

DRM and the recent copyright regime

How the new regime can impact interoperability

Piengpen Butkatanyoo

Copyright industries are using digital rights management (DRM) systems to prevent unauthorized copying or use of commercially valuable digital content. However, the DRM is not, in itself, a fail-safe measure. Copyright industries, therefore, had questioned the role of copyright on the Internet and the World Wide Web. They successfully persuaded legislatures in the USA, the EU and other countries to adopt broad anti-circumvention rules to protect DRM from being hacked. The article focuses on the legal protection of technological protection measures (TPM) for DRM and its ramifications for the digital ecosystem. In particular, it examines whether a strict application of the anti-circumvention rules could significantly discourage the legitimate right to engage in software reverse engineering and the development of interoperable or complementary products.



Dr. Piengpen Butkatanyoo

Policy Researcher

*National Electronics and Computer
Technology Center (NECTEC)
Ministry of Science and Technology
73/1 NSTDA Building, Rama 6 Road
Ratchatewi, Phayathai
Bangkok 10400, Thailand
Tel: (+66-2) 644 8150 ext. 622
Fax: (+66-2) 644 6653
E-mail:
piengpen.butkatanyoo@nectec.or.th
Website: <http://www.nectec.or.th>*

Introduction

Copyright is the most important form of intellectual property protection on the Internet. A large quantity of materials that move commercially on the Internet - such as musical works, movies, audiovisual works and computer programmes - are works of authorship protected by copyright law. Traditionally, the printing press created markets for information, and published literary and artistic work in a way that physical copies were made from a single original. Digital technology and the Internet, however, have created a powerful new medium of communication. The Internet has become a global marketplace to sell, deliver and com-

municate copyright materials and information across borders in a very short period of time. It also enables users to upload, download, print or reproduce unlimited copies at a low cost.

Traditional copyright law was designed to deal primarily with the creation, distribution and sale of protected works in tangible copies. In the past, it was relatively easy to know when or how many copies of a particular work, such as a book or a cassette tape, had been made and disseminated throughout the market. Digital technology and the Internet, however, have made it tremendously easy for a protected work to be reproduced, modified and disseminated. This naturally

causes fear to copyright owners.¹

Copyright industries are using digital rights management (DRM) technologies such as encryption envelopes, access codes, digital watermarking or digital signatures to prevent unauthorized copying or use of commercially valuable digital content. However, the DRM is not, in itself, a fail-safe measure because what technology can do, another technology can always undo.²

The copyright industries, therefore, had questioned the role of copyright on the Internet and the World Wide Web. They successfully persuaded legislatures in the USA, the European Union and other countries to adopt broad anti-circumvention rules to protect DRM from being hacked. The same rules also prohibit manufacturing or making available technologies, products and services capable of defeating DRM.

This article will focus on the legal protection of technological protection measures (TPM) or DRM and its ramifications for the digital ecosystem. In particular, it will examine whether a strict application of the anti-circumvention rules could significantly discourage the legitimate right to engage in software reverse engineering and the development of interoperable products.

This article initially reviews the basic principle of copyright law. It will then discuss how copyright industries protect their works from digital piracy and how copyright law struggles to adapt to technological changes and challenges posted by digital technology and the Internet. The article will briefly mention two international instruments of the World Intellectual Property Organization (WIPO) - the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). With these two treaties, protection of TPM or DRM used by copyright holders to protect their works, were for the first time formally integrated into international treaties.

We will examine the US Copyright Statutes and the EU Copyright Directives, which adopted the complex and controversial anti-circumvention rules under the WIPO treaties. Thereafter, we will illustrate a US court case applying the anti-circumvention provisions and its possible effects on the development

of interoperable products. We will then discuss and analyze France's most recent proactive approach to regulate DRM interoperability.

Finally, we will point out that, once a copy-control device is placed and a means to circumvent it is prohibited by law, both the technology and the law may effectively threaten to stifle innovation in the competitive market of interoperable and/or complementary products. And even as the French approach, which is new and innovative in the field of DRMs, has tried to fix this problem, it remains to be seen whether the regulation and its enforcing arms will be successful. The success or failure would be a strong indication as to whether DRMs should and can be regulated at all.

Copyright basic

Copyright encourages private investment in productive activity by giving its owners the right to exclude, and thus extract revenues from, anyone who wishes to make a use of his work that falls within the boundary of the law. "Encouragement of individual effort by personal gain is the best way to advance public welfare through talents of authors and inventors in science and useful arts."³

While patent protects new and useful innovation, copyright protects various kinds of creative literary and artistic works. Unlike patents, copyright protects a work upon its creation, regardless of its novelty. There are no prerequisites, such as registration or applications associated with copyright protection. The fundamental requirement for copyright protection is that the works must be independently created by the author, as opposed to copied from other works.⁴

The work of authorship may be embodied in a wide range of tangible copies, including books, periodicals, computer punch cards, microfilm, tape recordings, floppy disks, compact discs, CD Rom, DVD disk and other digital storage devices. Protection of copyrighted works is independent of the material objects in which the works are capable of being fixed.

The types of work eligible for copyright protection include literary, musical, pictorial and sculptural works; mo-

tion pictures; other audiovisual works; sound recordings; architectural works; and computer software. Copyright protection does not extend to any idea, procedure, process, system, method of operation or concept. Under the copyright law, the right holder is entitled to exclusive rights of reproduction, modification, distribution and public display and performance of his or her copyrighted work. Taken together, these rights encompass virtually all economically significant uses of copyrighted works.⁵

Copyright infringement takes place when any one of the exclusive rights is violated. However, certain uses of copyrighted works - such as for criticism, comment, news reporting, teaching, scholarship or research - may be fair and defended against infringement claim. The third party, in addition to the infringer, may also bear liability for the infringement if he has acted in concert with the direct infringer and has known of the infringing activities.⁶ Copyrighted work is generally protected through the life of the author plus 50 years. Some countries, especially the EU and the USA, protect the copyrighted works through the author's life plus 70 years.

DRM vs copyright law

For many years, copyright industries derived the bulk of their revenues from the sale of physical products, such as books, sound recordings, paintings and video cassettes in the marketplace. With the proliferation of digital technology and the Internet, however, two fundamental changes have restructured this economy: new opportunities have now opened up in which a substantial portion of copyrighted works are distributed rapidly without degradation of the quality of the works; and revenues gained in the copyright industries have come from the mass-marketing of such digital contents over the Internet.⁷

The same digital technology may, however, facilitate a rapid reproduction and dissemination of perfect copies of copyrighted works without proper authorization from the copyright owners. Therefore, the copyright industries have come to rely on the self-help: DRM or TPM enable them to trace, monitor and control dissemination and use of the copyrighted works as well as to prevent piracy.⁸

In fact, the use of technological measures as a way of controlling access to, and uses of, digital forms of copyrighted works has grown considerably since the early 1990s. For example, digital audio tape (DAT) machines were first released into the market with a built-in technological measure, the serial copyright management system (SCMS). This system allows one copy to be made of a work but prevents copies from being made of that copy, which means that it cannot be used as a "digital master".⁹

In the motion picture industry, the mass-market copies of DVD movies are technically protected by the "Content Scrambling System" (CSS).¹⁰ The CSS is used as an anti-copying mechanism and an authentication protocol to enforce country or region coding embedded in a computer disc drive and a DVD player.¹¹ The motion picture industry licenses manufacturers of equipment through CSS technology so that DVD drives and players have built-in technical controls.¹² These technical protection measures effectively prevent the making of any copies of the DVD files.¹³ One scholar believes that a fundamental transition is underway: from owning copies of the work to "experiencing works".¹⁴

Although technical protection systems provide new opportunities for content owners to protect commercially distributed copyrighted works against unauthorized uses, the technical protection measures are not, in themselves, fail-safe measures.¹⁵ As a precondition for the release of their copyrighted works onto the Internet, copyright industry groups persuaded the US Congress to provide legal reinforcements to protect these DRM systems so that it would be illegal to circumvent DRM used to protect copyrighted works, and to develop or distribute circumvention-enabling devices.¹⁶

In its 1995 White Paper, and as part of its National Information Infrastructure Initiative, the Clinton Administration proposed amending copyright law to outlaw circumvention technologies.¹⁷ The White Paper expressed concern that, without anti-circumvention regulations, copyright owners would not provide content for this infrastructure because their works would

be too vulnerable to widespread infringement.¹⁸ To give new assurances to copyright owners, it proposed a ban on making or distributing technologies whose primary purpose or effect was to circumvent DRM or technological protection measure (TPM) used by copyright owners to protect their works.¹⁹

The Clinton Administration proposed a similar rule for a draft copyright treaty which was scheduled for consideration at the 1996 Diplomatic Conference convened at the World Intellectual Property Organization (WIPO).²⁰ The draft treaty established several important international norms for applying copyright law in the digital environment that would aid the growth of the global digital economy.²¹ The draft treaty's anti-circumvention provisions, however, proved controversial, for many delegates challenged the impact these provisions would have on traditional copyright limitations and exceptions.²²

On 20 December 1996, diplomats eventually adopted the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT),²³ which contain an agreed-upon provision directing member states to provide "adequate legal protection" and "effective legal remedies" against circumvention of effective technical protection measures.²⁴ Member states of WIPO agreed that these treaties shall enter into force after at least 30 member states have ratified the treaties. Accordingly, on 6 March 2002 the WCT, and on 20 May 2002 the WPPT, entered into force.

These anti-circumvention provisions, set forth in article 11 of the WCT and article 18 of the WPPT, are however very general in character and provide treaty signatories with considerable latitude in the national implementation. Thus different implementation régimes are evolving around the globe, mostly influenced by the approaches of the USA's Digital Millennium Copyright Act (DMCA) and the European Union's Copyright Directive (EUCD).

In compliance with the treaty obligation to provide legal remedies against the circumvention of technological protection measures, the US Congress added Chapter 12 to the Copyright Act by passing into law the Digital Millennium Copyright Act (DMCA) on 28 Oc-

tober 1998. The DMCA has become a complex piece of legislation that makes sweeping changes to the Copyright Act to address copyright issues in the digital networked environment.²⁵ With respect to the issue concerning technical measures, although the WIPO Copyright Treaty only requires signatories to provide adequate protection against the "act" of circumvention of such measures, the DMCA went far beyond treaty requirements in broadly outlawing both the "acts" of circumvention and the "devices" that have circumvention-enabling uses.²⁶

In the hearing process prior to the adoption of the DMCA's anti-circumvention rules, there was an intense debate in Congress between the copyright industry group (Hollywood) and the innovative information technology sector (Silicon Valley).²⁷ In particular, the copyright industry group sought the strongest possible ban both on the act of circumventing a technical protection system and on devices having circumvention-enabling uses.²⁸ The Silicon Valley firms and their allies, however, opposed this broad legislation because of deleterious effects it would have on their ability to engage in lawful reverse engineering, computer security testing and encryption research.²⁹

Finally the US Congress adopted the broad anti-circumvention legislation that was favoured by the copyright industry group, although it is now subject to some specific exceptions that respond to some concerns raised by the innovative information technology sector in the legislative process.³⁰

One commentator pointed out that the debate in the legislative process was driven by "high rhetoric, exaggerated claims and power politics from representatives of certain established but frightened copyright industries".³¹ Various commentators also pointed out that the content industries were merely crying wolf³² in similar fashion to the way traditional print publishers had argued that public libraries,³³ and later photocopiers, would undermine the market for books and journals; radio would rob the music industry; the video cassette recorder would lead to the demise of the film and television industries; and analogue cassette recorders would destroy the sound recording industry.³⁴

These same commentators also contended that the content industries were merely trying to re-impose bottlenecks within the distribution pipeline and exert unwarranted control over the works of authorship. Following the printing press and the wireless broadcasting technology, digital technology represents the third wave of technology ultimately reshaping copyright law.³⁵

In Europe, Directive 2001/29/EC, better known as the European Copyright Directive (EUCD), entered into force on 22 June 2001. The original purpose of the EUCD was to harmonize the divergent European copyright régimes that were increasingly seen as an obstacle to the EU single market getting ready for the information age, and to transpose the two WIPO treaties.³⁶ Although the Directive came three years after the existence of DMCA, it similarly went far beyond the treaty requirements in broadly outlawing certain “acts” of circumvention and “devices” designed to circumvent technological measures used by the copyright holders to protect their works. In addition, ways in which national implementations addressed the scope of anti-circumvention provisions and the public policy exceptions have gone under differing degrees.³⁷

The EU member states were granted a short 18 months to implement the provisions of the directive into their national laws.³⁸ A significant number of member states were not able to comply with this time-frame. The European Commission (EC) proceeded in the European Court of Justice against six member states for failure to implement the Directive within the required period. Even the UK, Finland and France missed the deadline. However, as of September 2006, only Spain and Czech Republic had “pending implementation” status.³⁹

Rights beyond copyright: Anti-circumvention rules

WIPO treaties

As mentioned earlier, only two provisions, one under the WCT and another under the WPPT, addressed broad anti-circumvention rules. Article 11 of the WCT states that:

“Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.”

Article 18 of the WPPT states similarly, but the word “authors” is replaced by “performers or producers of phonograms.” Obviously, the protection set forth in the two articles is to be transformed into national laws of the WIPO member countries and is to be seen as a minimum standard. They are indeed of general wording, which allows member countries suitable liberties in transposing it into their national laws as long as the legal protection is “adequate” and the legal remedies are “effective.” Moreover, both article 11 WCT and article 18 WPPT neither defines the term “effective” nor “technological measures.” Member states have to provide their own definitions and thus set the scope of protection and bring meaning to the broad provisions of the WIPO treaties. It is this leeway that causes much despair wherever the implementation process is under way and interest groups are trying to have the balance shift their way.⁴⁰

The DMCA

To bring US law into compliance with the obligations under the WCT and the WPPT, the Congress passed and President Clinton signed into law the DMCA, which provides a definition concerning circumvention technological protection measures in section 1201⁴¹ and thus sets forth the scope of protection. The technological protection measures are divided into “access control” and “copy control” technology.

There are three principal rules in the DMCA’s anti-circumvention provisions. The first focuses on the “act” of circumvention and the other two focus on the “devices” capable of defeating DRM technologies. In particular, section 1201(a)(1) prohibits gaining unauthorized access to a work by circumventing technological protection measures that effectively control access to the copyrighted work. Section 1201(a)(2)

and 1202(b)(1) both regulate technologies or devices with circumvention-enabling capabilities. While the former prohibits trafficking or providing the means to circumvent technological measures controlling access to a copyrighted work (access control), the latter prohibits trafficking or providing the means to circumvent technological protection measures protecting the rights of copyright owner, e.g. measures that prevent reproduction (copy control).

In each case, the devices prohibited under Section 1201 are those (1) primarily designed for the purpose of circumvention, (2) have “only limited commercial significant purpose of use other than to circumvent”, or (3) are knowingly marketed for use in circumvention. Therefore, those devices that are capable of commercially significant non-infringing uses, such as personal computers and videocassette recorders, would not fall under these provisions.⁴²

It is important to note, however, that the DMCA has a specific mandatory provision in section 1201 (f) for reverse engineering for the purpose of achieving programme-to-programme interoperability.⁴³ The details are much in line with EU’s 1991 Software Directive.

The DMCA’s provision prohibiting “acts” of circumvention also permits lawful circumvention for other purposes: legitimate law enforcement and national security purposes; legitimate encryption research; security testing of computer systems; enabling non-profit libraries, archives and educational institutions to make purchasing decisions; allowing parents to control their children’s use of the Internet; and protecting personal privacy.⁴⁴

European Copyright Directive

Similar to the anti-circumvention provisions of the DMCA, the EUCD article 6(1)⁴⁵ and 6(2)⁴⁶ oblige the EU member states to provide for protection against the “act” of circumvention of effective technological protection measures as well as against the trafficking of circumvention “devices and services”. In both paragraphs it does not matter whether the act actually infringed a copyright or not - merely the act of circumvention is relevant. Unlike the DMCA, there is no explicit distinction - though there is an analytical one - be-

tween “access control” and “copy control” in the EUCD. Both types of technology are granted equal treatment.

The EUCD does provide exceptions to the “act” of circumvention in relation to photocopying, copy and archive purposes of educational facilities, broadcaster’s own ephemeral recordings, non-commercial broadcasts, teaching and research, use by disabled individuals and public safety.⁴⁷

However, it is important to note that these exceptions do not apply to “on-demand” services, i.e. works “made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.”⁴⁸

Anti-circumvention rules and interoperable products

The problem is that, in some cases, the anti-circumvention provisions may be applied as a new and lucrative form of control of copyrighted works never attainable under a régime of traditional copyright law.⁴⁹ In other cases, once a copy-control device is placed and a means to circumvent it is prohibited by law, both the technology and the law may effectively threaten to stifle innovation in the competitive market of interoperable and/or complementary products.⁵⁰ The court case explained in the following section will illuminate the point.

Application of the DMCA

In a relatively short time after the enactment of the DMCA anti-circumvention rules, the anti-circumvention provisions were invoked by the owners of technical protection systems. The decision in *RealNetworks, Inc. v. Streambox, Inc.*⁵¹ will illustrate that a major issue in the DMCA disputes is control over interoperable technology rather than an explosion of unauthorized copying, an original argument raised by the copyright industry groups.

In *RealNetwork v. Streambox*, the DMCA action was brought by RealNetworks, Inc., the publisher of a popular software package used to receive music or video “streams” via the Internet.⁵² The RealPlayer receiver software is used to access “on demand” audio and video content over the Internet. Through

a “streaming” method of broadcast, the audiovisual information from the originating server can be viewed and listened to on an end-user’s computer without transferring the file.⁵³

The servers residing elsewhere on the network communicate with the RealPlayer receiver through a “secret handshake” protocol. The “secret handshake” is an authentication sequence that allows the server and receiver to recognize one another.⁵⁴ Unless this authentication sequence takes place, the server does not stream the content it holds. Once the connection is achieved, the system containing a feature called the “copy switch” determines whether the audio or video files sent by the server may be copied by end-users, or only be viewed and evaporated as the user listens to or watches them.⁵⁵

The defendant, Streambox, produced a competing receiver, as well as several other pieces of software designed to be interoperable with the RealPlayer system. The Streambox receiving component (Streambox VCR) connected with the server by emulating the “secret handshake” protocol.⁵⁶ However, once connection was established, the Streambox VCR lacked the “copy switch” feature that would prevent unauthorized copying of streamed music or video content. Thus, the Streambox VCR allowed the end-user to download the file even if the content owner had used the “copy switch” to prohibit the end-user from downloading the files.⁵⁷

RealNetworks brought suit against Streambox, alleging that their receiving components constituted a “circumvention device” in violation of section 1201(a)(2) and 1201(b) of the DMCA.⁵⁸ In its complaint, RealNetworks emphasized two concerns. First, content owners would lose significant advertising revenue from decreased website traffic as a result of users viewing their downloaded copies rather than streaming the content from the copyright owner’s website each time they wanted to view it.⁵⁹ Second, the downloaded files would be easily redistributed over the Internet as pirated copies, thereby undermining the market for the copyrighted original.⁶⁰

The District Court for the Western District of Washington issued a preliminary injunction against the Streambox

VCR.⁶¹ The court held that the Streambox VCR circumvents both the access control and the copy control for two reasons. First, it found that RealNetwork had employed technological measures to ensure that only users of the RealPlayer could access RealMedia content placed on a RealServer. By emulating the “secret handshake” protocol to gain access to the RealMedia files, Streambox had circumvented the access control measures.⁶² Second, the court reasoned that the RealNetworks system also allowed copyright owners to specify whether or not their works can be copied by end-users, even if access is permitted. Because the Streambox VCR ignored the copy switch and enabled a user to make a copy of the file that the copyright owner had sought to protect, it effectively circumvented the copy protection measures.⁶³

Analogizing this case to *Sony Corp. of America v. Universal City Studios, Inc.*,⁶⁴ Streambox argued that there were substantial non-infringing uses of the Streambox VCR.⁶⁵ In particular, Streambox claimed that the VCR allowed consumers to make “fair use” copies of RealMedia files, notwithstanding the access control and copy protection measure that a copyright owner may have placed on that file.⁶⁶ The court, however, held that the users’ conduct was irrelevant to the circumvention device ban and that the *Sony* decision did not involve interpretation of the DMCA.⁶⁷

The court explained that the *Sony* decision turned in large part on a finding that substantial numbers of copyright holders who broadcast their works either had authorized private viewers to time-shift their works, or would not object to such.⁶⁸ Here, by contrast, copyright owners have specifically chosen to prevent the copying by putting their content on RealServers and leaving the Copy Switch off.⁶⁹ Furthermore, the court stated that “Congress specifically prohibited the distribution of the tools by which such circumvention could be accomplished”.⁷⁰ The court also cited “Nimmers on Copyright” for the proposition that manufacturers of consumer products with substantial non-infringing uses that would otherwise immunize them from liability

under the *Sony* doctrine are nonetheless subject to suppression under Section 1201.⁷¹

In its final argument, Streambox asserted that it was not required to manufacture the VCR with features responding to the copy switch because of the no-mandate provision of the DMCA.⁷² The court disregarded this defense, but concluded instead that the circumvention of the “secret handshake” access control measure was sufficient to create liability under Section 1201(a)(2) and warrant the injunction against the Streambox VCR.⁷³

There are at least two important issues that one could learn from the application of the DMCA anti-circumvention rules in *RealNetworks*. First, the DMCA provisions appeared to make no accommodation for any unauthorized uses of the protected work, even when the Streambox VCR allowed end-users to access otherwise unobtainable files and to make legitimate fair use of them.⁷⁴ It is unclear whether the proprietary aspect of the RealPlayer system, including the “secret handshake” protocol, allows RealNetworks to have the exclusive authority for granting access to all RealMedia files. At the very least, allowing RealNetworks to control access to RealMedia files that are in the public domain is certainly outside the sphere of copyright law.

Second, the most striking feature of this opinion is that, although the DMCA was purportedly enacted to protect owners of the copyrighted content, the parties involved in this case are not even the copyright owners of the RealMedia files, but the producers of competing software technology used as a technical protection system. In addition, the claim was focused on applying the DMCA provisions to prevent the distribution of the interoperable software product that could have been used to facilitate unauthorized copies of copyrighted content.

By making it unlawful to develop the Streambox VCR, which was designed to be interoperable with the RealPlayer system, the DMCA effectively granted RealNetworks (the publisher of technical protection software) absolute control over interoperable and complementary products. At least

one way of interpreting this case is as an attempt by a software publisher to impede or prevent the distribution of a competing, interoperable product. At a minimum, the case also demonstrates that control of interoperability lies at the heart of the DMCA disputes and that the DMCA provisions could be turned into such purposes.⁷⁵

Perhaps the legal requirement of interoperability of the DRMs or TPMs may be regulated. This approach was formally set forth in the most recent copyright amendment in France.

Interoperability approach - France

On 1 August 2006 the French Parliament passed their law on copyright and related rights, which implements the EU CD 2001/29 on the harmonization of certain aspects of copyright and related rights in the information society. The implementation of the EU CD had become a pressing matter for France, which faced the threat of financial sanctions after being condemned in 2005 by the European Court of Justice for failure to comply with the 2002 implementation deadline.⁷⁶

The main feature of the French law is the introduction of legal mechanisms to protect and enforce technological protection measures. The law also aims at combating digital piracy and touching upon the exceptions to private copying. As a whole, the law is in line with the spirit and the letter of the directive, as it reinforces the means to combat piracy and to protect the interests of right holders.⁷⁷ For example, the illegal file-sharing by individuals remains classified as a criminal offence; the law creates a new criminal offence for publishers of software used for illegal file-sharing, which is punished by three years in jail and • 300,000 fine⁷⁸ and it recognizes and protects technological measures.

The French law, however, would have provoked the anger of many big media companies. Although the EU CD does not set forth the rules on DRM interoperability,⁷⁹ France, the only EU member state to do so, explicitly provides in its EU CD implementation that DRM “must not have the effect of preventing effective interoperability.”⁸⁰ This provision stems from the concern that the online music platforms did not pro-

vide enough compatibility, some platforms having taken the strategic commercial decision to sell protected music files, which can only be played by a specific brand of electronic devices.

This situation is exemplified by Apple’s products and services, which are tied together by an exclusive DRM system called “FairPlay” and based around Apple’s proprietary AAC file format. Because of this DRM, people who have an iPod can only buy legal content from Apple’s iTunes online music store. And people who buy songs from iTunes can only play them on an iPod, to the exclusion of any other portable player. The law makers argued that the absence of an industry-wide standard is detrimental to the consumers and to the dissemination and equal access to cultural products. The lawmakers then concluded that DRMs or TPMs needed to be made interoperable through regulations.⁸¹

In addition, the law also provides that suppliers of DRMs or TPMs can be required to give access to “the information essential for interoperability.”⁸² This information is defined as the technical documentation and the interface of programming necessary to access a work protected by a TPM.⁸³

These provisions, which set the principle of interoperability, raise numerous practical questions: Who is entitled to ask for such sensitive information? Who would be required to disclose the information? What are the terms and conditions of such disclosure? What is the consequence if such access is refused by the TPM supplier?⁸⁴

The French Parliament finally set up a new regulatory body, “*Autorité de Régulation des Mesures Techniques*” (the ARMT), and also created procedures and powers to enforce DRM interoperability. The ARMT is an independent administrative authority whose powers are to mediate interoperability requests on a case-by-case basis. Under this régime, DRM providers can be forced (under certain conditions) to disclose interoperability information on non-discriminatory terms, but they have the right to reasonable compensation in return.⁸⁵

In fact, interoperability is a matter of degree. In some cases, interoperability information is available, but only under restrictive and somewhat open-

sive licensing terms. This is, as mentioned earlier, the case of the DVD format, where DVD Copy Control Association controls the necessary information to produce compatible DVD players. Arguably, proprietary DRM systems are, in general, a problem for both consumers and competitors.⁸⁶

In any event, supporters of interoperability, like consumer groups, praised France for taking the lead in this matter. The barriers to entry are lowered if new companies are given necessary recipes to compete in the markets for DRM content. Consumers would also be clear winners because of new compatible products. They pointed out that this statutory approach was the only way to increase competition in digital music systems by opening up the iPod-iTunes restrictions.⁸⁷

However, some argued that such a regulatory approach would threaten the efficiency of DRMs. If there is less incentive for anyone to introduce a new and more innovative DRM standard, this would hinder and potentially destroy online content distribution.⁸⁸ The arguments were continued that Apple's dominance was the result of the quality of its product and services. Apple's customers were aware and not deterred by the lack of interoperability. Ultimately, the market, not the regulators should be shaping the rules of digital content distribution.⁸⁹

Finally, the rhetorical discussion used in the DRM interoperability debate needs backing from economic analysis. Does interoperability in particular circumstances increase competition and generate welfare? Did those companies that opposed the interoperability initiatives retreat from affected markets? Did incentives to compete increase or decrease? Did consumers lose or win? Obviously, one can study the French copyright directive implementation as empirical tests.

Conclusion

While DRM systems can certainly prevent illegal copying and public distribution of copyrighted works, they can do far more than the copyright law provides. And when copyright law is adapted to accommodate protection to DRMs, the scope of protection to a copyrighted work and to the DRM itself seems to broaden more than ever before.

It is also evident that this legal régime may possibly discourage the development of interoperable or complementary products. However, any mandatory interoperability in the field of intellectual property law may also stifle the incentive to innovate. Furthermore, the anti-circumvention provisions adopted globally may become relatively meaningless. France's proactive interoperability approach and its coming experiences would be a strong indication as to whether DRM should or can be regulated. In the mean time, other legal remedies provided by such law as anti-competition or consumer protection may be viable options.

Footnotes

1. Pamela Samuelson, *Digital Media and the Changing Face of Intellectual Property Law*, 16 Rutgers Computer & Tech. L. J. 323, (1990).
2. Pamela Samuelson and Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L. J. 1575, 1632-33 (2002).
3. Mazer v. Stein, 347 U.S. 201, 219 (1954).
4. Feist Publication, Inc. v. Rural Telephone Services Co., 499 U.S. 340 (1991).
5. Paul Goldstein, *Copyright* 2nd Edition, Vol. 5, No. 2 (1996). "For example, if the copyrighted work is a novel, the reproduction rights would prohibit the unauthorized reproduction of copies of the novel; the right to adapt the work would prohibit the novel's unauthorized translation or its adaptation into a motion picture; the distribution right would prohibit the unauthorized sale, lease, lending or other transfer of copies of the novel to the public; the performance right would prohibit the unauthorized public recital of excerpts from the novel; and the display right would prohibit the unauthorized public projection of pages from the novel." Each of the exclusive rights may be owned and enforced separately. For example, the copyright owner of a novel may grant to a particular theater a licence to perform his work as a play. However, the author retains his performance rights with respect to other performers and theaters, and he also retains other exclusive rights.
6. Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).
7. Per S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. Sch. L. Rev. 63, 101 (2002-2003). For example, digital technology and the Internet connection have dramatically reduced the cost of producing, recording, marketing, and distribution sound recordings, suggesting that the supply of new music is richer and more diverse than ever before.
8. Pamela Samuelson, *DRM (and, or, VS) The Law*, Vol. 46, No. 4, Communication of the ACM, pp. 41-44 (2003).
9. 17 U.S.C. Section 1002 (c) (1994). The US Audio Home Recording Act requires that all consumer-grade DAT machines include a SCMS chip that allows users to make individual personal-use copies of DAT sound recordings while ensuring that perfect digital copies could not be made from those personal use copies.
10. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F. 3d 429 (2d Cir. 2001).
11. *Id.*
12. Samuelson and Scotchmer, *The Law and Economics of Reverse Engineering*, supra note 2 at n. 262. The DVD Copyright Control Association (DVD-CCA) licenses the Content Scrambling System, certain patent rights necessary to make DVD players, and other know-how to equipment manufacturers.
13. Some technically protected content is already being delivered to end users' computers "on demand" without transferring the file, such as by the "streaming" of audio or video files over the Internet. See RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889, at 5* (W.D. Wash. Jan. 18, 2000). Once the audio and video content is encoded in the "RealMedia" format, it can be hosted on any web server and contains security measures that prevent the downloading of the file onto the end-user's computer.
14. Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, Public Law & Legal

- Theory Working Paper Group, Columbia Law School, Paper No. 8, 2000. Available at http://papers.ssrn.com/paper.taf?abstract_id=222493.
15. Samuelson and Scotchmer, *The Law and Economics of Reverse Engineering*, *supra* note 2.
 16. *Id.* at 1630.
 17. Bruce A. Lehman, Working Group on Intellectual Property Rights, *Intellectual Property and the National Information Infrastructure*, pp. 230-34 (1995).
 18. *Id.* at 230.
 19. Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 Va. J Int'l L. pp. 369, 411-13 (1997).
 20. Basic Proposal for the Substantive Provisions of the Treaty on certain Questions Concerning the Protection of Literary and Artistic Works to Be Considered at the Diplomatic Conference, WIPO Doc. CRNR/DC/4, (Aug. 30, 1996).
 21. Samuelson, *The U.S. Digital Agenda*, *supra* note 20, at pp. 398-409.
 22. Nearly 160 nations signed this treaty. This indicated a strong consensus that digital works should be given appropriate protection on an international scale. See Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 Berkeley Tech. L.J. pp. 519, 528-29 (1999).
 23. WIPO Copyright Treaty, Art. 11. An equivalent provision is found in Art. 18 of the WIPO Performance and Phonograms Treaty, concluded at the same time at the Diplomatic Conference in December 1996 in Geneva.
 24. The DMCA changes the copyright law at least in three significant ways: circumventing technical protection measures, copyright management information, and liability of online service providers.
 25. WIPO Copyright Treaty, Art. 11 and 17 U.S.C. Section 1201.
 26. WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary 105th Cong. pp. 78-82 (1997) (hereinafter "Judiciary Hearing") (statement of Jack Valenti, President and CEO, Motion Picture Ass'n of America); see *Id.* at pp. 256-65 (statement of Edward J. Black, President, Computer and Communications Industry Association).
 27. Judiciary Hearing, *supra* note 27, at pp. 78-82 (statement of Jack Valenti); *Id.* at pp. 204-12 (statement of Allan R. Adler, Vice President for legal and governmental affairs, Association of American Publishers).
 28. Judiciary Hearing, *supra* note 27, at pp. 256-65 (statement of Edward J. Black); *Id.* at pp. 249-256 (statement of Chris Byrne, Director of Intellectual Property, Silicon Graphics, Inc., on behalf of the Info. Tech. Indus. Council); *Id.* at pp. 148-154 (prepared statement of Prof. Robert L. Oakley, Georgetown University Law Center).
 29. 17 U.S.C. Section 1201 (f) (g) (j).
 30. Samuelson, *Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Tech. L.J. pp. 519, 522-24, 533-34 (1999). This group also seems to think that they are entitled to control every facet of what Americans do with digital information, as well as to control the design and manufacture of all technologies that can process digital information.
 31. Siva Viddhyanathan, *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*. (New York University Press 2001); Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. Chi. L. Rev. 263 (2002).
 32. Charles Knight, *The Old Printer and the Modern Press*, London, J. Murray 1854, 285 (New York, AMS Press 1974) (when circulating libraries were first opened, the booksellers were much alarmed; and the rapid increase of circulating libraries added to their fears, and led them to think that the sale of books would be diminished by such libraries. But experience has proved that the sale of books, so far from being diminished (by public libraries), has been greatly promoted; as from these repositories many thousands of families have been cheaply supplied with books by which the taste of reading has become more general, and thousands of books are purchased each year by those who have first borrowed them at those libraries, and after reading, approving of them, have become purchasers); Carl Shapiro & Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy*, pp. 94-95 (1999).
 33. Peter Menell, *Envisioning Copyright Law Digital Future*, *supra* note 7, at pp. 101-103.
 34. Siva Viddhyanathan, *Copyrights and Copywrongs*, *supra* note 32.
 35. Michael Hart, *The Copyright in the Information Society Directive: An Overview*, 24 EIPR 2, 58 (2002).
 36. *Id.*
 37. Urs Gasser and Michael Girsberger, *Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States, A Genie Stuck in the Bottle?*, Berkman Publication Series No. 2004-10, November 2004. Austria, Denmark, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Slovak Republic, Slovenia, UK and finally France have formally implemented the EUCD.
 38. http://en.wikipedia.org/wiki/EU_Copyright_Directive (retrieved on 16 April 2008).
 39. Urs Gasser and Michael Girsberger, *supra* note 38, at pp. 6-7.
 40. 17 U.S.C. Section 1201(a)(3)(A). To circumvent technical measures means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise, avoid, bypass, remove, deactivate, or impair a technological protection measure."
 41. H.R. Rep. No. 105-551 (II), at 38 (1998).
 42. The legality of reverse engineering for DRM interoperability has been on trial for a few times in the US, Chamberlain Group, Inc. v. Skylink Technologies, Inc. (Fed. Cir. 2004), Lexmark Int'l, Inc. v. Static Control Components, Inc. (6th Cir. 2004).
 43. 17 U.S.C. section 1201 (d)-(j).
 44. Article 6 (1) EUCD states that "Member States shall provide adequate legal protection against the circumvention of any effective technolog-

- ical measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.”
46. Article 6 (2) EUCD states that “Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which: (a) are promoted, advertised or marketed for the purpose of circumvention, or (b) have only a limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling of facilitating the circumvention of any effective technological measures.”
47. Article 6 (4) EUCD.
48. *Id.* sub para. 4.
49. Kamiel J. Koelman, *The Protection of Technological Measures vs. The Copyright Limitations*, Institute for Information Law, Faculty of Law-University of Amsterdam (2001). www.ivir.nl/publications/koelman/alaiNY.html
50. *RealNetworks v. Streambox*, 2000 WL 127311 (W.D. Wash.) (2000); *Universal City v. Reimerdes*, 82 F. Supp. 211 (S.D. N.Y. 2000); *Sony v. Gamemasters*, 87 F. Supp. 2d 976 (N.D. Cal 1999); and, *Lexmark v. Static Control*, 253 F. Supp. 2d 943 (2003).
51. *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash.) (2000).
52. *Id.* at 1.
53. *Id.* at 2 (In his finding, the court pointed out that “to guard against the unauthorized copying and redistribution of their content, many copyright owners do not make their (digital) content available for downloading, and instead distribute the content using streaming technology in a manner that does not permit downloading.”).
54. *Id.*
55. *Id.* Many copyright owners make content available on their website as a means to drive traffic to the website. The more traffic a website generates, the more it can charge for advertisements placed on the Website. The plaintiff testified that “without RealNetworks’ security measures, a copy owner could lose the traffic its content generates. An end-user could obtain a copy of the content after only one visit and listen to or view it repeatedly without ever returning to the website. That end-user could also redistribute the content to others who would then have no occasion to visit the site in the first instance.” *Id.* at 3.
56. *Id.* at 4.
57. *Id.* In other words, the Streambox VCR is able to convince the RealServer into thinking that the VCR is, in fact, a RealPlayer.
58. Complaint for Violation of the Digital Millennium Copyright Act, Contributory, Vicarious and Direct Copyright Infringement, Tortious Interference with Contract, and Lanham Act Violations at pp. 31-46, *RealNetworks (No. C99-2070P)*, available at http://www.realnetworks.com/company/pressroom/pr/99/rnwk_complaint.html.
59. *RealNetworks*, *supra* note 51, at 3.
60. *Id.*
61. *RealNetworks*, *supra* note 51, at 12.
62. *Id.* at 4.
63. *Id.*
64. 464 U.S. 417 (1984) (holding that the private home viewing of TV programmes on copies made by videotape recorders is considered “fair use” and that manufacturers of those recorders cannot be held liable for vicarious or contributory infringement).
65. *RealNetworks*, *supra* note 51, at 8.
66. *Id.*
67. *Id.*
68. *Id.* (citing *Sony*, 464 U.S. at 443, 446).
69. *Id.* at 8.
70. *Id.*
71. *Id.* (citing 1 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* 12A.18[B] (1999 Supp.)).
72. *Id.* at 9. The DMCA Section 1201(c) (3) states that “nothing in this section shall require ... a response to any particular technological measure, so long as ... the product ... does not otherwise fall within the prohibitions of subsections (a)(2) or (b)(1).”
73. *Id.*
74. Eddan Elizafon Katz, *RealNetworks, Inc. v. Streambox, Inc. & Universal City Studios, Inc. v. Reimerdes*, 16 Berkeley Tech. L. J. 53, 65-66 (2001). For example, most audio and video clips of courtroom proceedings or congressional hearings remain on the CSPAN website for only a few days. Without a device like the Streambox VCR, users cannot view the files after they are removed from the servers.
75. Dan L. Burk, *Anti-Circumvention Misuse*, available at: www.law.berkeley.edu/institutes/bclt/pubs/wp/502.pdf
76. ECJ Commission v. France C-59/04 (in French only), available at: <http://curia.europa.eu>
77. Nicolas Jondet, *La France v. Apple: who’s the dadvsi in DRMs?*, Vol. 3, Issue 4, Scripted, pp. 473-484, June (2006).
78. CPI, Article L. 335-2-1.
79. EUCD Recital 54 only mentions that DRM interoperability is something member states should encourage, but does not provide further guidance and seems to trust in market forces. Also of note is recital 48, which states that DRM systems should not prevent “the normal operation of electronic equipment and its technological development.”
80. CPI, Article L. 331-5, § 4.
81. Rapport no. 2349, p. 20.
82. CPI, Article L. 331-5, § 4.
83. CPI, Article L. 331-7, § 2.
84. Nicolas Jondet, *supra* note 76. at 480-481.
85. CPI, Article L. 331-7, § 1, § 4.
86. Mikko Valimaki and Ville Oksanen, *DRM Interoperability and Intellectual Property Policy in Europe*, available at: www.valimaki.com/org/drm_interoperability_final.pdf
87. However, Virgin Media tried to use competition law as an instrument to enforce access to iTunes Fair-Play system. The French competition authority, nevertheless, has ruled in favour of iTunes, partly because it considered the market for probable music players to be sufficiently competitive. See: http://www.theregister.co.uk/2004/11/11/apple_vs_virgin_ruling
88. Thomas Crampton, *France weighs forcing iPods to play other than iTunes*, *The New York Times*, 17 March 2006.
89. *Id.* □