of every possible use

[104] Armstrong, *supra* note 95, at 65-66.

[105] *See id.* at 57-58.

[106] *Id.* at 99-108. In response to this problem, Timothy Armstrong proposes a design solution that, in theory, provides a way out of this pre-authorization structure. It relies on the general Burk/Cohen scheme, but substitutes the third part of the scheme (conditional application of anti-circumvention laws upon submission of key) with an affirmative permission to "challenge the code." In this system, users go through a local permission mechanism with basic defaults, then, if necessary, through a remote location trusted-third-party-key-escrow system and, finally, instead of ending there as in the Burk/Cohen approach, if still unsatisfied, the user would be able to challenge the code. This "assertion of rights" structure, allows users to freely circumvent DRMs after the third party denies use. A DRM-compliant device must be able to allow the use. In exchange for this freedom to hack, devices would be required to store an audit trail (with privacy-safeguarding mechanisms). Where content owners suspect copyright infringement, they will be able to tap into the audit trail (after showing appropriate reasons and after going through several layers of non-identifying information) to commence legal proceedings. *Id.* at 98-101.

[107] *See* Mark Steffik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997).

[108] Bill Rosenblatt, *DRM, law and technology: an American perspective*, 31 ONLINE INFO. REV. 73, 81(2007).

that the market can tolerate.[109]

There is currently no uniform standard for Home Networks, which leads to a severe interoperability problem. As Rosenblatt acknowledges, "[t]he home entertainment network market in the USA is currently too disjoint[ed] and confusing."[110] However, content providers are beginning to see value in developing a uniform standard for interoperable use of content and devices within this Home Network.

One version being designed by a European consortium (the Digital Video Broadcasting Project, DVB)[111] is called the Content Protection and Copy Management system (CPCM).[112] One significant feature of the CPCM home network is what the DVB calls an "authorized domain." The authorized domain is defined as "a distinguishable set of DVB-CPCM compliant devices, which are owned, rented, or otherwise controlled by members of a single household."[113] This technology is concerned with the content *after* the consumer has acquired it, not transmission or initial access.[114]

Another proposal is being promoted by the Digital Living Network Alliance.[115] They propose a network of interoperable devices and standards that is substantially similar to the DVB "authorized domain" concept.[116]

Finally, a third proposal, the Sun Microsystems[117] DReaM system is an open standard for interoperability that links usage rights, not to a particular device, or to a set of devices, but to individuals:

> [U]sage rights are defined in a separate license management system that is facilitated by DReaM, allowing consumers to use players and DRM clients already installed on their devices without inheriting their limitations. Equally important, identity and authentication services are separated from individual hardware devices. Rather than merely authenticating the device on which content can be viewed, identity can be bound to a smart card (a Java Card or a SIM card, for example) for personalization in DRM systems. So the content rights are bound to individuals (or roles) rather than devices.[118]

[109] VAN TASSEL, *supra* note 55, at 15-16.

[110] Rosenblatt, *supra* note 108, at 82.

[111] Digital Video Broadcasting Project, http://www.dvb.org (last visited Feb. 1, 2009).

[112] Digital Video Broadcasting Project, *DVB-CPCM - Content Protection and Copy Management*, June 25, 2008, http://www.dvb.org/technology/fact_sheets/.

[113] *Id.*

[114] *Id.*

[115] Digital Living Network Alliance, http://www.dlna.org (last visited Feb. 1, 2009).

[116] Digital Living Network Alliance, *DLNA Overview and Vision Whitepaper 2007*, http://www.dlna.org/en/industry/pressroom/DLNA_white_paper.pdf (last visited Feb. 1, 2009).

[117] SUN Microsystems, *Dare to DreaM*, Sept. 1, 2006, http://research.sun.com/spotlight/2006/2006-08-30_Dare_to_DReaM.html.

[118] *Id.*

The common thread among these geographic proposals is the development of a personal sphere that intends to map individual usage expectations and content owners' monetization capabilities. Their focus is not on tying one piece of content with one type of device, but on tying one piece of content with multiple devices that are associated to users. The objective is, of course, the monetization and control of personal use, but within a delineated area or sphere of personal usage. To the extent that these systems' objectives are to define a "valid" household and the permitted uses within it, there is certainly cause for concern.[119] Specifically, there are issues regarding (1) the delimitation of this domain and the values inscribed in this delimitation; (2) the criteria for defining authorized devices (i.e, ownership and personal relations); (3) substantial privacy considerations;[120] and (4) the possibility of more nuanced control over the kinds of uses than can be made of the content within the domain.

These technologies also present, however, an opportunity for changing the way we traditionally think about DRM design and the development of free use domains, as opposed to authorized domains.[121] Hence, using technologies designed to afford fine-tuned control over personal usage within a specific predetermined domain, one could propose a sphere for complete and absolute free use of legally-acquired content. The technology for combining the dual goals for flexible use within an interoperable architecture is available. The question is: will we get there?

B. Incompatible Systems

It is a widely-known fact that the DRM environment is diverse, and that it is defined by low levels of interoperability.[122] A brief survey of available

[119] *See* Cory Doctorow, *A behind-the-scenes look at how DRM becomes law*, July 11, 2007,
http://www.videsignline.com/howto/showArticle.jhtml?articleId=201001112&pgno=1.

[120] *See* Julie Cohen, *A right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

[121] Fox and LaMacchia hint at this approach when they refer to their safety-harbor approach as one possible starting point for such defaults to allow "a single copy of a digital work (exclusively for personal use) to a designated and verifiable network of devices." Fox & LaMacchia, *supra* note 93, at 63. Unfortunately, this suggestion does not go far enough.

[122] *See* Gasser & Palfrey, *supra* note 36; Palfrey, *supra* note 49; Andrea U. Schmidt, Omid Tafreschi & Ruben Wolf, *Interoperability Challenges for DRM Systems*, 2004, http://virtualgoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf; *Digital Music Interoperability and Availability: Hearing before the Subcomm. on Courts, the Internet, and Intellectual Prop. of the H.R. Comm. on the Judiciary*, 109th Cong. (2005); Gregory L. Heileman & Pramod A. Jamkhedkar, *DRM Interoperability from the Perspective of a Layered Framework*, PROCEEDINGS OF THE 5TH ACM WORKSHOP ON DIGITAL RIGHTS MGMT. (2005); Gelareh Taban, Alvaro A. Cárdenas, Virgil D. Gligor, *Towards a Secure and Interoperable DRM Architecture*, PROCEEDINGS OF THE ACM WORKSHOP ON DIGITAL RIGHTS MGMT. (2006); Rob H. Koenen, Jack Lacy, Michael MacKay &Steve Mitchell, *The*

standards confirms this. As previously stated, the most relevant technology for interoperability purposes where DRM discrepancies occur is Rights Expression Language.[123] The DRM interoperability debate has significantly gravitated around two REL technologies: extensible Rights Markup Language (XrML) and the Open Digital Rights Language (ODRL).

The XrML REL was developed by ContentGuard. Microsoft owns one third of this company and uses one variant of XrML in its own DRM technology.[124] Microsoft's implementations of XrML are, however, not necessarily interoperable with other XrML-enabled DRMs, although Microsoft's version is available for licensing to third parties.[125] The XrML REL has been adopted by the International Standards Organization (ISO) as part of the MPEG-21 standard,[126] an open framework for multimedia applications.[127] Microsoft, however, has not adopted the MPEG-21 standard, and thus remains incompatible with MPEG-21 implementations.[128]

The gulf between REL standards is demonstrated by ContentGuard's broad claim that it owns patent rights not only for XrML, but for the entire Rights Expression Language concept and to any rights grammar.[129] If such claims were valid and effectively enforced, ContentGuard would possess an effective

Long March to Interoperable Digital Rights Management, PROCEEDINGS OF THE IEEE (2004), http://www.intertrust.com/main/research/ whitepapers/Interoperable_DRM.pdf; Spencer Cheng & Avni Rambhia, *DRM and Standardization—Can DRM be Standardized?*, *in* DRMS: TECHNOLOGICAL, LEGAL AND POLITICAL ASPECTS, *supra* note 59, at 162.

[123] Gasser & Palfrey, *supra* note 36, at 14 ("[S]everal market players have argued that the development of a uniform REL is a first step toward enabling DRM interoperability.").

[124] Bill Rosenblatt, 2004 Year In Review: DRM Standards, January 6, 2005, http://www.drmwatch.com/standards/article.php/3455231.

[125] *See* Microsoft, *Licensing Windows Media DRM Technologies*, http://www.microsoft.com/windows/windowsmedia/licensing/drmlicensing.aspx (last visited Feb. 1, 2009).

[126] DRM Watch Staff, *ISO Approves MPEG REL*, DRM WATCH, Apr. 1, 2004, http://www.drmwatch.com/standards/article.php/3334611.

[127] *See* Organisation Internationale de Normalisation, *MPEG-21 Overview v.5*, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm (last visited Feb. 1, 2009); MPEG-21, http://en.wikipedia.org/wiki/MPEG-21 (last visited Feb. 1, 2009).

[128] Gasser & Palfrey, *supra* note 36, at 14-15; Bill Rosenblatt, *2005 Year In Review: DRM Standards*, DRM WATCH (Jan. 2, 2006), http://www.drmwatch.com/standards/article.php/3574511.

[129] *See* Susanne Guth & Renato Iannella, *Critical Review of MPEG LA Software Patent Claims*, INDICARE PROJECT, Mar. 23, 2005, http://www.indicare.org/tiki-read_article.php?articleId=90. Invented by Mark Stefik, Xerox Corp. holds a patent with the following claim: "a grammar for creating instances of usage rights indicating a manner by which a possessor of an associated digital work is able to transport said associated digital work, and said grammar further specifies a default plurality of conditions for an instance of a usage right, wherein said one or more conditions must be satisfied before said usage right may be exercised." U.S.Patent No. 5,715,403 (filed Nov. 23, 1994) (issued Feb. 3, 1998).

monopoly over all DRM technologies, which would have an enormous impact on innovation in this field. In January 2005, MPEG LA ("MPEG-LA"), a patent pool organization,[130] announced a patent portfolio comprising ContentGuard REL patents.[131] MPEG-LA offers licenses to companies that use an open DRM REL (the OMA-DRM specification), which is the most popular DRM REL for mobile products.[132] It is unclear, however, whether ContentGuard's patent claims have had any effect on innovation in the DRM area or if the relevant mobile firms have taken them seriously. According to one industry observer, by December 2006 there were approximately five-hundred million mobile devices using OMA DRM, presumably without licensing ContentGuard's patent, and the patent pool organization (MPEG-LA) has made little progress licensing the patents to the wireless industry.[133] Furthermore, there appears to be no pending litigation on this matter.[134]

The other major REL contender is ODRL: an open REL that has been a major success in the mobile industry.[135] It was adopted by the Open Mobile Alliance (OMA), an organization composed of close to three-hundred mobile industry players.[136] On another front, Apple has designed its own closely-guarded DRM standard, which it rarely licenses to third parties. Apple's DRM coexists with a host of other self-contained technologies such as the ones mentioned in the previous section for Home Networks.

Finally, the Coral Consortium has developed specifications for allowing different DRM RELs to communicate with each other. Instead of trying to create its own DRM standard, Coral's approach is to develop a common language (a sort of meta-REL) to make incompatible DRMs "talk to [one] another."[137] Coral's proposal is a significant development in DRM

[130] MPEG LA, *About Us*, http://mpegla.com (last visited Feb. 1, 2009).

[131] MPEG LA, *MPEG LA Announces OMA DRM Patent License Terms*, Jan.6, 2005, http://www.mpegla.com/news/n_05-01-06_drm.pdf.

[132] Gasser & Palfrey, *supra* note 36, at 14.

[133] "The patent pool for OMA DRM 1.0 implementations put together by the patent licensing organization MPEG LA last year appears to be dead, as no progress in negotiations with the wireless industry on licensing terms has been made in over a year and a half, and MPEG LA has been focusing on Blu-ray and other fronts." Bill Rosenblatt, *2006 Year In Review: DRM Standards*, DRM Watch, Dec. 27, 2006, http://www.drmwatch.com/standards/article.php/3651126.

[134] Renato Iannella, founder of the competing Open Digital Rights Language (ODRL), told me that the ODRL was unaware of any litigation between ContentGuard and any implementator of rights expression languages. *See* E-mail from Renato Iannella, ORDL Initiative, to Hiram Meléndez-Juarbe, author (Apr.1, 2008) (on file with author).

[135] Rosenblatt, *supra* note 136.

[136] *See* Open Mobile Alliance, *Current OMA Members*, http://www.openmobilealliance.org/Membership/CurrentMembers.aspx (last visited Feb. 1, 2009).

[137] Gasser & Palfrey, *supra* note 36, at 15.

interoperability technology and will be addressed later.[138] For now, it is sufficient to acknowledge its presence to understand that there is an intense competition among DRM standards – a competition that is at the root of the interoperability problem.

C. Why Incompatible?

Perhaps economic analysis might explain why, despite arguable consumer demand for interoperable digital products, DRM technologies (and hence DRMed goods) are not interoperable.

1. Copying, digital goods and DRMs

DRMs emerged as a reaction to the threat of digitization upon content owners' interests. Economists explain how this came about in ways that might be useful to understand DRM incompatibility. According to economists, there are two circumstances under which unauthorized copying of information products might be beneficial for a producer.[139] These circumstances, however, are rare in the case of digital information products, and, therefore, might explain why firms rely on DRMs. When digital products are easily and cheaply reproduced with little or no cost, and there are few differences in quality between the original and the copy, the benefit to producers of allowing unauthorized copying disappears.

In theory a firm may be able to benefit from what is called "indirect appropriability." In these cases, a producer might benefit from copying if it is able to price discriminate between primary purchasers (original) and secondary users (copiers). The producer might even encourage unauthorized copying and "add[] the additional marginal willingness to pay by the secondary users on the price for the primary user and buyer of the original. The price of the original then increases with indirect usage (by copying) and the demand includes the demand for copies."[140] Hence, the price of a journal sold to a library is higher than what is charged to individuals because it reflects an estimate of the number of library patrons who will copy or borrow from the library.

According to this view, copying might benefit the producer, but only if it is able to "estimate . . . the number of secondary users and their individual willingness to pay in order to set the prices on the primary market accordingly"[141] and estimate the differences in quality between the original and the copy in order to determine whether the copy is a perfect substitute of the original.[142] However, because digital products exhibit no practical differences

[138] *See infra* text accompanying notes 204-211.

[139] Tobias Bauckhage, *The Basic Economic Theory of Copying*, *in* DRMs: TECHNOLOGICAL, LEGAL AND POLITICAL ASPECTS 234, *supra* note 59, at 242.

[140] *Id.*

[141] *Id.* at 243.

[142] *Id.*

between originals and copies, and copying and distribution is costless, "in the case of digital information goods it would be at least difficult for the producer to identify and price discriminate those primary buyers that let secondary users reproduce their master copies. . . . In consequence producers would probably raise prices for every primary user, exceeding the willingness to pay of those primary users not sharing their master copy with others."[143] Producers would then lose many purchasers to the secondary market. From the consumer's perspective, DRMs are justified because if producers were not able to control copying, they would have to charge high prices and sell only a few copies to primary purchasers.[144] Hence, "DRM together with an according pricing scheme would enable the producer to price discriminate the primary users and take advantage of the concept of *Indirect Appropriability*".[145]

Another scenario in which copying might be profitable for producers is one in which network effects are present, so that when "the utility that a user derives from consumption of [a] good increases with the number of other agents consuming the good."[146] I will further discuss network markets below, as they are important to understanding the current state of affairs regarding DRM interoperability. For now, only the following is important: In cases where the original and its copy are qualitatively different, a producer in a network market may not need strong copyright or DRM protection since, thanks to network effects, buyers of the original will not shift to the secondary market for the imperfect copies regardless of whether they are capable of copying or not.[147] In these circumstances producers may price primary purchasers according to their willingness to pay.[148] But if there were no differences between the original and the copies, so that the copies were perfect substitutes for the original, purchasers would prefer copying and the producer would not make any profit.[149] In these cases a high level of copyright or DRM protection is preferable for producers to prevent purchasers from moving to the secondary market.[150] Because digital copies are identical to their original and relatively costless, "all — or at least many — of the users of the primary market would switch to the secondary market, where the (almost) same product is available at a lower price"[151] which tends to justify, from the producer's perspective, strong copyright or DRM protection.

This analysis, however, ignores the fact that DRMs can curtail users'

[143] *Id.*

[144] For a similar view, *see* Ginsburg, *supra* note 27, at 127-28.

[145] Bauckhage, *supra* note 59, at 244 (emphasis in original).

[146] Michael Katz and Carl Shapiro, *Network Externalities, Competition, and Compatibility,* 75 THE AMERICAN ECON. REV. 424, 424 (1985).

[147] Bauckhage, *supra* note 61, at 246.

[148] *Id.* at 247.

[149] *Id.*

[150] *Id.*

[151] *Id.* at 248.

flexibility to the degree that DRMs affect demand for original products. In fact, a recent survey conducted in the United Kingdom indicates users' intense disapproval of DRM technologies.[152] If this is the case, users may switch to the secondary market for DRM-free copies, even with strong DRM or copyright protection.[153] One economist suggests that when users of a purchased original are restricted in what they can do with a digital product (compared to a user of a DRM-free copy), the perceived value of the original will be smaller than the perceived value of the DRM-free illegal copy (if there are no further differences between the original and the copy).[154] Thus, because DRM restrictions lower the original's perceived value to the consumer, she may still be willing to pay for the original *if* the restrictions are "smaller than the perceived quality difference between the original and the copy".[155] Hence, if there are no differences between copies and the original (as is generally the case with digital products), consumers will perceive the unprotected copy as having a higher value than the DRM-restricted original and will tend to shift to the secondary market for DRM-free products.[156] According to this view, instead of increasing technical protection measures that curtail user flexibility and hence reduce the original's perceived value, the challenge for content owners should be to increase the perceived value of the original by providing primary purchasers additional services and products.[157]

If DRM-restricted digital products decrease the value of originals and consequently make identical DRM-free copies more attractive to consumers, why do content owners insist on restrictive DRMs (in part because of lack of interoperability), and ignore consumer demand, instead of focusing on increasing the value of originals? The dynamics of network markets may help to answer this question.

2. Network effects, interoperability and standards

It seems uncontroversial to assume that, like many other digital products, the

[152] When asked about DRMs individuals agreed with the following statements as indicated by the percentage in parentheses: It's a nuisance and I don't like it (48%); It invades the rights of the consumer (50%); Have concerns that it invades my privacy (50%); Content providers should trust consumers not to share content with friends with others (49%). *See* WIGGIN, 2008 DIGITAL ENTERTAINMENT SURVEY, FULL REPORT, at 220 (2008), http://www.entertainmentmediaresearch.com/reports/DigitalEntertainmentSurvey2008_FullReport.pdf.

[153] *See* Marc Fetscherin, *Evaluating Consumer Acceptance for Protected Digital Content*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 301, 315 (Eberhard Becker, et al. eds., 2003).

[154] *Id.* at 317.

[155] *Id.*

[156] *Id.* at 318.

[157] *Id.* at 318-20.

value of DRM technologies increases with the number of users.[158] As described by Lemley and McGowan[159] there are several kinds of network markets: (1) actual networks, like telephones and email, in which the value of the network lies in consumer's access to other consumers within the network;[160] (2) virtual networks, such as the market for computer software, where the value of a product increases with the number of users of identical products or interoperable goods (unlike actual networks, these goods do not have to be connected in a cohesive system);[161] and (3) positive feedback effects, which are not technically networks or compatible goods, but simply reflect the fact that "a given degree of demand [is needed] to sustain production of the good and complementary goods or services".[162]

Because use increases the value of a product, a firm whose product becomes dominant in a network market and, thus, becomes the *de facto* standard, will reap the benefits that accrue from network effects. This may be especially true in the case of first movers: "Because of the strong positive-feedback elements, systems markets are especially prone to 'tipping,' which is the tendency of one system to pull away from its rivals in popularity once it has gained an initial edge."[163] Hence, before a standard becomes dominant, there will be intense competition between firms *for* the market. As described by Katz and Shapiro,

> Because a firm with a small, initial advantage in a network market may be able to parlay its advantage into a larger, lasting one, competition in a network industries can be especially intense –at least until a clear winner emerges. . . . If the ultimate outcome is going to be one of tipping to a single system, the firms are effectively biding for future monopoly profits.[164]

Because the prize is so valuable, competition in network markets is particularly intense. Under these circumstances interoperability is unlikely, and diverse incompatible products are likely to emerge.[165]

A clear winner does not always arise in this scenario. If competing systems possess distinct attributes and consumers prefer variety to the potential benefits of a single product, tipping may not occur as incompatible products may coexist for these different consumer groups[166] and the standards war will

[158] *See* Gasser & Palfrey, *supra* note 36.

[159] Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

[160] *Id.* at 488.

[161] *Id.* at 491.

[162] *Id.* at 494.

[163] Katz & Shapiro, *supra* note 4, at 105-06.

[164] *Id.* at 107.

[165] *Id.*

[166] *Id.* at 106 ("Consumer heterogeneity and product differentiation tend to limit tipping and sustain multiple networks. If the rival systems have distinct features sought by certain consumers, two or more systems may be able to survive by catering to consumers who care

continue for an indefinite amount of time.[167] Alternatively, if consumers prefer a particular product over others, in the end, a *de facto* standard may emerge.[168]

Standardization of this sort might produce an appropriate outcome if a single standard (proprietary or not) is the best one, avoiding unnecessary heterogeneity.[169] On the other hand, if the selected product is inferior to other alternatives, consumers will be locked-in to a lesser standard. "With network effects, it can be very difficult to switch horses in midstream to a system that later proves superior."[170]

In light of the above, perhaps finally settling into one standard may inhibit innovation as the market will be dependent on obsolete technologies and other competitors may not have sufficient incentives to enter the market with innovative technologies. As observed by Landes and Posner, "an industry may be stuck with an inferior technology because of the cost advantage of the existing network." [171] While path dependency is a serious concern, it should not be overstated. Even when a technology becomes a *de facto* standard, it is possible for other entrants to introduce new and incompatible technologies.[172] This is especially the case where the technology does not require high levels of capital investment, as is the case with most digital technologies. As Landes and Posner explain:

> Traditional networks such as the telephone system and the railroads required enormous capital investments and were therefore difficult to duplicate. The owner of such network . . . had a pretty secure monopoly. The less capital investment the creation of a substitute network involves, the less secure the network monopolist's monopoly is. Because of the extraordinary rate of innovation in the new economy and the rapidity with which new networks that are primarily electronic can be put into service,

more about product attributes than network size. Here market equilibrium with multiple incompatible products reflects the social value of variety.").

[167] Joseph Farrell & Gath Saloner, *Converters, Compatibility, and the Control of Interfaces*, 40 J. INDUS. ECON. 9, 9-10 (1992).

[168] *See* Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 CAL. L. REV. 1889, 1899 ("[A] standard may arise from the operation of the market, as consumers gravitate towards a single product or protocol and reject its competitors. This form of 'de facto' standardization is particularly likely in markets characterized by strong network effects, because of the large benefits associated with adopting the same product everyone else does.").

[169] Lemley & McGowan, *supra* note 159, at 498.

[170] Katz & Shapiro, *supra* note 163, at 106.

[171] WILLIAM LANDES & RICHARD POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 396 (2003).

[172] Katz & Shapiro, *supra* note 3, at 108 ("Although it seems possible that the inertia associated with network effects has somehow deprived us of valuable new technologies, it is abundantly clear that many new, incompatible technologies are in fact successfully introduced.").

new economy networks may not be secure against competition . . . .[173]

The latter is a significant point. To the extent that a product's dominance in a network market is fragile, the prospect of new entrants rises and the likelihood that a dominant technology will stall innovation is reduced. In this sense, innovation for competition to become a *de facto* standard in a network market is still possible even when there is already one dominant product.

In light of the above, it seems clear that the current lack of interoperability in the DRM context is due in large part to a standards war.[174] In these cases it is usual to see the sponsor of an incumbent technology opposing interoperability while entrants can be seen as favoring interoperable standards.[175] This description is not always true, however, since, for the reasons outlined above: "[A]n entrant who has a superior technology may be the one that opposes compatibility," as it will be interested in breaking the incumbent's hold and benefit from the network market.[176] This explains Apple's and Microsoft's differing DRM strategies as they try to consolidate their respective strengths in the market and deflate the competition.

It is clear from the above that, even with consumer demand for interoperability and flexibility, it may not be in firms' interests to opt for interoperability even when it may benefit society as a whole. In spite of this, as a policy matter, DRM interoperability should be sought because, if accompanied by the allowance of flexible personal use of content, it would help spur innovation and creativity both at content and technological levels.

Regarding content, interoperability "enhances variety by allowing consumers to mix and match (differentiated) components from various systems,"[177] which is a necessary (albeit not sufficient) precondition for flexible personal use of content. The prospect of a semiotic democracy might very well depend on users' ability to fully engage with cultural digital goods in interoperable systems and devices.

[173] LANDES & POSNER, *supra* note 171, at 395.

[174] *See generally Gasser & Palfrey, supra* note 36; Olivier Bomsel & Anne-Gaëlle Geffroy, *DRMs, Innovation and Creation*, COMM. & STRATEGIES, June 2006, at 35, 42 ("The on-line digital music market illustrates the reasons behind and results of incompatible DRM systems. Four major players are trying to impose their proprietary DRM standard. Two of them, Sony and Apple, refuse to license their DRM technology to other digital music distributors and portable players' manufacturers. Their proprietary DRMs (Apple Fair Play and Sony Open Magic Gate) secure a complete music distribution system composed of an internet music store, a media player and mobile players. Real Networks and Microsoft are pursuing the opposite strategy, namely trying to attract as many music stores and portable players manufacturers as possible to their own DRM technology (WMA DRM and Helix). Helix is open and Microsoft sells very cheap licenses for its WMA. Given its large market share, Apple's proprietary strategy induces major incompatibility issues between on-line music stores and mobile players.").

[175] Katz & Shapiro, *supra* note 3, at 111.

[176] *Id.*

[177] *Id.* at 109.

With respect to innovation at the technology layer, interoperability (as in other network markets) may risk sacrificing technology variety in exchange for compatibility and functionality.[178] If and when a single standard is selected, however, innovation will not stop. It will simply be refocused. Competition ceases to be about the network itself and starts to become about the products within it: "[T]he locus of competition shifts from the overall package (including the network size) to the specific cost and performance characteristics of each component individually."[179]

With the competition for dominance in network markets, incompatibility might be the *status quo* for a long period of time. Hence, the way to interoperable systems may be difficult, uncertain, and very dependent on the particular market.[180] It is worth examining the roads that could be taken, however, to illuminate the interoperability question in the DRM context.

IV. Standards and Converters

It is possible to group alternatives to breaking the non-interoperability deadlock in two general categories: standards and converters (or adapters).[181] Standardization may be produced by different processes and, as already discussed, imposes a uniform technology or process. Adapters (also called converters, emulators, translators, or gateway technologies), on the other hand, do not focus on comprehensive uniformity, but on providing compatibility between different non-interoperable systems.[182] Both standards and adapters increase interoperability, but with different consequences. As explained by Katz and Shapiro:

> With adapters, the principal cost is that of the adapters themselves, plus the fact that adapters may work imperfectly. By contrast, the primary cost of standardization is a loss of variety: consumers have fewer differentiated products to pick from, especially if standardization prevents the development of promising but unique and incompatible new

[178] Ricahrd J. Gibert, *Symposium on Compatibility: Incentives and Market Structure*, 40 J. Indus. Econ. 1, 1 (1992) ("Variety may be the spice of life, but the price of variety is high in markets where products and services need to be compatible to function properly.").

[179] Katz & Shapiro, *supra* note 3, at 110.

[180] Lemley & McGowan, *supra* note 159, at 486 ("Network effects are complex, differentiated, and often indeterminate economic phenomena, and thus are not well suited to either fast or furious adaptation.").

[181] Katz & Shapiro, *supra* note 3, at 110 ("The potential costs of incompatibility depend upon the mechanism by which compatibility is achieved. Broadly speaking, there are two mechanisms: standardization, whereby systems are designed to have interchangeable components; and adapters, which attach to a component of one system to allow it to interface with another system.").

[182] Joseph Farrell & Gath Saloner, *Converters, Compatibility, and the Control of Interfaces*, 40 J. Indus. Econ. 9, 9-10 (1992).

systems.[183]

Mark Lemley describes three types of ways in which standards emerge.[184] First, *de facto* standards may surface as the result of competition in network markets, following the dynamics already described.[185] Second, as is the case of digital television, for example, the government may impose a standard requiring all market participants to follow its specifications.[186] One might include in this category government-imposed interoperability requirements that, while not imposing a particular standard, try to force firms to either select a single standard or open-up key elements of their technologies to allow interoperability.[187] Finally, another approach to achieving interoperability is through private standard-setting organizations composed of key market players.[188] De facto standards have already been considered and government-imposed standards will not be addressed in this article.[189]

Standard setting organizations (SSOs) are similar to the "private ordering" described by Merges - they are created to coordinate and administer intellectual property rights (such as patent pools).[190] Unlike patent pools, however, SSOs are not formed around patent rights but focused on technical challenges and goals. They are not necessarily formed by patent holders but rather are open to every interested stakeholder.[191] The goal of an SSO is first

[183] Katz & Shapiro, *supra* note 3, at 110.

[184] Lemley, *supra* note 168, at 1898-99.

[185] *Id.* at 1899.

[186] *Id.* ("[T]he government might identify and set the appropriate standards and compel all participants in the market to comply. The government does this from time to time. For example, the Federal Communications Commission ("FCC") sets standards for interconnection between telephone networks and standards governing the use of products that might interfere with broadcast communication.").

[187] This is the case in France where a law was passed in 2006 providing that DRM technologies "must not have the effect of preventing effective interoperability" and that suppliers of DRMs may be required to give access to "information essential to interoperability." CODE CIVIL art. 13 (LOI n° 2006-961 du 1er août 2006) (Fr.), *available at* http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MCCX0300082L, *translated in* Nicolas Jondet, *LaFrance v. Apple: who's de dadvsi in DRMs?* 3 SCRIPT-ed 473, 480 (2006). *See also* Bill Rosenblatt, *French Parliament Passes DRM Interoperability Legislation*, DRM WATCH, Mar. 23, 2006, http://www.drmwatch.com/legal/article.php/3593841.

[188] Lemley, *supra* note 168, at 1898.

[189] The Berkman Center report on DRM interoperability counsels against government-imposed standards since the government is not likely to measure clearly market needs and conditions and because a government imposed standard would probably rely in government enforcement to insure compliance. Gasser & Palfrey, *supra* note 36, at 51.

[190] Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293, 1301 (1996).

[191] Raymod Gifford, *Standards in the Digital Age*, Remarks delivered to PFF-IBL Conference: "Interoperability in the Digital World: Open Standards, Open Source, Property

and foremost to design a standard for the industry to use, not to worry about licensing IP rights."[192] Because patent rights are a secondary concern for most of the individuals who participate in SSO (i.e. engineers), intellectual property rules are set *ex ante* and are thus designed evenhandedly.[193] Hence, because intellectual property rights are generally an "afterthought,"[194] "the SSO can make it clear up front whether the standards it adopts will be fully open (no IP rights allowed), proprietary but with mandatory licensing on reasonable terms, or closed (fully proprietary)."[195] In many cases, SSOs require that IP owners give up their rights to allow for non-proprietary use, or proprietary use subject to reasonable non-discriminatory terms, which are then embodied in the SSO's bylaws.[196]

Because consumer demand for interoperable products and services exerts pressure for open standards available to all market participants, there are only a few completely closed standards in the case of digital technologies, whereas open standards abound.[197] Because joining an SSO is voluntary, however, if a firm that holds patents on a needed technology refuses to join and tries to develop a *de facto* standard by "tipping," the standardization effort might fail.[198] Furthermore, there is also the risk that an SSO member will withhold information about patents on the relevant technology so that, when the SSO's standard becomes dominant, the firm will license its technology at monopoly prices with potential anticompetitive effects.[199]

In any event, because *de facto* standards that emerge from competition in a network market may produce a single proprietary product, and during the interim a host of diverse incompatible technologies may arise, cooperative open standards appear to be better alternatives for standardization because they lend themselves to a high degree of interoperability and tend to reduce entry barriers.[200] Thus, following the Berkman Center's recommendation, if a single standard is to arise, it would be best if it were open.[201]

Rights and Markets" (Feb. 11, 2005), *in* THE PROGRESS AND FREEDOM FOUNDATION, March 2005, at p. 3, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987307.

[192] Lemley, *supra* note 168, at 1951.

[193] *Id.* at 1951, 1956.

[194] *Id.* at 1956.

[195] *Id.* at 1952.

[196] *Id.* at 1944.

[197] Gifford, *supra* note 191, at 5.

[198] *See DRM-protected Music Interoperability and eInnovation*, *supra* note 36, at 46-47; Lemley, *supra* note 168, at 1898.

[199] *See* Rambus Inc. v. FTC, 522 F.3d 456, 463 (D.C. Cir. 2008) (withholding information from the SSO is not *per se* anticompetitive from an antitrust standpoint).

[200] *See* Gasser & Palfrey, *supra* note 36, at 46-47. *See also*, Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting*, *in* INNOVATION POLICY AND THE ECONOMY 140 (Jaffe, Lerner & Stern eds., 2001).

[201] Gasser & Palfrey, *supra* note 36, at 44-48. However, as demonstrated by Rajiv Shah

This, however, has not been the case in the DRM context.[202] Because of the standards war in this network market, open alternatives still have to compete with proprietary and incompatible alternatives.[203] In this scenario, the likelihood of a single interoperable open standard diminishes.

The second approach to break the interoperability deadlock is through converters or adapters. Adapters use technological intermediaries to achieve interoperability between incompatible products, instead of providing a single and uniform standard for the market. If a converter is able to bring together incompatible products, such technology may achieve interoperability while preserving variety.[204] By competing for market dominance, converters might transcend standard diversity and, hence, achieve compatibility "*ex post*—*i.e.*, after a variety of products has been introduced, without the constrains of *ex ante* standardization."[205] The TCP/IP internet protocol, for instance, is an interesting adapter example. From a technical point of view, the TCP/IP protocol provided a simple way to connect three separate experimental non-interoperable networks operated by ARPA in the 1970s (ARPANET, PRNET, and SATNET).[206]

In the DRM context there is one noteworthy "converter" effort. The Coral Consortium is an initiative with a goal "to create a common technology framework for content, device, and service providers, regardless of the DRM technologies they use."[207] Coral's main strategy is to create a common language for all DRMs through the development of "Coral Nodes."[208] These nodes can exist as part of existing services, such as broadband Internet Service Providers (ISPs), and can be set up to broker the relations between content

and Jay Kesan, if there is no interoperability with regards to the software needed to implement and run open standards, then the benefits of open standards are lost. Rajiv C. Shah, and Jay P. Kesan, *Lost in Translation: Interoperability Issues for Open Standards - ODF and OOXML as Examples* (September 2008). The Proceedings of the 36th Research Conference on Communication, Information and Internet Policy (TPRC), Arlington, VA, Sept. 26-28, 2008 ; Illinois Public Law Research Paper No. 08-02; U Illinois Law & Economics Research Paper No. LE08-026. Available at SSRN: http://ssrn.com/abstract=1201708.

[202] For example the ODRL REL which has significant support from the mobile industry (ContenGuard's patent threats notwithstanding) and Sun Microsystem's DReaM which also promises to encode fair use values and, hence, user flexibility. *See* Sun Microsystems Laboratories, *Support for Fair Use with Project DReaM*, Feb. 2008, http://www.openmediacommons.org/collateral/DReaM-MMI-Fair-Use-v1.0-CClicensed.pdf.

[203] *DRM-protected Music Interoperability and eInnovation, supra* note 36, at 18.

[204] Farrell & Salone, *supra* note 182, at 10.

[205] *Id.* at 2.

[206] JANET ABATE, INVENTING THE INTERNET 118-133 (1999).

[207] Coral Consortium, http://www.coral-interop.org/ (last visited Feb, 12, 2009).

[208] Coral Consortium, *Coral Consortium Whitepaper*, at 10, Feb., 2006, http://www.coral-interop.org/main/news/Coral.whitepaper.pdf.

providers' and users' devices, even when these two do not speak the same DRM language.[209] As Coral's nodes are not an open technology, broadband service providers can license the technology from the Coral Consortium and become Coral Nodes (i.e., adapters) in order to sell interoperability services to consumers who would like to use digital content in all their devices.[210] This "adapter" system would allow the development of diverse DRM systems and it would look something like this,

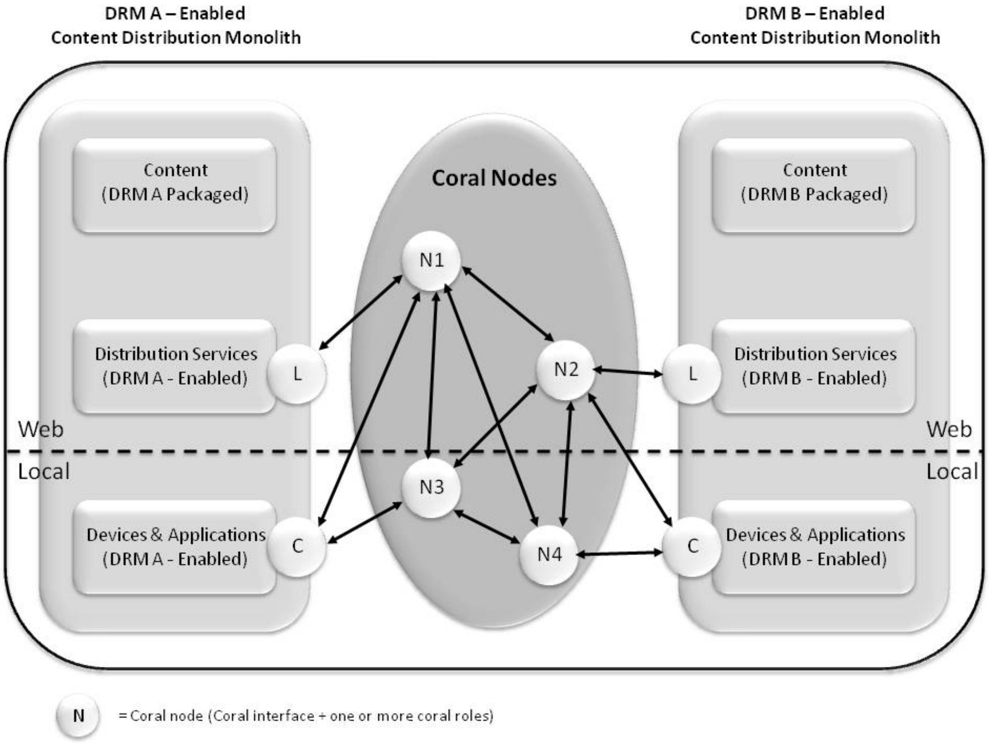

Figure 2: Example of an adapter system.[211]

One industry commentator observes that the Coral initiative has lost significant traction among industry players because (a) at least in the music industry the movement for DRM-free files and paid subscription has mooted much of the need for interoperability and (b) the cost of the infrastructure necessary to set up the system has kept Coral's potential clients (ISPs and

[209] *Id.*

[210] Bill Rosenblatt, *Coral Consortium Releases First Public Spec*, DRM WATCH, June 15, 2006, http://www.drmwatch.com/standards/article.php/3613776.

[211] Diagram by Rafael Pagán Colón derived from Coral Consortium, *Coral Consortium Whitepaper*, at 10, Feb. 2006, http://www.coral-interop.org/main/news/Coral.whitepaper.pdf.

online retailers) distanced from the idea.[212] Perhaps, if a converter system of this sort were openly available, much of the interoperability problem would be solved, as intermediaries could presumably translate permission languages between content distributors and users.

V. TRENDS AND CONCLUSION

The dual goals identified in Part II of this article (interoperability and strong personal use of content) go hand in hand, especially when considered from a user's perspective, because both are necessary to allow people to fully engage with cultural products. These goals must be addressed in tandem if we are seriously committed to the political implications of a semiotic democracy and a rich cultural environment.

Although they are complementary goals, interoperability and flexible use do not necessarily implicate each other. One might find a highly permissive DRM system designed to recognize fair and flexible use liberties that is unable to interoperate with devices tuned for other DRM languages. Similarly, a fully-fledged interoperable DRM environment might be designed to be precisely opposite to flexibility. Indeed, most DRM environments are designed to perfect architectures of intricate personal use control (with the notable exception of Sun Microsystems's DReaM).

While consumer demand might someday push content providers to use DRM systems designed to allow both flexibility and interoperability, so far the pressure has not been enough, and perhaps it never will. I have suggested that the main reason for ignoring consumer demand is that major firms are engaged in a standards war typical of a network market that has no foreseeable end, even when there are parallel efforts to design open DRM systems with reasonable personal use affordances. That we have proposals for interoperable DRMs that would allow even more control over personal use (such as Coral and the DVB's authorized domain system), coexisting with proposals for open DRMs (e.g., ODRL), and fair use-conscious DRMs (Sun Microsystems), is a testament to the fact that we are a long way from a consensus on the dual goals of interoperability and flexibility.

There are, however, signs of hope. For example, EMI, Universal, Warner, and Sony recently announced the release of DRM-free music for downloaded and purchased files on Amazon,[213] and Apple recently announced the release of its entire music catalog without DRMs.[214] Following in their footsteps,

[212] Bill Rosenblatt, *2007 Year In Review: DRM Standards*, DRM WATCH, Jan. 10, 2008, http://www.drmwatch.com/standards/article.php/3720886.

[213] Bill Rosenblatt, *All Music Majors to Go DRM-Free on Amazon*, DRM WATCH, Jan. 10, 2008, http://www.drmwatch.com/ocr/article.php/3720921.

[214] Jesús Díaz, *iTunes Gets DRM Free, New Prices, Purchase Over 3G*, Jan. 6, 2009, http://i.gizmodo.com/5124588/itunes-gets-drm-free-new-prices-purchase-over-3g. Since 2007 Apple had been seeling songs from EMI's entire music catalog without DRMs. *See* Apple, *DRM-Free Songs from EMI Available on iTunes for $1.29 in May*, Apr. 2, 2007,

Random House and Penguin Books have also recently announced a similar move for audio books.[215] The reason reportedly is that publishers do not want to hold consumers hostage to only one kind of non-interoperable device (i.e., the iPod).[216] This trend in the music industry is accompanied, as one might expect, by a dramatic increase in the use of identification DRM technologies such as watermarking and fingerprinting.[217] The music industry may be doubling its efforts in identifying illegally distributed content on the internet rather than focusing on the kinds of uses allowed.[218]

Because the field seems to be in constant flux, it is difficult to predict the direction in which the DRM interoperability problem is headed. The differences in consumer demand from industry to industry also make the future difficult to predict. For example, consumers in one industry (i.e., music) might exert a level of pressure that is not characteristic of other industries (i.e., movies and software). But in light of the issues described in this article, I will make the following general observation which, if proved true, may have interesting policy implications: *while flexibility does not necessarily follow interoperability, interoperability may follow flexibility*.

The first part of this proposition has already been addressed. That is, interoperability itself does not guarantee flexible personal use of content. Hence, while lack of flexibility may be one consequence of low levels of interoperability, flexibility does not necessarily follow from higher levels of interoperability. Indeed, high interoperability may even aggravate the flexibility problem as the idea of "authorized domains" suggests. Furthermore, for the reasons described in this article, the prospect of interoperable DRM systems is currently elusive and uncertain. The possibility of tipping has not allowed a standard to emerge (be it *de facto,* or collaborative, open or proprietary) and the only adapter technology being seriously considered has not gained sufficient support from the industry.

The way to interoperability may not lie in trying to address incompatibility of DRM standards up-front. Rather, it may be more useful to solve the interoperability problem by addressing one of the consequences of lack of interoperability: flexibility in personal use. As the examples in the music

http://www.apple.com/pr/library/2007/04/02itunes.html.

[215] Brad Stone, *Publishers Phase Out Piracy Protection on Audio Books*, N.Y. TIMES, Mar. 3, 2008, at C2, *available at* http://www.nytimes.com/2008/03/03/business/media/03audiobook.html.

[216] *Id.* ("Book publishers do not want to make the same error originally made by the music labels and limit consumers to a single online store to buy digital files that will play on the iPod. Doing so would give that single store owner — Apple — too much influence").

[217] *See* Rosenblatt, *supra* note 61. *See also* Bill Rosenblatt, *New Market Study Predicts Growth in Watermarking and Fingerprinting Markets*, DRM WATCH, Jan. 24, 2008, http://www.drmwatch.com/watermarking/article.php/3723626.

[218] Bill Rosenblatt, 2007 Year in Review, Part 1, December 27, 2007, *available at* http://www.drmwatch.com/article.php/3718531.

industry indicate, interoperability has become a byproduct of increased flexibility in personal use due to reduced reliance on access control DRMs and an increased emphasis on identification DRMs.

The reasons for this allowance of personal use in the music industry might be due to the pressure of consumer demand, a strategic move to dilute Apple's hold on the market,[219] acceptance of the fact that DRMs have no impact on illegal copying,[220] or a combination of factors. Whatever the reasons, one consequence of the allowance of personal use in the music industry is that users are able to play and use such files in other devices making them interoperable. In this sense, interoperability has followed flexibility.

As is readily apparent, the proposition that interoperability follows flexibility is not necessarily applicable to all cases and carries a significant fallacy, namely, just because DRM-free music files allow interoperability, does not mean that all *permissive* DRMs will be compatible among themselves. If there are several DRM systems in the market, they may be incompatible even if all of them allow flexible use. The proposition that flexibility drives interoperability is, hence, applicable to cases where there are *no* DRMs but not where there are *permissive* DRMs.

Still, this relation between flexibility and interoperability does carry some insight. If, for example, instead of relying on market pressures for motivation (as did the music industry) content providers were *required* by law to design DRM technologies to reasonably track users' traditional usage freedoms (such as fair use and personal use of content), one might speculate that content providers could give up the difficult task of encoding indeterminate standards such as fair use into DRMs, and follow the alternate (and, from their perspective, second-best) path of tracking illegally-acquired content on the internet while allowing broad uses.

The same could be hypothesized if a limited threshold were applied for criminalizing circumvention. That is, instead of *requiring* that DRMs follow users' freedoms, the DMCA could be amended to narrow its reach only to those DRM circumvention activities that affect a copyright owner's legal rights. As was previously discussed, because section 1201(a) of the DMCA currently prohibits the manufacture of technology and circumvention of TPMs

[219] Bill Rosenblatt, *All Music Majors to Go DRM-Free on Amazon*, DRM WATCH, Jan. 10, 2008, http://www.drmwatch.com/ocr/article.php/3720921 ("The primary impetus for this move is a strategic attempt to destabilize Apple's dominant market position in the industry.").

[220] Bill Rosenblatt, *Is EMI's DRM-Free Strategy Working?*, DRM WATCH, Aug. 8, 2007, http://www.drmwatch.com/ocr/article.php/3693316 ("[T]he online media measurement firm BigChampagne has been keeping a close eye on EMI-owned content since the DRM-free launch, and its CEO Eric Garland says that the effect on P2P traffic has been statistically insignificant. He adds that there is little overlap between people who purchase content on iTunes and people who upload files to P2P networks like LimeWire, so therefore P2P piracy is not likely to be affected one way or another by content protection methods used in the iTunes/iPod universe.").

that control "access to a work," the Act prohibits circumvention even for legitimate fair use purposes. Accordingly, this section could be amended to prohibit only manufacture of technology and circumvention of TMPs "that effectively *protects a right of the copyright owner*," similar to what section 1201(b) provides.

If users were able to circumvent DRMs for personal non-commercial use, it may not make sense for the industry to develop DRMs covering such use, even if they were able to. I say that it "*may* not make sense" because, even without the DMCA, there still might be incentives to employ DRMs for private use. DRMs could still be enforced by way of (a) the law of contracts and (b) the DRMs themselves (since those without the anti-circumvention technology would still be affected by the DRM). Because there would be mechanisms available to circumvent DRMs for legal and protected uses, however, one could expect increased consumer demand for content with built-in flexibility of use as consumers get accustomed to such uses.

If the content industry has incentives to allow flexible use in the private realm, then it may have incentives to develop interoperable DRM standards, because interoperability is an important dimension of flexible use. In the scenario I am describing, consumers would have increased expectations of personal use, including the ability to use content in different devices, regardless of the content's source. If this were the case, flexibility for the consumer would not only mean the ability to use content in many ways with a limited number of devices, but the ability to use content with many different applications and devices. Because the content industry would want to employ DRMs for other uses, it would have an incentive to create DRMs that can distinguish between personal (more flexible and interoperable) and public uses, just as is happening in the music business with identifying technologies (such as watermarking).

Hence, in order to allow flexible private use (while keeping DRMs for other purposes), firms will have to agree on DRM standards that allow content to be used flexibly among different platforms and devices in the personal realm. In this sense, increased flexibility of use (i.e., by amending the DMCA) may end up creating conditions for interoperable DRM systems.