The Problem of Freedom Override by Digital Rights Management Technologies:
the Market Mechanisms and Possible Legal Options

Abstract
One of the major problems of copyright regulations in the digital and network era is
that the Digital Rights Management (DRM) technologies are overriding the freedom
incorporated within the copyright regulations in the analog world. The override
problem partly comes from the strict implementation of the DRM systems by the
market, and partly from the anti-circumvention regulations that almost blindly protect
such implementation. This research reviews the scope of anti-circumvention
regulations by introducing Japanese regulations, which are rather modest, and by
comparing with the U.S. regulations. It also extensively analyzes the market
mechanisms that cause rather strict implementation of DRM systems based on
interviews of key persons in the market. At the end, it suggests several legal options to
improve the problem of freedom override by DRM technologies, either by direct legal
means or through market mechanisms, to keep a better balance of interests between
right-holders and users of copyrighted information.

1. Introduction

Digital and network technologies have dramatically changed the world of
copyright. They are used not only to exploit and distribute copyrighted works, but also
to control the usage of copyright, often referred to as Digital Rights Management
(DRM) technologies. One major problem is that the DRM technologies are overriding
the freedom incorporated within the copyright regulations in the analog world. Even
worse, such override is often supported by the anti-circumvention regulations which prohibit the circumvention of DRM technologies. This problem has been discussed rather extensively,¹ however, we still do not see a substantial improvement. This article is to research the reason of this slow change, and to suggest possible improvements in law to assist the solution to this problem of overriding freedom.

This article uses two approach that has not been seen in the past. One is to provide lessons learned from comparing contemporary copyright regulations in the U.S. and Japan. Japanese scholars have not been particularly active in discussions about the digital dilemma, especially outside the Japanese domestic forum. This is a pity, because Japanese regulations are relatively unique and different from those of the U.S. in several material respects. By explaining the Japanese legislation and comparing it with the U.S. regulation, it shows the flexibility in implementing the two WIPO Treaties in 1996 (the WIPO Copyright Treaty [WCT], and the WIPO Performances and Phonograms Treaty [WPPT], which are collectively referred to as the 1996 WIPO Treaties), and how the difference impacts the society.

Another contribution this article attempts to make is including some of the voices from the market in the course of the analysis. Copyright regulations, digital and

¹ See, infra note 15, 18.
network technologies, and market (business model) and social norms (i.e., people’s perceptions about copyrighted works) are becoming more closely related to each other in the digital and network environment. Previous research in the field, however, does not contain enough clear and verbatim expression of the thinking and ideas of people currently working in the marketplace. This article includes quotes from these interviews and conference remarks, in order to illustrate the thoughts and experiences which are actually forming the practice in this growing field on a daily basis.²

Through these interviews, this article analyzes the reason why the implementation of the DRM technologies tend to be restricting, and concludes that it is rather difficult for the market to self-correct this unbalanced implementation.

At the end, using these two research methods, this article suggests the following three possible options to change the anti-circumvention regulations. One is to repeal the current anti-circumvention regulations when the implementation of the DRM technologies fail to consider the balance. It also analyze why repealing part of

---

² The author conducted many interviews of the key players in the digital networking fields to get their views. Included are executives and other businesspeople in Internet-related businesses, including right-holders, content providers, vendors, and systems designers. The interviews were conducted as free discussions; i.e., the author presented topics and asked the interviewees to discuss what they cared about or what concerned them the most about each topic. The author felt that this would be a reasonable way to avoid asking possibly biased questions. The results were recorded and transcribed. Interviews in Japanese were translated into English by the author. The transcripts presented in this article may have been edited on a grammatical level, but not further. Some of the remarks are from major conferences in the research field. The actual speeches were recorded and transcribed by the author. All the positions or titles that appear in this article are the ones at the time of the interview.
anti-circumvention regulations may not be as problematic as it may appear. The second is to expand the exemption to anti-circumvention regulations, or “the right to hack.” The third is to support the effort to incorporate the freedom within copyright regime into the DRM systems by tailoring copyright law.

Section 2 briefly describes the problems caused by DRM technologies: the problem of overriding freedom. Section 3 introduces the anti-circumvention regulations over DRM technologies in the U.S. and Japan, and the problems caused by these regulations, with special attention to the difference between Japan and the U.S. Section 4 studies some reasons for biased DRM implementation based upon interviews of the key players in the DRM arena, and analyzes whether such unbalanced implementation could be improved by market mechanisms. Section 5 looks into legal tools that might help solve the problem of overriding freedom. Section 6 concludes this article.

2. Brief Overview of DRM Technologies

Although there are many definitions of DRM technologies, this article will refer collectively to technologies that control access to or exploitation of digital materials as

---

“DRM technologies.” More concretely, encryption, watermark, metadata (especially “rights expression languages,” or “REL”) are among the technologies that are heavily used to control access to and exploitation of digital materials. Some systems can allow copyright owners to control users’ ability to view or listen to materials (access control). The same systems, or different ones, can control users’ ability to print, copy, download, upload, perform, distribute, modify, or otherwise exploit digital materials in a manner that is regulated by copyright law (usage control).^4

2.1 Pros of DRM Technologies

Overall, DRM technologies are thought to be an important enabler of new business models by right-holders and content distributors. First, DRM technologies can reduce the nonexclusivity of intangible content. Copyrighted works are often claimed to be public goods in an economic sense, which results in an undersupply of those goods in the market.\(^5\) Using DRM technologies, one can, at least in part, fix the problem of nonexclusivity.\(^6\) This can turn digital content into a marketable good. Second, as a result, DRM technologies help right-holders generate different business models for the

---

^4 See, Bill Rosenblatt et al., Digital Rights Management: Business And Technology (M&T Books 2002). See, also, Bechtold, Id. at 326-31.

^5 See, e.g., Pindyck And Rubinfeld, Microeconomics 593 (Prentice Hall 5th ed. 2000).

^6 Of course, if there is the same content available without any restrictions, DRM systems that are partly applied to the content cannot eliminate the problem of nonexclusivity in a complete manner. However, because of the transaction cost to get the unrestricted content, content providers still form a market with people who are willing to pay for the DRM-employed content.
same content. For example, DRM technologies can enable a price-discrimination model in a more secure way by combining technologically enforced usage restrictions and prices. If based on an economic judgment that a price-discrimination model increases social welfare by reducing deadweight loss compared to monopoly without price discrimination, DRM may be said to help increase such social welfare by sustaining such price-discrimination models.\(^7\)

Third, DRM-based transactions are often claimed to reduce the transaction cost of content distribution in various ways, if designed wisely and properly.\(^8\) It can reduce the costs of rights clearance by providing a direct license online, and enable direct distribution along with monetary transactions from creators to end users without an intermediary.\(^9\)

Finally, DRM technologies may be able to provide protection (or security) to make

---

\(^7\) There is an important suggestion made by Wendy Gordon, however, that such “increase of social welfare” brought by price discrimination is only when compared to a monopoly market without price discrimination. Gordon warns that price discrimination does not legitimatize the shift from free use to controlled use with price discrimination, as free use often provides more social welfare than monopoly that is required as prerequisite to price discrimination. See, Wendy Gordon, “Intellectual Property as Price Discrimination: Implications for Contract” (Symposium on the Internet and Legal Theory), 73 Chi. Kent. L. Rev. 1367.

\(^8\) However, the actual effect of reducing the transaction cost heavily depends upon the design of the DRM systems that are actually implemented. If poorly designed, they may even increase the transaction cost. For example, badly designed DRM players will take a great deal of time and energy for users to install and handle, and impose high cost on service providers to provide users’ support.

\(^9\) Direct distribution is more the fruit of network technologies than of DRM technologies. However, DRM technologies actually help enable businesses by providing payment mechanisms or increasing nonexclusivity.
content providers feel safe enough to release their content.\textsuperscript{10} For example, NTT Docomo, a Japanese company that first in the world created the mobile content distribution business model, explained that one of the reasons for their success was technological protections. Toshihiro Kuwabara, a member of the legal department of NTT Docomo explains:

The concept [of i-mode business] is to provide superior service at a low price. For example, downloading ring-tones costs 300 yen. We asked content owners to provide a low-priced license based on the fact that handsets are designed to prohibit copying of ring-tones among users. The fact that users are incapable of transferring ring-tones is a very important point in making the price inexpensive.\textsuperscript{11}

Bob Ohlweiler, Senior Vice President of Business Development at Musicmatch, an online Windows-based music store, explains the importance of providing a secure system as follows:

The bottom line is [that] we live in a world now where you can take a piece of valuable content and make unlimited numbers of perfect copies of it, so we go back to the problem which I believe is solved, which is, convincing the people who own the content to let us commercialize it in a digital medium. But part of the deal was you have to keep it somewhat safe from that kind of mass piracy…Without DRM …, it will be very difficult for us to convince all the rights holders to give us access to commercialize the contents.\textsuperscript{12}

\textsuperscript{10} However, this effect heavily depends upon how much security content owners ask in order to release their content. Often times, the level of security that content owners ask is very high, or not precise that it creates a lot of confusion and loss in the market of technology research and development.

\textsuperscript{11} Interview with Toshihiro Kuwabara, NTT Docomo, in Tokyo, Japan (Nov. 20, 2002).

\textsuperscript{12} Bob Ohlweiler, Address at Digital Hollywood Spring 2005 (Mar. 30, 2005)
Content owners agree. Amanda Marks, Senior Vice President of eLabs at Universal Music Group, made it clear: “We are not going to sell our content in an unprotected format.”

2.2 Cons of DRM Technologies and New Problems

As DRM technologies can have several positive functions in content distribution, they also create several concerns and problems. One of the problems that DRM technologies override and diminish the freedom incorporated in the copyright regime, as described below.

2.2.1 Diminishing Freedom Incorporated into the Copyright Regime

There are four categories in which “freedom of speech” is reserved within the copyright law: (1) idea/expression dichotomy; (2) copyright exemption such as fair use (in the U.S.) and copyright limitation statutes (in Japan); (3) copyright duration; and (4) what is outside the scope of copyright protection. Courts have acknowledged such freedom within the copyright regime. For example, the U.S. Supreme Court, in

---

13 Id.

14 There is another whole set of problem regarding privacy, which is outside the scope of this research. For details, See, e.g., Jonathan Zittrain, What the publisher can teach the patient: intellectual property and privacy in an era of trusted privication, 52 Stan. L. Rev. 1201 (2000); Jonathan Weinberg, Hardware-Based Id, Rights Management, and Trusted Systems, 52 Stan. L. Rev. 1251 (2000); Mark Stefik, The Internet Edge: Social, Legal, and Technological Challenges for a Networked World 197-231 (Cambridge: MIT Press, 1999).

Harper & Row,16 declared that First Amendment protections are “already embodied in the Copyright Act’s distinction between copyrightable expression and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use.”17

However, DRM technologies, by being implemented and enforced in a way that overrides the legal rules set by copyright law, diminish these freedoms.18 It can enclose the public domain, or can eliminate the copyright exemption. The conflict with fair use and other non-infringing uses created by DRM technologies is well recognized even by the U.S. courts.19

In addition, DRM technologies that are used to control people’s access to copyrighted work override the principle of “free access” in copyright law. Such phenomena were hardly observed in the analog era, simply because it was very costly to do so. You are free to walk around and peep into books that you are interested in, or can even read the entire book without violating copyright regulations. However, such

---

17 471 U.S. at 560.
freedom either is not granted or is very limited when it comes to DRM-protected works.\textsuperscript{20} As a result, it reduces a chance for people to be exposed to many kinds of information, or at least biases the kind of information that people can freely access.

2.2.2 Two Sources of the Override Problem

These problems of DRM technologies overriding freedom within the copyright regime come primarily from two sources: one from the manner in which the DRM technologies are implemented, and the other from the difference between computers and human beings as decision makers.

The problems of overriding copyright “freedom” can be partially avoided when DRM technologies are implemented in a considerate way. Usage rules designed to implement DRM technologies can be loose enough to respect the “safety valve” inside the copyright law: for example, allowing some private copies; allowing content to be transferred to a friend and family; excluding the public domain from the portfolio with DRM protection; and allowing as much preview as possible before purchase.\textsuperscript{21}


\textsuperscript{21} For an attempt to create or define such user-friendly rules in the DRM implementation, see, Digital Media Project, http://www.dmpf.org/, (last visited April 25, 2006). It states, as one of their mission, to map rights and usages traditionally enjoyed by users to the Digital Media space. See, http://www.dmpf.org/manifesto/dmm.htm#3.1.1, (last visited April 25, 2006).
Michael Miron, the CEO of ContentGuard, Inc., makes this point clear:

[One] misleading assertion … is that somehow DRM will necessarily erode consumer rights such as fair use and first sale…. There is a fair amount of belief that DRM somehow is going to take away legal rights necessarily, and therefore we have to ban it, stop it, undermine it, no matter what. This is misleading. DRM certainly can be misused in this way, but … this is really a systems’ implementation issue…. [Y]ou can use, for example, the MPEG well to create a license grant to mimic fair use for particular domains.22

However, so far, copyright owners and content providers tend to provide usage rules that are much less flexible than what was possible under the copyright law in the analog world.23 Whether this problem can be solved by the market will be analyzed below in Section 4.

Secondly, even if copyright owners and users of copyrighted works fully agree to set very flexible DRM usage rules, there still remains a problem of whether DRM technologies are capable of providing the same freedom as was allowed in the analog setting. The control and judgment made by computers and human beings (especially judges) are different in nature. Especially, DRM technologies can behave only as they are programmed, and are not good at considering the purpose or the situation of the use. Given such nature, Section 5 suggests to combine human intelligence with

---

23 See, e.g., Bechtold, supra note 3 at, 340 footnote 84, 344-6 (explaining that DRM technologies are often used to enforce strict contractual terms).
computers to embody the freedom properly within the DRM system.

3. Anti-circumvention Regulations in the U.S. and Japan

If DRM technologies are causing this override problems, one of the easy solutions would be to take away the cause of the problems: i.e., to circumvent DRM technologies when problematic. However, such a solution is prohibited by the anti-circumvention regulations. “Anti-circumvention regulations,” in a narrow sense, usually refers to two kinds of regulations. One is the “direct circumvention regulation,” which prohibits the acts of circumventing technological protection measures, such as “usage control” and “access control.” The other is “anti-device regulation” (or “indirect circumvention regulation”), which regulates production and/or dissemination of devices and/or information that allows people to circumvent technological protection measures. Here, “usage control” is referred to as technological measures that control the usage or exploitation of works for which copyright owners have rights defined in copyright law (such as rights to reproduce, modify, distribute, or perform). “Access control” is referred to as technological measures to control people’s access to copyrighted materials (including viewing, reading, and listening to the materials).
Legislators also decided to prohibit alteration of copyright management information,\textsuperscript{24} which is often referred to as “copyright management information regulations.” This article collectively refers to these two regulations using the expression “anti-circumvention regulations,” unless otherwise indicated, to make the argument simple, because their functions and problems overlap with each other in many areas.

Anti-circumvention regulations have their bases in the 1996 WIPO Treaties, which require contracting parties to provide legal protection remedies against “the circumvention of effective technological measures”\textsuperscript{25} and “rights management information.”\textsuperscript{26} In the U.S., Congress passed the Digital Millennium Copyright Act (“DMCA”) in 1998 in order to implement the 1996 WIPO Treaties.\textsuperscript{27} For the same reason, Japan amended the Copyright Law\textsuperscript{28} and Unfair Competition Prevention Law\textsuperscript{29} in 1999.

In the following, this Section describes the substance of anti-circumvention

\textsuperscript{24} Here, “copyright management information” refers to information attached to copyrighted work for the purpose of managing copyright, including metadata such as REL description of licensing terms, names of right-holders, and copyright terms.
\textsuperscript{25} WCT Article 11 and WPPT Article 18.
\textsuperscript{26} WCT Article 12 and WPPT Article 19.
\textsuperscript{27} 17 U.S.C. Chapter 12.
\textsuperscript{28} Article 2 Paragraph 1 Items 20 and 21; Article 30 Paragraph 1 Item 2; Article 113 Paragraphs 3 and 4; Article 119 Item 1; Article 120 \emph{bis} items 1, 2, and 3; and Article 123.
\textsuperscript{29} Article 2 Paragraph 1 Items 10 and 11, and Article 2 Paragraphs 5 and 6.
regulations, with an emphasis on explaining the Japanese regulations and comparing between the U.S. and Japan (3.1), and some pros and cons of anti-circumvention regulations (3.2 and 3.3).

3.1 Substance of Anti-circumvention Regulations

3.1.1 Direct Circumvention Regulation

3.1.1.1 Japanese Regulations

In Japan, the scope of direct circumvention regulations is very limited compared to that of the U.S. in two major aspects: the scope of protected technologies and the effect of violation.

First, in terms of protected technologies, Japanese copyright law protects only usage controls, and not access control.30 Article 2 Item 20 of the Copyright Law of Japan defines “technological protection measures” as “measures to prevent or deter such acts as constitute infringements on moral rights or copyright … or neighboring rights.”

According to the legislative history, the rationale behind this limitation is that

---

copyright law should support only established rights entitled in the law, but nothing further. It is stated that, because copyright owners do not have a right to monopolize mere access to copyrighted works by people, protection of access control technologies should be outside the scope of the Copyright Law.31 Nobuhiro Nakayama, Chief of the Copyright Council for the legislation of anti-circumvention regulations, explains why the legislation avoided regulation over access control: “because regulating people’s access [to information] includes a broader problem that is beyond the issue of protecting property: that is, academic freedom, freedom of speech, right to access, etc.”32 He recognizes voices that express concerns about the practical efficiency of the regulations because of the “lack of protection toward access control.” However, Nakayama explains that the legislation chose the moderate or prudent regulation on access “because the issue of controlling access to information has an enormous impact, good or bad, for the society in the information age to come. Therefore, a long-term careful discussion is necessary.”33

31 See, 著作権審議会マルチメディア小委員会ワーキング・グループ（技術的保護・管理関係）報告書（平成 10 年 12 月 10 日） [the Multi-media Subcommittee of the Copyright Council, the Final Report of the Working Group regarding Technological Protection and Control] dated December 10, 1998, Section 2.4, http://www.mext.go.jp/b_menu/shingi/12/chosaku/toushin/981201.htm#2-4, (last visited April 25, 2006). However, it is questionable whether the distinction between usage control and access control ban be made clear.
32 See, Yoshida et al., supra note 30 at ii.
33 Id.
Second, situations in which direct circumvention of usage control technologies is prohibited are very limited. Circumvention of usage control by users is prohibited only when users do so in order to make private usage of protected works (which is otherwise exempt from copyright under Article 30). In sum, circumvention of usage control only causes the loss of statutory exemption regarding private copies and modification of such works (thereby making circumventor liable for reproduction and modification of the work). Circumvention for the purposes of other statutory exemptions, such as reproduction in libraries, quotation, and educational purposes, is generally regarded to be allowed under Japanese copyright law.

Because the scope of regulation is very limited, especially because it does not regulate access control, there is no statutory exemption regarding the direct circumvention regulations in Japanese copyright law.

3.1.1.2 Difference between the U.S. and Japan

The largest difference between the direct circumvention regulation in the U.S. and Japan is whether it includes access control. Although the U.S. Federal Circuit

---

34 Of course, the resulting copyright infringement which became possible because of the circumvention of usage control is regulated by traditional copyright law, which is not a direct effect of circumvention.
35 Article 30 Paragraph 1 Item 2 of the Copyright Law of Japan.
36 See, Yoshida et al., supra note 30 at 95. In such a case, although not clearly stated, reproductions necessarily made in the course of exempted uses should be also exempted regardless of Article 30 Paragraph 1 Item 2.
recognizes the principle of free access under copyright law,\(^{37}\) it concludes that it was Congress’s intention to prohibit circumvention of access control that leads to the exploitation of copyright.\(^{38}\) On the other hand, Japan decided not to regulate direct circumvention under copyright law, paying full respect to the principle of free access.

The second difference is the respect for copyright exemptions. In Japan, circumvention for the purposes exempted under copyright law is allowed, thereby giving exemptions priority over the regulation of circumvention. This issue is treated in a more unfriendly manner for users in the U.S.\(^{39}\)

The conflict between fair use and anti-circumvention regulations had already been recognized at the time of legislation in the U.S.\(^{40}\) For example, the Second Circuit states that §1201 (c)(1) does not justify circumvention for the purpose of fair use.\(^{41}\) Therefore, as Ginsburg points out, §1201 (c) is “irrelevant” to the problem of diminishing fair use chances.\(^{42}\)

Difference in culture or social norms between the two countries may have some

\(^{37}\) Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1193 (Fed. Cir. 2004).

\(^{38}\) Id. at 1197-1203.


\(^{41}\) Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001).

\(^{42}\) See, Jane C. Ginsburg, Copyright Use and Excuse on the Internet, 24 Colum.-VLA J.L. & Arts 1, 8, (2000).
influence in the different treatment regarding the “right to hack for fair use.” Although an amendment to allow people to “hack for fair use” has been proposed in the U.S., it was unsuccessful because of the concerns of the “misuse” of such a right. As Kevin Saul, Director of the Trademark, Copyright & Corporation, Marketing and Legal Department of Apple Computer, Inc. says:

If we state fair use as a right, I think there would be more abuses of copyright. It is different from “Well, it could be an infringement, or could be fair use.” Because that is how I support the business people. They are very loose minded on fair use. It really helps to say to them, “look, if we are not sure it’s fair use, it’s an infringement.”

Yoshisuke Kuroda, General Manager of the Planning Department, Network Application & Solutions Division of Sony Corporation has a similar impression:

[Our DRM design called] “Open MG” is based on specifications decided in SDMI. Therefore, you can check in and check out content to portable devices three times. In Japan, when we released the Open MG, both end users and right-holders accepted the rule almost without any opposition or resistance because it is based on SDMI. However, in the U.S., there is still resistance in the market. We have already released the devices in the U.S. market, but both media and users give us comments or complaints like “why is there such restrictions?” I don’t know whether such a difference comes from cultural differences, or whether the U.S. people have a stronger feeling toward Fair Use “rights.” Anyway, I feel a real difference.

---

43 Interview with Kevin Saul, Director, Apple Computer Inc., in Cupertino, Cal. (Nov. 20, 2003).
44 The Secure Digital Music Initiative (SDMI) is a forum of more than 200 companies to discuss data protection of digitalized music in the world of digital and network technologies. It released technological specifications in 1999-2001, but was never widely implemented as a common commercial platform. See, http://www.sdmi.org/ (last visited April 25, 2006).
45 Interview with Yoshisuke Kuroda, General Manager, Sony Corporation, in Tokyo, Japan (Dec. 17,
3.1.2 Anti-device Regulation (or Indirect Circumvention Regulation)

3.1.2.1 Japanese Regulations

It is a strange twist that Japan is very modest regarding direct circumvention regulations while rather aggressive regarding anti-device regulation. This is mainly because of the amendment of the Unfair Competition Prevention Law (UCPL), the idea of which was to “protect the services that rely on access control,” while regulation under the Copyright Law is as modest as direct circumvention regulation is.

3.1.2.1.1 Copyright Law

In Japan, the scope of anti-device regulations is also limited under the copyright law. In terms of protected technologies, anti-device regulation also focuses only on usage control and not on access control. The rationale is the same as that for direct circumvention regulations described above.46

The scope of acts that are regulated is narrower than most other implementation examples. The key points are: (a) devices are limited to those with the “principal function” of circumventing technological protection measures, which is narrower than devices with “only limited commercially significant purpose for use other than”

---

46 See, supra Section 3.1.1.1.
circumvention in the U.S.; (b) the dissemination is limited to the public; and (c) remedies are granted only through criminal procedures.

To explain in more detail, the definition of devices that are regulated is a “device having a principle function for the circumvention of technological protection measures (such a device includes such a set of parts of a device as can be easily assembled) or copies of a program having the principal function circumvention of technological protection measures.”

And the efforts that are regulated under anti-device regulations are: (1) to transfer to the public the ownership of; (2) to lend to the public; (3) to manufacture, import or possess for transfer of ownership or lending to the public; or (4) to offer for use by the public those circumventing devices. Manufacturing such a device and transferring a copyrighted work to a specific person does not constitute a violation of this regulation. The reason for limiting device regulation to actions toward the public is to limit the regulation to actions that have a large impact on the interests of copyright owners.

In addition, there is only a criminal statute and there is no civil remedy for the violation. According to the official commentary, this is because copyright owners can

---

47 Article 120 bis Paragraph 1 the Copyright Law of Japan.
48 Id.
49 See, Yoshida et al., supra note 30 at 97.
anticipate the circumvention of usage control of copyrighted materials at the time of manufacture or offer of the circumventing devices, and thus it is regarded that the interest of the copyright owner is not mature enough to be granted civil remedies based on specific copyrighted materials.\textsuperscript{50}

\textbf{3.1.2.1.2 Unfair Competition Prevention Law}

As can be seen above, anti-device regulation is rather limited in the Copyright Law in Japan. However, the National Diet at the same time amended the UCPL to regulate circumventing devices for access control, based on an approach of competition regulation rather than of copyright protection.\textsuperscript{51} That is, in the UCPL, the anti-device regulation is much broader compared to that under copyright law as described above.\textsuperscript{52}

First, it is broad in a sense that the anti-device regulation under the UCPL includes both usage control and access control. The idea is to protect the businesses of content providers who charge fees for providing technologically controlled content, and from

\textsuperscript{50} Id. at 99.

\textsuperscript{51} The official commentary explains that the UCPL does not regulate the act of circumvention (by using circumventing devices) because such circumvention would be difficult to find and would give less damage compared to the commercial sale of the devices. See, Yoshida et al., supra note 30 at 244.

\textsuperscript{52} Article 2 Paragraph 1 Item 10 of the UCPL defines as unfair competition: commercially transfer, display for transfer, export and import of devices and software program; and public transmission of software program; that has the sole function of circumventing technological measures commercially employed to control the access and copy of images, sounds and software programs. Item 11 prohibits the same conduct listed in Item 10 for the purpose of circumventing technological protection measures commercially employed on services that allows specific audiences to access or copy images, sounds and software programs. [Official English translation of the UCPL not available.]
this perspective, the distinctions between usage and access that are relevant under copyright law are not competent.

Second, the regulation in the UCPL lacks a distinction between copyrighted materials and the public domain, because this regulation is designed to be outside the copyright regime. From the perspective of unfair competition among content providers, it is claimed to be unimportant whether the distributed materials are copyrighted or not. Any kind of digitalized materials can be commercial goods for fair competition. Therefore, it does not matter whether the materials the entrepreneurs provide are copyrighted or not. Content providers who are providing others’ copyrighted materials or even materials in the public domain can seek civil remedies based on the UCPL.

Third, the UCPL does not limit the entitled persons to copyright owners: all entrepreneurs using controlling technologies for their business (mostly broadcasters and other content providers) are entitled to seek injunctions and/or damages. This means that even a non-exclusive licensee (distributor) of copyrighted works, who is not entitled to exercise copyright, can assert and enforce protections toward circumventing devices under the UCPL.
The UCPL has only one statutory exemption for “testing and research.”\textsuperscript{53} The article is very simple. It states that to assign, transfer, display, export, import, or provide over the Internet the circumvention devices or programs “for the purpose of testing or research regarding technological protection measures” is exempt. There is no detailed limitation regarding the definition of “testing” and “research,” as is the case in the DMCA. The official commentary explains that the aim of the exemption statute is to ensure free and competitive activities targeted toward developing more sophisticated technological protection measures.\textsuperscript{54} The exemption is intended to include all of the following activities: testing and research done by the service providers alone, or together with device manufacturers for developing new technologies; testing and research for validity and vulnerability of technologies currently used in the service or to be used in the future service; and testing and research done by content owners to ensure the effectiveness of the protection measures, or comparing the pros and cons of the several technologies that may be applied to their content.\textsuperscript{55}

However, the commentary also explains that it was a deliberate decision of the

\textsuperscript{53} Article 11 Paragraph 1 Item 7 of the Unfair Competition Prevention Law of Japan.
\textsuperscript{54} See, Yoshida et al., supra note 30 at 252-253.
\textsuperscript{55} Id.
legislators not to have any other statutory exemption.\textsuperscript{56} With regard to exemptions for law enforcement or other government activities, the legislators decided them unnecessary because circumvention devices provided for such purposes cannot be regarded as “unfair competition” and, therefore, are not regulated under the UCPL in the first place. The legislators also talked about creating a statutory exemption to respect the copyright limitation statutes, but they finally decided not to. Their reasons were: (a) circumvention devices could create considerable economic loss to content owners if misused, and (b) legitimate and acceptable uses would not be regulated under the UCPL because such uses would not cause “commercial damages” large enough to be regulated under the UCPL.

3.1.2.2 Difference between the U.S. and Japan

In terms of regulated devices and information, anti-device regulation is broader in Japan than in the U.S. in two aspects. First, although limited to commercially based activities, technological protection measures are protected even when applied to the public domain under the UCPL in Japan. However, this difference does not make a large difference in practice, because, in most cases, the same technologies would be used to protect copyrighted as well as public domain works, and it is very hard to

\textsuperscript{56} \textit{Id.} at 253 footnote 25.
imagine a device that circumvents technologies only when protected works are in the public domain, given the current situation where there is no systematic ways to mark the difference between the public domain and copyrighted works. Therefore, the devices that are regulated under the UCPL in Japan would probably be also regulated under the anti-device regulations in the U.S.

Second, Japanese anti-device regulations have a broader scope of regulation in terms of persons entitled to the claim, i.e., the UCPL protects content providers (or licensees and distributors) in addition to copyright owners, while in the U.S., it protects only copyright owners.

On the other hand, there are several points where the U.S. anti-device regulations seem to be broader. First, both copyright law and the UCPL in Japan limit controlled devices to those whose “principal function” is to circumvent protection measures. In the U.S., devices that have “only limited commercially significant purpose for use other than” circumvention are also regulated, which is tailored in a broader manner than in Japan.

In the U.S., some cases ruled that anti-device regulations are even applicable to devices that have several different functions, one being “only limited commercially
significant purpose for use other than” circumvention, but others being legitimate.\footnote{See, \textit{RealNetworks, Inc. v. Streambox, Inc.}, 2000 U.S. Dist. LEXIS 1889, 22-23 (D. Wash. 2000) (quoting Nimmer \& Nimmer, \textit{Nimmer on Copyright} (1999 Supp.), 12A.18[B], stating that “a given piece of machinery might qualify as a stable item of commerce, with a substantial noninfringing use, and hence be immune from attack under Sony's construction of the Copyright Act- but nonetheless still be subject to suppression under Section 1201.”); followed by \textit{Chamberlain Group, Inc. v. Skylink Techs., Inc.}, 292 F. Supp. 2d 1023, 1037 (D. Ill. 2003) (“Indeed, in the \textit{RealNetworks} case, the court was presented with a product that had both a legitimate purpose and also functioned as a means to circumvent the plaintiff's protective measures. The RealNetworks court found that the portion of the product that circumvented the protective measure was enough to violate the DMCA.”). This interpretation is also supported by \textit{Chamberlain Group, Inc. v. Skylink Techs., Inc.}, 381 F. 3d 1178, 1198 (Fed. Cir. 2004), although given a different fact, they concluded differently.\footnote{See, Felton case described in \textit{infra} Section 3.3.2.}}

Even though this issue has not yet been heavily tested in front of the court, if this trend continues, there may be a clear difference in scope of anti-device regulations between the U.S. and Japan. Though not yet ruled by the courts, if the requirement of the “principal function” being circumvention of protection measures is interpreted as “no other significant functions,” multiple-functioned devices may be exempted under Japanese anti-device regulation. The answer remains to be seen at this point in time.

Second, the regulated devices in the DMCA may cover a broader scope of tangible or intangible goods, or at least causes some ambiguities as to what kind of goods are regulated. As described below,\footnote{See, \textit{Felton} case described in \textit{infra} Section 3.3.2.} the RIAA once alleged that even an academic paper discussing a security hole regarding watermarks can be a “technology” regulated under the anti-device regulations in the U.S. This would not happen in Japan, as both copyright law and the UCPL make it clear that they regulate tangible devices or their
parts and computer software, thereby avoiding some chilling effects.

Third, under the DMCA, manufacturing even a single device can be illegal. In addition, statutory exemptions are very narrowly defined. On the other hand, under Japanese copyright law, anti-device regulations prohibit only activities targeted toward the public. This means that, under Japanese copyright law, a hacker (whether a good researcher or a bad pirate) can do their “research” and try to develop and design a device that circumvents DRM technologies without permission, as long as the hacker does not engage in mass-scale activities. This would explain why Japanese copyright law does not have exemptions for scientific research, security testing, or other legitimate activities. The UCPL, on the other hand, regulates distribution of a single device as long as such distribution is made for commercial purposes. However, the UCPL has a broad, general exemption statute that includes almost all kinds of “testing and research” regarding technological protection measures. Therefore, Japan is overall friendly to scientific research.

3.1.3 Copyright Management Information Regulation

Another regulation that legally supports technological controlling measures is the
“copyright management information (‘CMI’) regulation.” The CMI regulation is also an implementation of the requirement of the 1996 WIPO Treaties.

Metadata, such as terms and conditions of use and information about copyright owners, are protected under the CMI regulation. Included are metadata written in REL and other contractual languages used in DRM systems.

The scope of CMI regulations in the U.S. and in Japan are similar. In addition to the obligations set forth in the WIPO Treaties, both the DMCA and Copyright Law of Japan prohibit people from providing false CMI.

As there are not any distinct cases that have tested CMI regulations in either the U.S. or Japan, it is rather difficult to determine the real scope of the regulations. However, because CMI regulations prohibit changing metadata, including REL descriptions, and because REL is one of the major components of the DRM technologies, CMI regulations can have almost the same impact as the rest of the anti-circumvention regulations.

3.2 Pros of Anti-circumvention Regulations

---

59 17 U.S.C. §1202, Article 2 Paragraph 1 Item 21 and Article 113 Paragraphs 3 and 4 of the Copyright Law.
60 WCT Article 12 and WPPT Article 19.
62 Article 2 Paragraph 1 Item 21 and Article 113 Paragraphs 3, 4 of the Copyright Law.
63 17 U.S.C. §1202(a), Article 113 Paragraph 3 Item 1 of the Copyright Law.
The merit of anti-circumvention regulations is that they can add protection to the DRM technologies as business enablers. As Nobuhiro Nakayama points out, for example, every DRM technology is destined to be broken, and, in practice, given the acceptable cost to be spent on DRM technologies from a business perspective, content providers often have to put up with DRM technologies that are not strong enough. Therefore, he concludes that providing legal protection to DRM technologies is necessary for the growth of a “healthy” information society.

It also helps add deterrence to break DRM technologies with the intention of pirating copyrighted works. To form this point slightly differently, it may help right-holders to release more content in a digital form by providing additional protections. For example, Shiburo Tokano, Manager of the Musical Copyright Section of the Intellectual Property Division at Yamaha, states that technological protection measures and deterrence added by anti-circumvention regulations are very important for ring-tone providers, as the data of ring-tones are very small and easily distributed.

3.3 Cons of Anti-circumvention Regulations

3.3.1 Impact on Overriding Problems: Fixing problems created by DRM

---

64 See, Yoshida et al., supra note 30 at ii.
65 Id.
66 Interview with Yoichi Misawa, Assistant Manager, Yamaha, in Tokyo, Japan (Dec. 24, 2002).
Technologies

However, anti-circumvention regulations, both in the U.S. and Japan, are also causing problems by fixing the problem DRM technologies are causing by blindly protecting any kind of DRM systems/designs.

For example, the Second Circuit declared in the Corley case that circumventing DRM technologies even for the purpose of fair use is not permissible under the DMCA.\textsuperscript{67} This means that the DMCA is fixing the problem of diminishing the benefit of or adding cost to fair use. Realizing that copyrighted works with analog output can be recaptured and used, the Second Circuit states that “the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses.”\textsuperscript{68} However, Corley does not refer to cases where analog output is not available, such as use of computer software codes.

In Japan, the problem of overriding some freedoms is less problematic, as circumvention is allowed under copyright law if it is made for the purpose of uses exempted by law. However, this “freedom to hack” is helpful only for technologically savvy people who have enough knowledge and skills to circumvent DRM technologies.

\textsuperscript{67} 273 F. 3d. at 443.
\textsuperscript{68} Id. at 459.
Those who are not technologically savvy need to have a tool to make the necessary circumvention. Therefore, the anti-device regulations create unfairness between the technologically savvy and non-savvy.⁶⁹

### 3.3.2 Impact on Scientific Research: Chilling Effect

In the U.S., anti-circumvention regulations can create a chilling effect on scientific research, especially in the field of security research. This is because the basic manner of security research is for researchers to investigate security problems, discuss them among themselves, write code to fix the problems, and test and challenge such codes with each other.⁷⁰ If the circumvention itself is generally prohibited, they are not able to do research.

Because in the DMCA the statutory exemption for conducting research is narrowly tailored, it has been claimed that it causes a chilling effect.⁷¹ The famous case is the “Felten” Case, where Princeton Professor Edward Felten once withdrew from presenting his paper about the security hole because of a threat based on the DMCA.⁷²

---

⁶⁹ Benkler, *supra* note 18 at 416.
⁷¹ For example, Niels Ferguson, a Dutch cryptographer, declared that he would not publish his article regarding the security weaknesses of a cryptographic system due to his fear of violating the DMCA. *See*, Niels Ferguson, *Censorship in Action: Why I don’t Publish My HDCP Results*, August 15, 2001, http://www.macfergus.com/niels/dmca/cia.html,(last visited April 25, 2006).
Carter Laren, Senior Security Architect at Cryptography Research, describes the chilling effect created in the field of security research as follows.

I understand the motivation behind [the DMCA]. I understand that studios don’t want their content stolen, and I agree that content shouldn’t be stolen.

However, DMCA is actually bad for security. The reason for this is: DMCA makes it illegal to build bypass equipment, for example. Of course, they have carve outs for research and those kind of things, so you are supposed to be able to do it for these reasons anyway, but working for a security company, let me tell you, that has scared us away. No one wants to test that.

We used to, before DMCA, break things all the time. We wouldn’t release them publicly, but we would get things in, evaluate them, find the security faults, and figure out how to be able to fix them or what people are doing security-wise, and that was generally good for security. Security works by people breaking stuff. That’s how the industry works, and if you look at the publications from the cryptography conferences, I pick up any of these books and you’ll see people breaking algorithms, and someone else introducing a new algorithm in the same book and that goes on constantly. That’s how we’ve worked as a community. DMCA has been bad from that perspective; it does stifle research regardless of the intent. We were not surprised by [the Felten case when it happened].

3.3.3 Impact on Developments of Devices, Services, and Software

In the U.S., because of the narrowness of the exemptions for reverse engineering,
encryption research, and security testing, it has become much more difficult to design
new devices or new services that require reverse engineering, testing, and research
without being chilled by the DMCA.

Also, in both the U.S. and Japan, it has become even more difficult to provide
devices or services that provide interoperability with DRM-protected devices or
services. Even a device provider who provided transmitters for a garage-door opener
was sued under the DMCA.\(^\text{74}\) Without having permission from either DRM providers
or copyright holders, it is almost impossible to provide interoperability under the
current regulations, except for the very narrow exemption of §1201 (f) in the U.S.

In addition, anti-circumvention regulations have a huge impact on software
development. For example, in the U.S., a Russian programmer, Dmitry Sklyarov, was
arrested and jailed on a charge of a DMCA violation in 2001, because he was alleged
to have been involved in creating a software program that allows circumventing some
restrictions on Adobe electronic books.\(^\text{75}\)

These restrictions generally have an impact on competition and innovation, as has

\(^{74}\) Chamberlain, 381 F. 3d at 1192.

\(^{75}\) See, Electronic Frontier Foundation, Unintended Consequences: Seven Years Under the DMCA, 4
already been pointed out.  

3.3.4 Risk of Abuse by Right Owners and the State

The fundamental difference between anti-circumvention regulations, especially anti-device regulations and the traditional copyright law, is that anti-device regulations outlaw the technologies themselves rather than a particular use of the technologies.  

Carter Laren describes his fear of the abuse of such regulations:

One of the things that bothers me about this idea of legislation designed to outlaw technology is: it’s a principle that is more widely applicable than to just [stop piracy]. You can start applying it to anything that you think is immoral or wrong….  

Laren elaborates his fear, which is based on the danger of misusing a broad regulation.

I heard a lecture from an FBI cyber squad a couple of years ago…. [H]e made this argument that they needed laws that outlaw these various pieces of technology, because the more they could nail someone on, the more violations they could get, which is better. … The populace should trust the FBI to not misuse those… Don’t worry, just make it illegal and we would only go after the people that really deserve to have this happen to them.

---


77 For criticisms toward too broad anti-device regulations, see, Alfred C. Yen, What Federal Gun Control Can Teach Us About the DMCA’s Anti-Trafficking Provisions, 2003 Wis. L. Rev. 649 (2003)

78 Interview with Carter Laren, Senior Security Architect, Cryptography Research, in San Francisco, Cal. (Apr. 8, 2005).
Well, great, but there’s no guarantee that they are going after only bad people, and the government has a history of expanding their powers and doing bad things for years… So, from a philosophic standpoint, I really dislike legislation that tries to limit technology in various ways.\textsuperscript{79}

As Laren points out, the police power of the government is in question of abusing the statute in criminal cases. In civil cases, it is a private party that could abuse the regulations. There are already a couple of lawsuits based on the DMCA that can be seen as an issue of fair competition rather than of protecting copyrighted materials in the U.S.\textsuperscript{80} It is not surprising that right-holders try to exercise their rights to have a better position in the market. In the future, even an antitrust guideline might be necessary for exercising rights regarding anti-circumvention regulations, as it is now regarding patents and other intellectual property law.\textsuperscript{81}

3.4 Revisiting the Rationale Behind Anti-circumvention Regulations

Given the pros and cons described above, it is useful to ask whether any part of the anti-circumvention regulations should be re-examined, especially when its cons

\textsuperscript{79} Id.


overweighs its pros. Although the concrete legal proposal of how the
anti-circumvention regulations can be revised is discussed in Section 5 below, it is
helpful to revisit the rationale behind the regulations here to see that legal protection
over DRM technologies may not be the ultimate solution for stopping piracy and
sustaining content business in the digital and network environment.

3.4.1 Business Can Be Made with Broken DRM Technologies

If prohibiting circumvention of DRM technologies is for the purpose of enabling
content transaction, a question can be posed about its necessity, given the fact that
even a broken technological protection measure can successfully enable a content
business model.

This point is clearly shown by the example of DVD. Content Scramble System
(“CSS”), a software mechanism that tries to stop illegal access and reproduction of
content in DVD discs, was broken and made possible to circumvent using the software
called DeCSS. Regardless of several lawsuits,82 DeCSS is still widely available over
the Internet.83 Still, the DVD business is a profitable business for motion picture

82 E.g., Reimerdes, 111 F. Supp. 2d 294 (S.N.D.Y. 2000); Corley, 273 F. 3d 429 (2d Cir. 2001).
83 For example, a Webpage called “DeCSS Central” has a link to DeCSS software,
industries and sales have continued to grow every year in both the U.S. and Japan.\textsuperscript{84}

This example suggests that, having complete security may not be as necessary to sustain businesses as it is often claimed, even in the age of digital and network technologies. Also, the necessity of giving legal protection is not inevitable to sustain content business. It is rather a policy question of which is better for a society as a whole by comparing its marginal deterrence added by anti-circumvention regulations (note that right-holders already have traditional copyright to punish piracy as a result of circumvention) and their negative impact on societies.\textsuperscript{85}

3.4.2 Outlawing Circumvention of DRM Technologies Does Not Practically Stop Piracy

It is very ironic that the anti-circumvention regulations, which try to ensure that content is securely protected by DRM technologies, are strongly criticized by security experts. Carter Laren,\textsuperscript{86} Senior Security Architect at Cryptography Research,\textsuperscript{87} claims


\textsuperscript{85} For possible pros and cons of anti-circumvention regulations, see supra Section 3.2 and 3.3. However, the final answer to this policy question should be based on an empirical analysis of whether the positive or negative effects outweigh the other, which is outside the scope of this research.

\textsuperscript{86} Carter Laren did graduate work at the University of Pennsylvania in the Electronics Engineering Department. He has experience in designing secure communication system for the military. His role in Cryptography Research is to help design and implement Pay TV security technologies. Currently, he is
that anti-circumvention does not help solve the security side of the technological problem, especially in the long run. He understands that the basic idea behind the anti-circumvention regulations is to make the transaction fair. As Jeffery Lawrence at Intel says, “if there is naked content next to protected content, no one is going to buy the protected content.”

Still, Laren believes that such legislation cannot practically stop those who want to hack technologies. As Laren says:

You cannot [stop them]. You can make [circumvention] software available by download from anywhere in the world, [and] there’re jurisdictional issues…. Even though DeCSS is totally illegal, someone has a server that’s in the Bahamas that has DeCSS and you can download it. If they try and put filters on it, [in order] to filter and see you’re getting DeCSS, they will encrypt it and give you a key. And you’ll download it and decrypt it…. There’s always a way to get around this kind of stuff.

Therefore, according to Laren, prohibiting circumvention of technological protection measures by law does not solve the problem in a substantial way. Of course, it is true

in charge of building high definition optical disks, and is heavily involved with efforts to make them secure.

Cryptography Research is a 10-year-old cryptography research company founded by Paul Kocher, an expert in the U.S. cryptography community. The company deals primarily with the implementation of cryptography in the social system, such as Pay TV services, credit cards, and coming high definition optical media by consulting, analyzing the systems, anticipating attacks on their security systems, and coming up with counter measures, such as re-designing the system, among others. Recently, they spent several years thinking about optical media. In the late 1990s, they concluded that DVD was clearly bad from a cryptographic point of view, although it was a successful business model. They started their project by thinking what they would do if they had had a chance to redesign the DVD security mechanisms. They spent couple of million dollars on research, which led to their involvement in the discussion of the security design high definition optical disks.


Interview with Carter Laren, Senior Security Architect, Cryptography Research, in San Francisco, Cal. (Apr. 8, 2005).
in every case that having an enforceable law does not completely stop illegal actions. It
is also true that outlawing some action may serve as a deterrent to some extent.

However, given the impracticality to stop circumvention, Laren points out that the
effect of outlawing circumvention does more harm than good, as it chills the
“good-minded hackers”, i.e., security researchers who find security holes earlier than
bad-minded hackers, who often do not care about the risks of breaking the law.90

3.4.3 DRM Technologies Are Not the Final Solution to the Piracy Problem

In addition, anti-circumvention regulations that legally protect DRM technologies
also may not be as efficient for reducing mass-scale piracy as people expect, because
DRM technologies are not the final solution to the problem of piracy.

The problem of piracy fundamentally exists in the evil minds of those who steal
content, not in the incompleteness of technological security. However secure the DRM
technologies are, they can be broken if one spends enough time and money. And even
more importantly, the protected content should be able to be played and exploited by
“customers” who purchased the content, and such “customers” can be the largest
security hole in a distribution chain.

Carter Laren discusses this point in detail. First, he says that DRM technologies

90 See, supra Section 3.3.2.
cannot cure the piracy problem.

The interesting thing is that, a lot of people that are not cryptographers, that are not security experts, have this idea that cryptography is really good for fixing their problems [of piracy].

As Laren elaborates, he first explains the primary purpose of security technologies.

[Given my background of serving as a security expert in the U.S. military,] let me explain why cryptography is not really enough to solve the problem here. Cryptography is designed for a very different problem: and that problem primarily is one of secure communications. If I’m a trusted party and you are a trusted party, we both trust each other, we know each other. Let’s say we are both generals in the military. And we want to speak some secrets to each other, but we don’t want a third party to eavesdrop or change our conversation. Cryptography is great at solving that problem.… We can see that the data is encrypted, and there are a lot of great security statements that you can make about the fact that if someone is listening in the middle, they can’t change anything or eavesdrop. So, in military systems, cryptography is very important.

However, as Laren says, the piracy problem is different from the secure communication problem. He elaborates:

If you look at the problem of piracy, it’s not a secure communications problem at all. Piracy is a totally different problem, which is: I own some content, I trust you, and I want to let you see the content, so I am going to give it to you. But then after I trust you, you change your mind and become a traitor, and you share the content with someone else…. I can very easily send you content in a way that no one in between can get the content. But once you have it, cryptography doesn’t really help me control it in any way. And that’s really the problem with piracy. As a

---

91 Interview with Carter Laren, Senior Security Architect, Cryptography Research, in San Francisco, Cal. (Apr. 8, 2005).
92 Id.
result, piracy becomes a lot messier to deal with, because it starts to turn into an engineering problem with practical limits, and you start to try to minimize [the risk] instead of get rid of it.\(^9\)

In sum, Carter emphasizes that the core of the “piracy” problem is essentially in the evil intention of people who first get the content as “customers,” and not the security of content delivery. It is very hard, especially in the mass content market, to distinguish good-minded customers who use the content as they are expected to, and ill-intentioned “customers” who then turn into pirates. And this characteristic can be applied not only to the cryptographic component of DRM technologies, but to other parts such as REL and watermarks.

Given this fact, the role of DRM technologies, from a security point of view, is to increase the cost of piracy by making it difficult and costly rather than completely eliminate it. More secure DRM technologies make it harder for pirates with commercial intentions to build business on them, and at the same time, make it almost impossible for technologically non-savvy people to take out the content. If so, a solution to the problem of piracy that is effectively using DRM technologies, can be approached not from a legal viewpoint, but rather from the viewpoint of market and

\(^9\) Id.
technologies (or architecture),\footnote{As Lawrence Lessig points out, people’s behaviors can be regulated through any combination of the four factors: law, market, social norms and architecture (including technologies). See, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85-99 (Minneapolis: Sagebrush Education Resources 1999).} which is described in the next Section.

3.4.4 Problem of Piracy Can Be Solved Through Market and Technologies

There is an approach other than legislation to solving the problem of piracy: using technology and the market. As it takes time and money to break technologies, the more secure the distribution infrastructure is, or, more precisely, the more costly it is to steal content, the less likely piracy will occur. If circumventing technologies costs more than the benefit derived from such circumvention, commercial hackers will not try to circumvent the technologies. Also, in the case of non-commercial hackers who take delight in the act of hacking itself, if the damage is small enough to sustain the business model, it could be handled as a manageable risk by the industries.

Damage from piracy, from a business perspective, can be measured by the probability of circumventing the DRM technologies multiplied by the loss caused by such circumvention. Carter Laren explains:

I am going to use an example of credit cards here, because fraud is similar to [piracy]. Anyone can just decide to be you, or they can steal your credit card and commit fraud pretty easily. The way Visa and Mastercard, for example, look at their risk is, they really view it in terms of the probability of attack times consequences of the attack. They know that the probability is sort of high, and they have to mitigate the
consequences, and they can try to reduce both parts of the equation if they want. But in order to do this, they really set up an infrastructure that allows them to do two major things: one is to detect when there are problems, and the other one is to respond to problems when they occur.95

Then, Laren describes one possible business approach as an example, which tries to minimize both the damage of circumvention and the incentive to circumvent DRM technologies. First, Laren explains the mechanisms of commercial pirates.

In our work with Pay TV companies, if you look at the people who are actually pirates (… I mean, people who are actually developing the attacks and selling them to consumers), those are generally organized crime…. They are usually willing to invest a large amount of non-recurring engineering costs to develop an attack, if they know that they can then use this attack again and again.

So, in the pay TV space, for example, an organization will spend half a million to a million dollars to take a smart card, … [and the card would be] reverse engineered, and imaged. This is an expensive process, [but] they hire engineers to figure out exactly what it is doing, [and] reverse engineer all the code. They spend all this time and all this money, because, at the end of the day, they can produce a little box for $300 that they can sell over the Internet, that everyone would want, and … they make their money back pretty quickly. It’s a business to them.96

Then, Laren suggests a possible solution through market mechanisms.

One of the reasons that pirates can be successful is because they don’t have any recurring cost. A lot of these systems have got something like all these rules built into a smart card or built into a player…. Once [the pirates] attack them, all the content is subject to those rules, and that

95 Interview with Carter Laren, Senior Security Architect, Cryptography Research, in San Francisco, Cal. (Apr. 8, 2005).
96 Id.
attack works for everything.

If you sort of turn this on its head and you require, instead of the player being smart, the content has to be smart. Now, you can invest all this energy in this piece of content, but you cannot leverage it, because [for] the next piece of content, you have to reinvest all your energy [to break new technologies]. It means that your game with pirates is now a little more equitable. It means, instead of them being able to do this one shot deal and you are done, they have to keep investing, which is always good [for content owners]. You are not going to stop piracy, but it’s always good to make it harder for them and force them into these different business models.  

In sum, when you change technological protection measures on a content-by-content basis, for example, the gain from one case of circumvention is only one kind of content, which is far smaller than it is now. It will decrease the benefit, and thus the incentive for commercial pirates, to hack DRM technologies. It will also reduce the damage the content owner will suffer, even in the case of hackers without commercial intention.

Nobuyuki Watanabe at NTT Docomo describes this “protection by market” from a different aspect. As Watanabe explains, there are very few problems regarding piracy in the content distribution services in the i-mode market, and, to a large extent, this is because a rational person would not try to hack the content.

For persons with normal technical expertise, when they attempt to remove [content] from their handsets, they will end up breaking the handsets. And since [the content] is on a level of ¥300, if you ask

\[ Id. \]
whether breaking down a handset will pay, I don't think so. If the content were several tens of thousands of yen, it might be worthwhile obtaining the content even though the handset broke down, but … I think buying would be more reasonable at the cost of ¥100 or ¥300.98

It may not be clear whether these kinds of approaches using market and technologies would be better in every. However, it would have been at least worth studying such a question before taking legal action. In this regard, Carter Laren asks why content owners rushed to legislative means without even trying to take a “market and architecture” approach.

I think the reason why Hollywood is pushing [legislation that prohibits technology] more than other industries is because … they don’t know how to solve the problem any other way…. They have this problem; they don’t know about technology, they know about lobbying, so that’s what they are going to do: they jump on legislation.99

As Lawrence Lessig explains, legal regulation is only one means of regulating people’s behavior, such as copyright infringement.100 There is no reason why they should opt for only legal means. If copyright owners want to avoid piracies caused by circumvention of DRM technologies, they can also seek other means than law, i.e., technologies and the market. Whether adding legal protection is good for the society and thus justified should be answered by comparing the pros and cons of the specific

98 Interview with Nobuyuki Watanabe, NTT Docomo, in Tokyo, Japan (Dec. 11, 2002).
99 Interview with Carter Laren, Senior Security Architect, Cryptography Research, in San Francisco, Cal. (Apr. 8, 2005).
100 See, Lessig, supra note 94 at 87.
regulations, which is outside the scope of this research. However, it is useful to recognize that anti-circumvention regulations are not the only means to “fight with piracy.”


If not all, some of the override of freedom caused by DRM technologies and anti-circumvention regulations can be solved if the implementation of DRM technologies are well balanced. This Section explores whether the market can cure the problem of too strict implementation of DRM technologies.

After presenting this question (4.1), this article describes the differences in legal standing between right owners and the users of copyrighted works as one of the background factors in the market negotiation regarding DRM implementation (4.2). Then, this article describes the actual market mechanisms of development and implementation of DRM technologies (4.3). It concludes with some analysis of whether the market really can solve the problem of strict implementation of DRM technologies (4.4).

4.1 Problems of the Development and Implementation of DRM Technologies

As described in Section 2, the two sources of overriding freedom within the

---

101 See, supra Section 2.2.2.
copyright regime are (i) the manner of actual implementation of the DRM technologies, and (ii) the limitations caused by the differences in nature between computers and human beings. This research recognizes that it would be difficult in the short run to overcome the second problem. Therefore, this research focuses on the first issue: whether the market can fix the problem of too strict implementation of DRM technologies that overrides the freedom incorporated within the copyright regime.102

Obviously, the rules of DRM implementation make a large difference in the market, both for content users and right-holders. A good and well-known example is Apple’s iTunes Music Store, launched in April 2003.103 Before the iTunes service, the rules set by online music stores were very strict and hardly allowed copies or transfers of content that users purchased. Sales by these online stores were very low, and the RIAA accused peer-to-peer file-sharing software as the major reason for the low sales.104 However, after the launch of the iTunes Music Store, the recording industry is now convinced that people are willing to pay for the music they download.105 It may be

\[\text{\footnotesize 102 For a discussion of whether DRM technologies can be freedom-friendly, see infra Section 5.1.2.1.}\]
\[\text{\footnotesize 105 The iTunes Music Store sold over one million songs in its first week, reached to two million downloads in less than 20 days. In less than two months, the store hit five million downloads, and by the}\]
that one of the most important reasons the iTunes Music Store became so successful is because of the relatively flexible usage rules they applied to songs purchased from them. Users can burn unlimited number of CDs, although a particular playlist can only be burned up to 7 times before the playlist must be changed. They can also transfer the purchased song up to five different computers, or wirelessly stream it to another computer or stereo.106

Still, the trend of DRM technologies is to “manage and control” the usage of content. As Yoshisuke Kuroda, General Manager of the Planning Department, Network Application & Solutions Division, Sony Corporation, said in 2002:

With current technological development, it will ultimately become possible to control from delivery of contents to the user end. One could, if one wanted, create a system which enables the content provider to obtain information indicating how many times or from when until when the user has played [content]. Accordingly, the technological trend is toward [control]. The problem is rather how to show [such control] to the user, or to what extent to allow the user [to use the content]…. Amid these trends, technological development has become important in order to have compatibility, from the standpoint of the user, to allow the user to do the same things he has done up to this point.107

end of 2003, it had sold more than 25 million songs. Sales are still growing, and as of January 2005, Apple stated that their customers were downloading 1.25 million songs per day. Total downloads hit 300 million in March, 2005. See, Apple Computer Inc.’s Press Release Library, http://www.apple.com/pr/library/, (last visited April 25, 2006).

107 Interview with Yoshisuke Kuroda, General Manager, Sony, in Tokyo, Japan (Dec. 17, 2002). Note, however, that this is before the success of the iTunes Music Store, which might have affected his view later on.
In addition, even the DRM used in the Apple’s iTunes Music Store does not allow derivative uses or other uses that may be allowed under fair use or other copyright exemptions.

If one puts the popularity of the iTunes Music Store and the technological trend of control together, a question arises: Why did DRM technologies begin to be implemented with strict usage rules, even though it was possible to implement them in a more flexible way? Why is it not popular in the market to implement DRM in a manner that is flexible enough to make it popular among consumers, or to respect the freedom allowed under copyright law?

It is true that there are varieties of choices in how to implement DRM technologies. Chris Parkerson, DRM Evangelist at RSA Security, says that this problem may partly be solved by the market, as it finally comes down to the problem of a good business model.

The technology exists to do whatever consumers want, or whatever Hollywood wants to do to protect their content. It just comes down to best practices…. But the best practices really haven’t arrived yet.\textsuperscript{108}

However, finding the “best practices” is not an easy job. In addition, “best practices” in the market may not mean that it reflects the freedom incorporated in the

\textsuperscript{108} Interview with Chris Parkerson, DRM Evangelist, RSA Security, in L.A., Cal. (Mar. 31, 2005).
copyright regime. Therefore, it is interesting to look into the question of why DRM implementation tends to be favorable to right-holders. In the following, this section tries, based on interviews, to describe several factors that contribute to strict implementation of DRM technologies. It also tries to see whether the market can correct the problem of overriding freedom within the copyright regime, given the current legal regulations.

4.2 Legal Entitlement

The first issue to be pointed out is the difference in legal standing or entitlement between copyright owners and information users. This is important to notice, as the differences in legal standings appeared to have an impact on the power balance between copyright owners and users in the course of negotiations in the market, as described below.109

As is obvious, copyright owners have a legal entitlement to decide how their works are used, as long as copyright law grants such rights. Therefore, as a natural and logical consequence of who has the final say on deciding the implementation rules of a particular DRM system, both right-holders and device manufacturers agree that it is the right-holders. Howie Singer at Warner Music states that “It is the content

109 See, infra Section 4.4.
companies that decide what the usage rules are.”\textsuperscript{110} And so does Intel’s Jeffery Lawrence. To the question of who decides the actual usage rules of DRM, Lawrence answers, “It is the content provider. Because, under the copyright law, the law gives content providers the power to decide.”\textsuperscript{111}

On the other hand, the freedoms within the copyright law, such as fair use and other statutory exemptions, have been characterized as an “affirmative defense” in the U.S. copyright law.\textsuperscript{112} Thus, right-holders repeatedly claim that users of copyrighted works do not have a “right” to freely use copyrighted works, even with regard to uses that are exempted from copyright under the law.

The legal landscape regarding “freedom” within a copyright regime is not so different in Japan. There has been some discussion about whether some of the statutory exemptions could be regarded as “rights” or “mandatory statutes” that could invalidate inconsistent agreement clauses, but the issue is still far from being settled. For example,

\textsuperscript{110} Telephone Interview with Howie Singer, Vice President, Warner Music (Nov. 18, 2003).
\textsuperscript{111} Interview with Jeffery Lawrence, Attorney, Intel, in Hillsboro, OR. (Aug. 14, 2003).
\textsuperscript{112} It is usually said that fair use is an affirmative defense and not a right. See, e.g., Nimmer & Nimmer, \textit{Nimmer On Copyright}, Section 13.05 (LEXIS Publishing [Distributor], 2005). However, given the underlying values and its importance, there are also views to consider copyright exemptions as more than a mere defense. See, e.g., \textit{Bateman v. Mnemonics, Inc.}, 79 F. 3d 1532, 1542 n. 22 (11th Cir. 1996) (Birch, J.) (“Although the traditional approach is to view fair use as an affirmative defense, this writer, speaking only for himself, is of the opinion that it is better viewed as a right granted by the Copyright Act of 1976.”) See, also, supra note 15. For a freedom to read anonymously, see, Julie E. Cohen, \textit{A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace}, 28 Conn. L. Rev. 981 (1996).
Koizumi and Watanabe argue that the private copying statute does not grant an affirmative right and that users cannot, therefore, justify their violation of contracts or circumvention of DRM systems that eliminate private copying.\(^{113}\)

There is, therefore, an imbalance of power between the interests of the right-holders and the users, because the former are supported by legal entitlement, while the latter are not, even for uses that are exempted by the law and thus are legitimate.

### 4.3 DRM Development Process and Power that Copyright Holders and Users Have in the Process

Taking into account the imbalance of legal entitlement above, this section considers whether imbalanced DRM implementation could be cured through market processes. The considered factors are (a) how much copyright law impacts the process of DRM implementation (4.3.1), (b) de facto controlling power by right-holders arising from the process or procedure of DRM implementation (4.3.2), (c) relatively strict mind-set of right-holders (4.3.3), (d) tragedy of the anticommons that...

---

right-holders suffer (4.3.4), and (e) relatively weak voices and power of users of copyrighted works in the market (4.3.5).

4.3.1 Impact of Law in the Process of DRM Implementation

The first question in focus is this: to what extent is the copyright law, especially the freedom within the copyright regime, considered and respected in the course of implementation? This question is important, because if the technologist who designs and implements DRM technologies does not pay attention to the balance within the copyright law, it is impossible for DRM technologies to embody the balance that copyright law incorporates.

It is interesting to learn that law is not always the guideline that gives the final answer in the process. For example, answering the question of who determines how many copies of content are allowed in DRM-controlled devices, Noboru Tohyama, of the Legal Planning Department at Fujitsu, explained:

The engineers determine the actual specifications. I don't think legal affairs is involved all that much. For example, it was the technical people who determined a DVD format. Legal affairs become involved in the case of contracts, but it is the technical people who determine things such as how many times check-out [of content] can be performed.114

114 Interview with Noboru Tohyama, Legal Planning Department, Fujitsu, in Tokyo, Japan (Nov. 22, 2002).
In addition, many of the technical people who are deciding the actual conditions or usage terms of DRM technologies are not fully aware of copyright regulations, or, more precisely, the freedom incorporated within copyright law. Therefore, it is not surprising to find out that the consequences of the decisions made by such technical groups often do not reflect the “freedom” of users set forth in the copyright law.

Of course, a few technologists are familiar with legal issues. Yoshisuke Kuroda at Sony says that he pays attention to copyright law all the time.

Naturally, every country has its own laws, which must be obeyed absolutely. Areas not determined under the law … are determined by discussions with the content provider, and we introduce [new devices] in each country after such discussions.115

As his background, Kuroda represented Sony several times in standard-setting discussions such as SDMI. Given his background, paying attention to legal regulations is nothing surprising, even as a technologist.

However, having even a great deal of legal knowledge does not always guarantee a well-balanced DRM implementation. Specifically, device manufacturers and service providers who have sufficient legal knowledge are often very sensitive to issues related to their liabilities (including contributory and vicarious liability of users’ copyright infringement). For example, given the recent trend of increasing protection over

---

115 Interview with Yoshisuke Kuroda, General Manager, Sony, in Tokyo, Japan (Dec. 17, 2002).
copyright holders in the U.S. courts, Masaya Otsuka, Senior Patent Manager of Sony Corporation’s Planning & Control Department, said that even Sony no longer relied on the Sony rulings regarding private copying.

Within Sony, there is awareness that businesses that rely on statutes on private copying and Fair Use are now in danger. In the digital age, I don't believe the ruling in the *Sony* case will remain as it is for long. Accordingly, I believe that businesses that rely too much on statutes allowing private copying are in danger.116

In sum, the insufficient legal knowledge of the people who actually decide the usage rules of DRM systems, and some chilling effect on those who are aware of the legal issues, results in a situation where freedom within copyright law may not be paid as much attention in the course of DRM implementation as legal scholars wish.

### 4.3.2 Process and Procedure of DRM Development and Implementation

#### 4.3.2.1 Traditional Process and Procedure

Several processes of technology implementation and market release of devices also shows how much power or influence the content owners have in the market of DRM technologies. Although the following are only a few examples, it can be said that content owners clearly have had some influence over device designs.

---

116 Interview with Masaya Otsuka, Senior Patent Manager, Sony, in Tokyo, Japan (Dec. 17, 2002). As this interview was conducted before the ruling of *Grokster*, his view might be slightly influenced by the *Grokster* case. However, the point here is, that unclear legal changes regarding secondary liability could cause a chilling effect on device makers and service providers that know.
Yoshisuke Kuroda at Sony explains the custom of seeking consensus from the content owner about new devices that are released into the market. He made clear that before the release of products, the company brings the devices to industries that would have some interest in their release, and explains and negotiates laying the groundwork for the release.

Such negotiations before product releases would certainly have some impact on the features device makers could add to their products. The amount of influence is not the same, however, in the PC and consumer electronics (CE) markets. In general, the CE industry is more influenced by this consensus-seeking process than the PC industry is.

For example, regarding VAIO, personal computers designed by Sony, Kuroda admits that they always bring new VAIOs and explain the features to major right-holders. However, Kuroda says they do not always listen to what right-holders say.

I think VAIOs are taking relatively various “adventurous” features. If you ask content holders, sometimes they say no, but there are times we just go ahead and release them.

On the PC side, if we don’t offer something that other companies do offer, then from the users’ standpoint, a function is “lacking”, in which case the product won’t sell. For example, there was much debate inside Sony when we decided to add a CD-R burning function to VAIO, [but we decided to do so because we had to] in order to stay competitive in
Kuroda explains that such independence from content owners applies only to PCs, not to the CE or home electronics industries. The difference, Kuroda says, comes from the structural difference of the markets the devices are put in.

The difference in culture between the PC and CE industries is a difference of perspective. The world of home electronics is one in which you cannot do business without content. The PC world has the advantage that it is not really necessary to listen to music [using a PC]. Recently, it is becoming so that content is important for the PC as well. But the difference remains between whether having content is an absolute necessity or just “one of them.”

Bruce Polichar, former Vice President of the Entertainment Department at IBM, agrees with Kuroda’s point. Polichar elaborates the willingness of the CE industry to be more accommodating to right-holders, from the viewpoint of recouping research and development (“R&D”) costs that they have already invested. First, Polichar points out that the risks of developing new distribution technologies are always on the side of technology companies.

In almost every era of the entertainment business history, the entertainment companies have demanded that the technology companies take all of the R&D risks. The entertainment companies are always slow to make industry-wide choices about which technologies they want to endorse.

117 Interview with Yoshisuke Kuroda, General Manager, Sony, in Tokyo, Japan (Dec. 17, 2002).
118 Id.
119 E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 6, 2003, 09:45:24 PST) (on file with author).
Given such R&D risks, Polichar says that CE companies have an incentive to make the
device successful in the market, which often results in accommodating right-holders.

[CE companies] want to hear from the entertainment companies about
what kind of new delivery systems could build new sales of entertainment content. But in most cases, they have already been
working on new devices in their R&D labs by the time they start
discussions with the entertainment companies. Then they take the new
devices to the entertainment industry seeking its endorsement of the
new devices…

In other words, while the CE company is trying to achieve acceptance
of a new device, it needs the blessings of the content owners. It needs
the content owners to say they will release content on the new device.
The CE companies are often willing to give very favorable
compensation to the entertainment companies in order to get content for
the new device.120

For example, in order for DVD players to sell well in the market, the market also has
to have a variety of DVD disk titles available. Therefore, in order to convince content
owners to release the content in their format, the format has to be favorable to the
content owners.

In addition, Bruce Polichar maintains that this process matches the interests of
content holders.

The entertainment companies often fear that if they do not negotiate
licensing deals with the CE companies early in the development process
…, they will not be able to negotiate favorable deals once the device has

---

120 E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 10, 2003, 09:34:26
PST) (on file with author).
become a standard.121

Toru Maruhashi and Noboru Tohyama at Fujitsu agree with Polichar’s point. They explained their dilemma when they released DVD players. Answering the question of whose convenience they consider in determining the specifications of DVD devices, Maruhashi and Tohyama said:

(Maruhashi) It also varies according to the device. Since portable music delivery uses a complex system such as certification authorities, one also has to consider the side of operating the certification authorities. With a standalone device such as a DVD player, the sale of devices has more priority, so they pay more attention to the content holders.

(Tohyama) When DVDs were first started, we went straight to Hollywood to ask about the format, not to the users or the sales outlets.

(Maruhashi) That's true, but actually we would like to sell devices without going to Hollywood, if possible. Still, the idea was that, without any content to sell, one cannot sell players either.

(Tohyama) That's why DRM does exactly what Hollywood says.122

In sum, especially in the CE industry, there is a history of seeking the consent or blessing of the content holders, which often results in the implementation of favorable DRM rules. In the PC industry, such influence by right-holders seems to have been less in the past, which may be changing as described in the next Section.

4.3.2.2 Growing Influence of Copyright Holders in the Digital and Network

121 Id.
122 Interview with Toru Maruhashi and Noboru Tohyama, Fujitsu, in Tokyo, Japan (Nov. 22, 2002).
Environment

The influence of content owners over technological design seems to be growing in the broadband era, as the presence of entertainment content such as music, motion pictures, or books in electronic form is growing in daily lives. As these entertainments leave the tangible packages and started to be delivered online, the influence of content owners is expanding to many areas other than CE industry, such as PC industries and online distribution services.

For example, Bruce Polichar says the situation described above regarding CE companies is starting to expand to “the computer companies who are making more and more devices that are used for entertainment.”¹²³

Ron Bell, an attorney who supervises the licensing contracts and services at Yahoo’s Legal Department, says the following:

Copyright policy is a mix of content-provider friendly and user friendly. But I would put a measure of this probably more on content-provider friendly…. Some of the advocates are way in favor of consumers, and content providers are more on the DRM side of the defense, and Yahoo tries to strike a balance because we do both. Probably we are now a bit friendlier to the content providers, because we create content and we manage content, and we have contracts and restrictions and laws that we have to pay attention to.¹²⁴

¹²³ E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 10, 2003, 09:34:26 PST) (on file with author).
¹²⁴ Interview with Ron Bell, Yahoo, in Sunnyvale, Cal. (Jul. 9, 2003).
Another example in the field of online service is Musicmatch, a more focused content-distribution service online. Online content-distribution businesses in particular have to convince content owners in order to set up their business, just as the CE industry needs to have the blessing of the content owners. For this reason, when obtaining licenses, online service providers tend to have less bargaining power than right-holders, who are backed up by their legal entitlements as copyright.

First, Bob Ohlweiler, Senior Vice President of Business Development at Musicmatch, describes the long history of their struggle in starting up their music store:

Unfortunately, the download music business did not develop because the license from the music labels was not good enough to build business on. So, we had to stay [out of the distribution] business for a number of years…. At the end of 2003, Universal [Music] primarily, started to open up their mind toward to the download business. They started clearing rights for digital distributions with artists, and [provided with] reasonable licensing terms. Apple succeeded to convince several music labels to have reasonable licenses and was a big hit. That led us to do the download business at last,… 8 years [after starting the company].

He then explains that, after starting the business, their heavy dependency upon copyright influenced the usage rules of DRM technologies.

The way the DRM market works is that the DRM technology

---

125 Musicmatch is a Windows-based online music store. See, Musicmatch Homepage, http://www.musicmatch.com/, (last visited April 25, 2006).
126 Telephone Interview with Bob Ohlweiler, Senior Vice President, Musicmatch (Nov. 19, 2003).
companies go to the content owners (music and movies) and get approvals or permissions from content companies that their DRM offers sufficient protection for people to use their content. If I went to Universal Music and said I wanted to use this technology that they think is too loose, they would say “No, you can’t. Use something with higher standards.” This is the first thing. Content owners generally approve what their partners use to distribute their contents. The second is that the content companies own the usage models because that’s their product, so they defined how their content is used.127

Toru Maruhashi at Fujitsu admits this increasing influence of content owners in the online world. Maruhashi states that “[f]rom infrastructure providers, content holders to content providers, there is no incentive whatsoever to consider the freedom [of the users].”128

It is not only online distribution services where the influence of right-holders increases. The development of devices is not independent from such growing influence. Answering the question of whose convenience is considered in determining the specifications of DRM technologies installed into devices, Toru Maruhashi at Fujitsu says:

Our company wants to take various people into consideration, but when one talks with the people who are accomplishing technological development, they begin from the idea of having the content providers purchase their technologies. While, in the end, they think about matters such as ‘how many times check-out can be performed’ [from the users’ point of view]. But they first consider how to appeal to the people who

127 Id.
128 Interview with Toru Maruhashi, Fujitsu, in Tokyo, Japan (Nov. 22, 2002).
deliver content to them.\textsuperscript{129}

The same tendency can be observed in the DRM technology providers. As Jeffery Lawrence at Intel says:

If you talk with DRM solution providers, they just provide the technologies to the content providers to allow them to offer whatever they want, because they are not in the policy call; that’s not their business. That’s true for all the DRM stuff.

Now we are starting the high definition tools. [Many players in the market] need content for that. That is why you probably hear more people paying more attention to the content providers. And I don’t know how to change that, except that you come up with a good technology and get some bargaining power.\textsuperscript{130}

4.3.3 Mindset of Right Holders

If the influence of the content owners is growing, and if they legally have the final word for the actual usage terms implemented in the system, the question worth studying is the mindset of content owners: i.e., how strictly content owners want the DRM technologies to be implemented?

In the following, this research points out five characteristics of the content owners’ mindset as well as their obligations as commercial entities.

4.3.3.1 Fear of the Online World

The first to point out is the fear content holders have toward digital and network

\textsuperscript{129} Id.

\textsuperscript{130} Interview with Jeffery Lawrence, Attorney, Intel, in Hillsboro, OR. (Aug. 14, 2003).
technologies. As Bruce Polichar explains, content owners have almost always been somewhat afraid of the new technologies.

In the case of the entertainment industry, every single period of growth in the industry has been driven by technological innovations. This has been true for about 100 years. Think about it: the motion picture camera, film projection, color and sound in film, television broadcasting, long playing phonograph records, digital audio, video cassettes, etc. All have represented growth of the entertainment economy and all are based on new technologies at the time.

However, in every period of technological innovation, the media companies have been suspicious and fearful of the new technologies and the people who are offering them. They are worried that these technology providers will own the solution and develop control over the entertainment companies’ business by owning the technologies critical to growth of the industry.131

Recent technological changes brought by digital and network technologies are not exceptions: the fear of content holders toward digital network technologies was outstanding. This fear is very well represented in the U.S. by efforts to generate new copyright legislation, and the spate of lawsuits in the recent RIAA and MPAA campaigns.132

131 E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 6, 2003, 09:45:24 PST) (on file with author).
Because the dominant fear is that their content may be widely distributed in a
digital form over the network, especially peer-to-peer (P2P) file-sharing networks, the
main target of their concern is the digital output of devices. As one executive from a
major media company and motion picture studio in the U.S. describes this point:

There are some relatively simple initial licensing decisions that we can
make. If somebody came to us with a device that allows someone to
purchase a video online and download it to a device that has no outputs,
it would be relatively easy for us to get into business conversations,
because … it is clear that no copies will be made from the device.

If there is an analog output, it’s a little more difficult, because a
consumer could now copy to, say a VCR, and then to other devices that
have analog or digital outputs. But the copy would not be the highest
quality and even this is not that far outside the reasonable environment
that we have been in.

However, once a device has a digital output, we are in a different
environment because the digital output allows a perfect copy to be
made…. We are not happy if there’s a digital output without any
restriction, because once the content is out, it’s available to be recopied
without any restrictions by anyone….

Many people would agree that there are many situations in which
making one copy for personal use is reasonable, especially in situations
where you have paid for the original content. The question is where you
draw the line on additional copies or sharing of copies with other people,
and here it’s much harder to come up with a consensus.¹³³

---

¹³³ Interview with two executives from a major media company and motion picture studio, in Burbank,
Cal. (Oct. 6, 2003)
In Japan, things are no different. Izumi Fukuda, General Manager of the Business Planning Department of Tresola Corporation that was established for distributing TV program online,\(^{134}\) and employed at TV Asahi, one of Japan’s major TV stations, says that it was because of the content owners’ fears that they employed the DRM system in a very strict manner in their test webcasts in late 2002 and early 2004.

The right-holders believe that if something appears on the Net, it will be ripped. That is why we provided them with rock-solid security … in order to gain their trust…. There are some companies in the Net business who don't want to implement security because of its high cost. However, since things have become digital, the DRM aspect has become important, and it is a major premise that this is being implemented properly.\(^{135}\)

4.3.3.2 Is DRM-based Security the First Priority for Content Owners?

If content owners fear digital output, the natural consequence is to limit any digital copying or digital transfer from the devices. It was not surprising, therefore, that, especially in its infancy, the implementers of DRM technologies tried to avoid flexibility such as allowing copying or transferring content.

In order to express their concerns toward digital copies, content owners repeatedly

\(^{134}\) Tresola is a company funded by three major TV stations in order to exploit business opportunities in the Internet market. It conducted two series of tests for distributing TV program over broadband in 2002-3. After the tests, they announced that they would postpone the launch of the service, without any clear schedule for the future. For details about Tresola, see, infra Section 6.2.2.

\(^{135}\) Interview with Izumi Fukuda, General Manager, Tresola Corporation, in Tokyo, Japan (Feb. 6, 2005).
say, in the course of development of new devices, new business models, or new technological standards, that security is their priority. As an executive from a major media company and motion picture studio maintains:

One area where protection technologies haven’t been effective yet is in the DVD space. The industry deployed security technologies when they first set the standards, but some measures have been less than ideally effective. But now DVD manufacturers don’t have a lot of motivation to go back and fix that, because the margins on DVD players have become so low (now the price is $39.99 at Best Buy). They may not want to spend an extra ten cents per unit, figuratively, to make it more secure. And even if they are willing to spend the money, we still have the legacy problem of how to change the technology in a way that the next generation doesn’t disenfranchise the installed-based hardware of consumers.

So, now we are in this inflection point where the most efficient place we can do something effective is in next-generation media. Because we have to deal with the same manufacturers about high definition DVD, we have to move the DRM piece to be near the top of the list and say, “if we want to have even higher quality movies on this new platform, we need to make DRM a very high priority,” although we don’t know fully how we are going to implement it yet. The system has to have effective ways of exercising usage rules.

In practice, however, it is sometimes difficult to implement DRM-based protection with complete security because of the business costs. As Izumi Fukuda at Tresola, which invested a huge amount of money for a DRM-based player, explains his dilemma:

---

136 *Id.*
In order to ease the anxieties of the right-holders, we put a lot of effort into our explanations to obtain their consent, and also put a large effort into DRM, because it was necessary to allay their anxieties by showing them protection.... If these had to be considered unavoidable as necessary expenses, and if [running the business] didn’t pay under such expenses, then it means we would have no market.\textsuperscript{137}

In reality, Tresola decided to postpone their business because they found that it would not be profitable enough, given the high expenses of distributing DRM players and providing customer support.\textsuperscript{138}

There is, however, an objection to security being the first priority when thinking of DRM implementation. According to Gabe Zichermann, Vice President of Strategy and Communications at Trymedia Systems, a game distribution company using peer-to-peer network\textsuperscript{139} disagrees that the issue of security is important when pursuing an online distribution business.

There is a common misperception about DRM. DRM is not strictly about security. Making that mistake, and it will not work. The purpose of DRM is for the following three things, in this order. No 1: make it as easy as possible for consumers to buy the product in question. No 2: give consumers fair and reasonable use rights to the product that you are selling them. No 3: protect it. And this is the common error: that you

\begin{quote}
\textsuperscript{137} Interview with Izumi Fukuda, General Manager, Tresola Corporation, in Tokyo, Japan (Feb. 6, 2005).


\end{quote}
reverse the order of these things in most DRM architectures. And what you do is you make the consumers angry, and what they do is they make you and the press angry….\textsuperscript{140}

Trymedia acknowledges, after a survey on their customers’ behaviors on copying game software, that there are customers who copy their products and exchange them with friends.\textsuperscript{141} Still, Zichermann thinks that lightweight and user-friendly DRM is better for their overall business, as explained in the next Section.

4.3.3.3 Content Owners’ Duty and Incentive to Maximize Profit

Of course, it is the content owners’ duty to their shareholders to maximize profit. To be able to do this, right-holders often claim that they have to manage every use of the content to make sure they get a proper monetary return from such uses. As Jeffery Lawrence at Intel puts it:

\begin{quote}
\end{quote}

\begin{quote}
\end{quote}

The result of the survey is the following.

- 15% of consumers admit to copying retail games in the past 6 months.
- 66% asserted their right to make backup copies of games.
- 64% said that illegal copying hurt game developers.

Each admitted copier buys an average of 7 games per year and makes 17 copies. 35 copies are made per 100 units sold on average.

The top three reasons why people make copies:

1. Personal backup
2. To share with friends
3. To use them on multiple computers (such as desktop and laptop)

The top reasons consumers share games are:

1. To play multiplayer games with their friends
2. Their friends asked them to
3. They thought their friends would like the game

Consumers felt that their friends were honest people and that sharing could result in their friend buying his own copy about 50% of the time.
One true point is that, if they could, the content providers would try to extract as much value as they could from the consumers. So we have to make sure that the market works, and that they are always under some pressure to consider consumer preferences.142

Also, Bob Ohlweiler describes the reactions of recording companies when they struggled to start their online music store. Negotiations with recording companies were difficult even after the success of the iTunes Music Store.

Record labels originally did not want the other services to take the Apple model. They felt that Apple model was too liberal, and for one dollar the consumers should not be allowed to make copies for the entire life…. I spent my entire summer in New York to negotiate with the music labels. We ended up with pretty liberal rules.143

However, there are some disagreements as to how much control is “better to maximize their profits.” Gabe Zichermann says:

I think the recording industry and the motion picture industry need to step back and say, do I want to antagonize my customers, or do I want to sell products to my customers. Answer that first question. So, start by saying I want to sell products to my customers.

Two, say “do I believe that my customers have the right to use content in certain ways?” which is another important area.144

Then Zichermann describes responses of right-holders at a game developers’ conference.

[E]very single one that you talked to [at the game conference], and you say, “you know, consumers should be able to make back-up copies of

143 Telephone Interview with Bob Ohlweiler, Senior Vice President, Musicmatch (Nov. 19, 2003).
the games, right?” and they go “Absolutely.” “Consumers should be able to share copies with their friends and that results in revenues to you, right?” “Absolutely.”145

As a proof, Zichermann explains that his game distribution business uses P2P technologies and has many customers who make some copies but is still making a profit.

So last week,146 we announced the first coherent unified solution of digital rights on games and software that allows game and software publishers to protect the content with the same technique on discs and downloads. Consumers may now back up their game and software content that they buy on CD media, they may make copies, copies that are made on trial mode and may be passed along, with full track ability…. The reaction was phenomenal. Everybody in the game business gets it….147

Therefore, according to Zichermann, the obligation to shareholders to run the business profitably does not necessarily mean having DRM technologies implemented in a very strict manner.

In sum, the flexibility of usage rules in the course of DRM implementation seems to depend upon, at least to some extent, the right-holders’ recognition of what the “profitable” business models are, of consumer acceptance and satisfaction, or acknowledgements of users’ freedom or “rights” in using their works.

145 Id.
4.3.3.4 Licenses Are Difficult to Revise

The preference for strict DRM implementation by right-holders appears not only when one tries to start a new business model. It also impacts when service providers try to change business models in favor of users. For example, this kind of struggle can be found in the case of i-mode mobile content distribution business by NTT Docomo.

Nobuyuki Watanabe, a technology expert at NTT Docomo responsible for deciding the technological specifications of mobile handsets for the i-mode business, says that negotiations with content owners was relatively easy when they first started the i-mode business.

In the i-mode service, [every content] is from ¥100 to ¥300 per month. With mobile handsets, a system has been launched so that downloaded content as a general rule cannot be sent out. [Such a system] made it possible to negotiate [to have content licensed] at extremely low royalties.\(^\text{148}\)

Watanabe then explains that this rule of “no copy allowed” restricts the technology design of the newer handsets.

With camera phones, … since the copyright for photographs taken by the user basically belongs to the user himself, an external memory is provided. However, the form is such that downloaded content (including content forwarded from friends) cannot be stored into the external memory. Only photographs taken by the user himself can be stored in it. Also with the infrared communications of 504, the system is

\(^{148}\) Interview with Nobuyuki Watanabe, NTT Docomo, in Tokyo, Japan (Dec. 11, 2002).
designed so that all content downloaded from the Net can’t be stored [in the external memory]….The basic elements of these standards are from the i-mode Business Division, and were determined so as to satisfy the needs of protecting content providers.149

After describing the current system, Watanabe expresses the difficulty of revising their license terms with content owners, once agreements are made. This is not unique to copyright licenses. However, this difficulty is becoming a large concern for NTT Docomo, as the size of downloadable content becomes larger. Watanabe elaborates:

Currently, when switching to a new mobile handset for reasons such as breakage or a model change, telephone listings can be transferred, but Java game applications or other copyrighted content cannot be transferred [to the new handset]. The basic position is to have the buyer repurchase [the content]. However, there has been a desire to be able to move [the content], since the content [size] is large, and the call charges [for downloading] would be by no means negligible. In particular, there has been a strong request from service departments which handle customer needs.150

However, the request has not been accepted because of the reluctance to change the terms of content licenses.

The i-mode Business Division is somewhat backward looking, because they believe that the basis of the business is for the content provider to have peace of mind…. The difficult thing is that allowing content to be transferred has no merit as far as content providers are concerned. They can see the risk aspect and therefore can't give their consent. From the technical aspect, it may be possible to transfer [content] to an external memory or PC somewhat securely by providing encryption and

149 Id.
150 Id.
decryption keys, but the content providers have not given their OK.\textsuperscript{151}

Without a legal requirement or some other incentive to convince content owners to think otherwise, it may be difficult to persuade them to alter their favorable license terms in order to accommodate the user freedoms recognized in copyright law.

4.3.3.5 Desire, Need, or Right to Protect the “Brand” of Works

Another aspect of right-holders’ reluctance to employ “freedom-friendly” DRM implementation is their desire to protect the “brand image” or their copyrighted works, especially when they are well-known or established. In answer to the question of why they are not willing to let users modify their works as a part of fair use, an executive from a major media company and motion picture studio explained:

[T]he most fundamental problem of consumer editing is that, they may republish and sell our content or offer it in damaging ways. We actually license the products to consumers from which they can copy and print our characters on invitation cards. But it would be very damaging for us if somebody creates a version containing pornography. I don’t think the law requires that people should be allowed to do such things.\textsuperscript{152}

This question of maintaining the “brand image” of copyrighted works becomes crucial, especially with regard to cartoon characters or other copyrighted works that can also serve as trademarks. For example, Disney has registered Mickey Mouse and

\textsuperscript{151} \textit{Id.}
\textsuperscript{152} Interview with two executives from a major media company and motion picture studio, in Burbank, Cal. (Oct. 6, 2003)
other cartoon characters as trademarks, both in the U.S. and Japan.\textsuperscript{153} Although the question of protection in the intertwining area of copyright and trademark (or unfair competition) is beyond the scope of this research, it is worthwhile mentioning, as a reality of the market, that right-holders’ desire or need to protect copyrighted works under trademark law (especially after the copyright has expired) is another large factor preventing flexible DRM implementation.

This issue becomes more problematic in Japan, as the desire to keep the “brand image” of their works is legally protected as one of the moral rights.\textsuperscript{154} In Japan, copyright holders and performers have a “right to maintain the integrity of the work.”\textsuperscript{155} A great deal of attention has recently been called to this problem in Japan, and the government has started a working group to study a possible reduction in the

\textsuperscript{153} See, e.g., U.S. Federal Trademark registration No. 75-311898 (Figure 1), JP Trademark registration No. 226416 (Figure 2), and JP Trademark registration No. 982917 (Figure 3).

\textsuperscript{154} In addition, moral rights complicate the problem of the anticommons, as moral rights are not assignable in Japan, thus increasing the number of right-holders when copyrights are assigned.

\textsuperscript{155} Article 20 for copyright owners, and Article 90 \textit{ter} for performers.
scope of moral rights.156

4.3.4 The Problem of the Anticommons that Right Holders Face

One of the reasons DRM technologies tend to have restricted usage rules that override the freedom within the copyright regime surely has to be the mindset of right-holders. And one of the ironies here is that, in some cases, right-holders themselves suffer from the tragedy of the anticommons, or the underuse of copyrighted information because of the multiple right-holders in a piece of content157 regarding the copyrighted works that they have rights to.

Music and motion pictures in particular have many right-holders involved in one piece of content. Works of music have right-holders to melodies, lyrics, performance, and sound recordings. Motion picture right-holders include the authors of the original story and screenplay, directors, performers, other art designers, the people involved in the music included in the film. Therefore, right-holders such as record labels and

---

156 In January 2005, the Copyright Council pointed out the necessity of theoretical and systematic research regarding the moral rights of authors, which should be entrusted to an external group consisting of specialists on the issue. See, 文化審議会著作権分科会「著作権法に関する今後の検討課題」[Copyright Council, Current Issues Regarding Copyright Law] at footnote 1, http://www.mext.go.jp/b_menu/shingi/bunka/toushin/05012501/002.htm, (last visited April 25, 2006).

motion picture studios often are unable to offer flexible licensing terms because they do not hold all the rights.

For example, an executive from a major media company and motion picture studio says:

There are other rights holders in our movies, and we don’t have a right to say that consumers can take out music that we have been licensed from someone else … and include them in other works, for example.158

4.3.5 Voice and Power of Users of Copyrighted Works

In order for the market to solve the problem of DRM implementation too often favoring right-holders, the users of copyrighted works have to have some voice and power in the market to reflect their needs. This section analyzes what mechanisms exist for users to reflect their voice, and how powerful their voice can be.

4.3.5.1 Users Can Speak Through Money, but Not Efficiently

Of course, the simplest answer is that users can express themselves as consumers in the market. Intel’s Jeffery Lawrence explains:

At the end of the day, the market decides (the right balance between copyright holders and users)…. People won’t buy stuff they don’t like….159

Bruce Polichar agrees that users speak for themselves.

---

158 Interview with two executives from a major media company and motion picture studio, in Burbank, Cal. (Oct. 6, 2003)
The customer speaks with only one voice: MONEY! When the customer sees something it likes, it says so by spending money to get it. That is the only message the CE or PC or new services industries can rely on. Very few people will guess correctly what the right offering is before they try it... Customers don't ask anyone to look out for them. They just ask to be entertained. Whoever entertains them gets their money.\textsuperscript{160}

It is true that ultimately users speak as consumers in the market. For example, this has been somewhat true in the world of digital music distribution. The development of more flexible usage terms were pushed by consumer rejection of earlier and stricter usage rules, as well as by their clear preference for the flexibility manifested in P2P file-sharing networks.

Jeffery Lawrence points out:

In the case of music, content providers realize that you have to give a lot of flexibility to make them reach out for their content. People will steal it if you cannot make copies. They are learning in a hard way. The negotiations with the music companies have been very hard for us, because they want to hold back and have complete restraint. The truth is, it is not acceptable in the market place. And if you are a device manufacturer, you don’t want to invest a lot of money on technologies that you know consumers would reject. And so we have to negotiate with the content community to find a middle ground.\textsuperscript{161}

Kevin Saul, Director of Trademark, Copyright, & Corporation Marketing at the Legal Department of Apple Computer, Inc., pictures the episode of developing the

\textsuperscript{160} E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 11, 2003, 21:17:41 PST)(on file with author).

\textsuperscript{161} Interview with Jeffery Lawrence, Attorney, Intel, in Hillsboro, OR. (Aug. 14, 2003).
iTunes Music Store as follows:

There was not a true popular music store before us. Some of the services were very restrictive. In practice, music companies are losing single sales and also CD sales year over year, and all of what I call “futile” attempts by the music business to protect their CDs are essentially competing with free. We wanted to provide a legitimate alternative. Apple is known for its user friendliness…. We spent a lot of time thinking about how we can navigate the center....

So we went into negotiations with major labels. We have to keep honest people honest. There are so many hackers out there, and our thought was that if we took the position of trying to absolutely prevent hacking of any usage rules or DRM, it would significantly impact the customers’ acceptance of the music store, and they would flock to the free services.\(^\text{162}\)

The result of Apple’s “experiment” was a great hit. It could be argued that such “success” was partly led by market mechanisms, especially by users sending signals that they did not like the old services with strict rules and that they preferred much more flexible usage terms.

Chris Parkerson, DRM Evangelist at RSA Security, which provides DRM technologies to game consoles as part of their business, also recognizes the point:

Ultimately, no one is going to sell anything if there are not providing services that consumers want, and they aren’t [now].... There is always going to be a need, of course, for Hollywood and whomever to make sure that they are going to get paid and they are going to get their revenues, but nothing is ever going to be restrictive to the point that it

\(^{162}\) Interview with Kevin Saul, Director, Apple Computer Inc., in Cupertino, Cal. (Nov. 20, 2003).
starts interfering with what consumers want, because what we will end up having is that consumers just won’t buy it.

So, the weight is always going to hold with the consumers. I think we are still in very early stages; we’re really just trying to figure out exactly what it looks like.\(^\text{163}\)

However, the voice of consumers through money is not perfect, either. Although the purchasing practices of users in the market surely affect the direction of DRM developments, it sometimes takes a long time, a great deal of investments, and, in some cases, even illegal damage to both parties before the market reaches a better balance. This is because, in the market, users only have a choice “to buy or not to buy.” Money of users is not sufficient because it does not tell the content owners, service providers, or device makers what else users want or how they want the devices and services to be changed.

\section*{4.3.5.2 Users Speak Through Technology Companies}

Therefore, to avoid unnecessary cost and pain, it would be better for both the users and suppliers of the market to have some mechanisms to represent the concrete needs of users in the course of DRM development and implementation.

Michael Miron, CEO of ContentGuard, maintains that it would be “nice, and

\(^{163}\) Interview with Chris Parkerson, DRM Evangelist, RSA Security, in L.A., Cal. (Mar. 31, 2005).
maybe even desirable,”164 to have consumers represented in the venues of DRM development and implementation, although not necessary because “[t]hey vote with their wallets and with their feet.”165

It is easy to imagine that such a reflection of users’ voices is more difficult than suppliers’ voices because of the transaction cost. It is usually costly, and thus more difficult, to summarize the voices of users as a class in the market, which is already known in many fields such as product liability cases or environmental pollution or other nuisance cases, just to mention a few. In these cases, one approach to solving the problem is to use an agent. It is helpful to have an agent that understands the desire of the class properly and acts accordingly.

In the history of copyright regulation, it is often believed or hoped that the technology industries, such as the PC industry, the CE industry, and the technology providers, act as one of the agents of the users.166 Is this mechanism still valid under the issue of DRM implementation?

Technology industries have a strong incentive to know users’ preferences through

165 Id.
166 In the U.S., libraries have been another “agent” that has spoken for copyright users. However, because this chapter deals with the DRM implementation process, and because librarians are often not heavily involved in technology discussions, this research does not explore the role of librarians.
their response to products in the market. Some key players in the technology industry describe their attempts to reflect the preferences of users in the market. Jeffery Lawrence at Intel describes users’ needs and desires:

People always want to make recordings. And from our perspective, content protection and DRM is not about limiting copying. In fact, the DRM should be all about enabling copying and enabling consumer use. The truth is: the thing that makes people buy products or consume contents is the ability to do things with the contents. They like to make copies. That is what they want. So what DRM should do is to create a protected environment [to do so]. You cannot put it onto the Internet to give it away to the world, but you can do things you want in your own personal environment. From our perspective, if I make a hundred million copies but all protected so that other people cannot use them, who would care? Why do content providers have to care about the fact that I move the contents to this device and that device as long as it is not put onto the Internet to be given away? In fact, they should like that, because that would make people buy more content….

In your home environment, [people expect that] you have substantial flexibility. Unless that actually happens, and consumers can do what they want to do, no DRM in the world would ever be effective, because consumers would reject it. If the consumers reject it, they will opt out for the illegitimate alternatives.167

Bob Ohlweiler at Musicmatch describes the preferences of music listeners as follows:

We know a lot about our consumers. Generally what they want is a library on multiple PCs, and many CDs without worrying about dipping into some quota for burning. And music labels want some limits on that. So Apple came up with this idea of “playlist.”

---

[We understand their preferences] through focus groups, customer services, and speaking with customers, and talking with people inside the companies who are also the consumers of our product.\(^{168}\)

Given their understanding of customer preferences, technology companies and service providers convey the preferences to some extent in negotiations with content owners. Yoshisuke Kuroda at Sony explains:

Speaking of management of content by DRM, there are some points without which you will not have a marketable product. For such points, we propose them to the content side. We communicate with them, telling them that, if that doesn't happen, ultimately, DRM itself will not work and products won't sell. When the rules of DRM are specifically determined, the device manufacturers will basically state their opinions from the users’ side. Then, finally, decisions will be made based on negotiations with the content holders.\(^{169}\)

Of course, this is not an easy process, especially in the DRM implementation. Kuroda describes the difficulties he faces:

The position from the content side desiring to protect security is completely at odds with usability. We are stuck between the two sides and must make the adjustments. That is the hardest part.\(^{170}\)

Jeffery Lawrence admits that the influence of the copyright owners is growing in the area of DRM and that device manufacturers have more bargaining power than service providers do when negotiating with copyright holders.

[H]ere is the dynamic of [how we keep the balance in DRM systems]. We need content and to make it friendly for our customers. Content

\(^{168}\) Telephone Interview with Bob Ohlweiler, Senior Vice President, Musicmatch (Nov. 19, 2003).

\(^{169}\) Interview with Yoshisuke Kuroda, General Manager, Sony, in Tokyo, Japan (Dec. 17, 2002).

\(^{170}\) Id.
owners need content protection. Nobody wants to pay for content protection, but we need that to support a legitimate business model. And none of us want the government to come in and arbitrate what the rules should be.…

DRM solution companies and other Internet content service providers have to get content straight from the content providers. They don’t have leverage over content providers at all. They have to do whatever content providers want. In fact, that is the great beauty of DRM, because that would give content providers great flexibility, whether to offer to see it once, twice, or for a day. The only problem is, the DRM cannot reach everywhere in the home. DRM is only one piece of the technology. It has to have clients anywhere, otherwise it cannot go there.

Then there is other group of people who build devices. And device manufacturers have some leverage over content providers, because they have a variety of ways to get content. They can get content from TV, packages, the Internet; they can even have illegal [and unprotected] content. So, they are less dependent. And content providers need devices to see the content, and they need protection there. So, there is a room for content providers [to make compromises].

However, Lawrence also makes clear that there are limits in what they can get from negotiations with content owners.

We are trying to make sure we are engaged in the discussion, and the only leverage you have is to bring your technologies and find solutions to their problem that are reasonable. It’s a negotiation to get the minimum [of freedom].

That’s how we set the floor, i.e., set the minimum standards. That is the best we can do. We don’t have more leverage with the content providers. And we see what they offer. We cannot make them offer different

---

products….\textsuperscript{172}

Lawrence also makes clear that the fair use doctrine or other statutory exemptions are not necessarily the guiding principle of negotiations when they try to get flexibility in DRM implementation.

Fair use is great, but it is really a narrow exception. In practice, as a product maker, I am not interested in fair use. I want more than fair use. I don’t think people would buy a DVD to snip a small piece of the DVD and write a book report. That is not why people buy devices. I want more. That is where the technology community will get together and negotiate with the content community to have a deal. That should be done through business deals. The content community is coming to understand that they have to meet consumer expectations.\textsuperscript{173}

Lawrence says that in areas with established customs, it is easier to negotiate.

The only place we have public policy is the area that people are used to already. Cable TV and packaged media, these have been out there for some time now, and people have expectations of devices and media, [so DRM should meet these expectations].\textsuperscript{174}

Lawrence uses an example of usage rules in Digital Transmission Content Protection (DTCP), which is a cryptographic protocol to protect audio/video content while allowing the content to travel over the Internet.\textsuperscript{175}

In terms of DTCP, the primary use is to help you distribute TV and cable content. But the condition there is that, if the content is free cable TV, people can make as many copies as they want. If it is premium

\textsuperscript{172} Id.
\textsuperscript{173} Id.
\textsuperscript{174} Id.
cable, like HBO, people can still make copies, maybe not millions of them, but still can in archive as well. The only area that you cannot copy is the PPV. This was the deal made with content communities. Content providers gave up these rights to have protection technologies for them.\(^\text{176}\)

However, such a “policy call” does not exist where people try to establish a new business model. Lawrence maintains,

> But there are many new areas, and that’s where the all real business is going to be. Who decides the rules there? I don’t think that’s the role of the government. It is basically the role of content providers. But we can negotiate with them because they need us.\(^\text{177}\)

For such new areas of business, there is no other means but to negotiate using repeated trial and error in order to reach a comfortable solution. This process needs much more effort than is usually claimed in order to get a well-balanced DRM implementation. It is not an easy process, as every industry has its own goals and interests. As Bruce Polichar states,

> In some ways it is unavoidable that each industry pursues its own business. There is more dialog between these industries than there used to be. But it will never be a real partnership where they all collaborate to build new markets. Each part of the triangle still wants to maximize its own position.\(^\text{178}\)

However, people always learn lessons, and things are still getting better. As Chris Parkerson states,

\(^{176}\) Interview with Jeffery Lawrence, Attorney, Intel, in Hillsboro, OR. (Aug. 14, 2003).
\(^{177}\) Id.
\(^{178}\) E-mail from Bruce Polichar, Former Vice President, IBM, to the author (Nov. 10, 2003, 09:34:26 PST)(on file with author).
It is getting better…. I think [the success of iTunes] was really what has got a change, and the content owners are starting to get a little bit more engaged…. [but] the fact that they have been taking a more active role … in defining “what do you need to facilitate your business” has been rather a set back. I think it’s because there’s still an animosity on the content owners’ side toward new technologies, toward technology companies. I think they are getting better. [However,] I think we would be in a slightly different world right now, if content owners had been a lot more active in defining the rules of these digital contents.\textsuperscript{179}

In sum, in order to reflect users’ voices in the early stages of service and device design, technology companies make some efforts in negotiations with content holders. However, both the understanding and power of technology companies are sometimes rather limited to reflect the sincere voices of the users in the course of DRM implementation. Therefore, in new services or business models where customs are not yet established, technology companies can gain only the “minimum” freedom when copyright owners are unwilling to give it, given the difference in legal standings. Many efforts are made in the market, but it is still a very slow move. Also, it is questionable whether DRM implementation completely reflects the freedom implemented in the traditional copyright regime, as players in the market do not fully respect the rules in the law as their guiding principles.

\section*{4.4 Can the Market Really Solve the Problem of Override?}

\textsuperscript{179} Interview with Chris Parkerson, DRM Evangelist, RSA Security, in L.A. Cal. (Mar. 31, 2005).
Given the description of the players in the market above, it is now useful to ask this question: Can the market really solve the problem of strict DRM implementations overriding the freedom within the copyright regime? Or, more precisely, can the market bring DRM implementations that fully respect the freedom within the copyright regime?

As described above, some of the freedom is actually implemented given the pressure of the market. Online music stores now respect freedom or “users’ rights,” such as the freedom to make backup copies or freedom to give the content to a limited number of friends. It took several years and significant suffering in the music industry before they reached the current business model.\textsuperscript{180} Still, many people attribute this “success” to the market.

However, not every problem can be solved in this way, especially for issues which a limited number of people are involved in. For example, making backup copies is important, but it is still only one form of fair use or statutory exemption. There are many other exemptions to be taken care of. Even the iTunes Music Store does not allow exempted uses which include modification of works such as quotations. This may be because (1) the need to make quotations or re-mixing is much smaller or far

\textsuperscript{180} This is partly because of the transaction cost and the agency problem in the market.
less recognized by the market than the need to make backup copies; (2) some content owners have negative feelings toward modification, and in Japan, there is a moral right to maintain the integrity of works; (3) it is technologically much more challenging to protect the content while allowing modification compared to allowing simple copying; and (4) the value of such utilization of copyrighted works is a positive externality and thus will not be fully considered by the market.\footnote{See, Wendy Gordon, The 'Market Failure' and Intellectual Property: A Response To Professor Lunney, 82 B.U.L. Rev. 1031, 1033, Mark A. Lemley, Property, Intellectual Property, and Free Riding, 83 Tex. L. Rev. 1031, 1046-50, 1058-65 (2005).} Given these factors, it can be said that it is much more difficult for the market to make DRM implementation include exemptions with modifications.

Another difficulty in solving the problem through the market is caused by the highly technological aspect of DRM technologies. Content owners, who have the final word in deciding the use of content (which in many cases determines the design of services and devices), are still slow in fully understanding the technologies. Therefore, they may not completely understand the limitations of DRM technologies, or may not understand the best use of them. The highly technological aspect also makes it difficult for end-users of content to feed back their voices into the market, as they may not fully understand what technologies are doing in their devices, and they may not be able to
provide sufficient proposals to solve the problems they encounter.

In addition, as has been repeatedly pointed out, differences in legal standings between right-holders and content users\textsuperscript{182} creates a difference of bargaining power in the negotiations, and makes the content rules heavily dependent on right-holders. Under such circumstances, it is very hard to implement fair use and other copyright exemptions.

Therefore, it seems that some part of the override problem may not be able to be solved through the market, at least in the short run. In some areas, the market process is in a vicious circle: DRM implementation is very strict; which causes less consumer acceptance in the market and more illegal conduct by consumers; which creates the fear and defensive attitude of content holders; which may lead to a stronger desire for stricter usage rules of content. In order to improve the situation, Section 5 below explores some choices of what law can do to keep a better balance of interest between copyright owners and users in DRM implementations.


As explained above, this section explores some legal options to help keep a better balance of interest between copyright owners and users in DRM implementations.

\textsuperscript{182} See, supra Section 4.2.
balance of interests between right-holders and content users within the field of DRM technologies. 183

The following first explores the possibility of repealing the current anti-circumvention regulations under certain conditions (5.1). It then explores some legislative options under the basic frame of anti-circumvention regulations to help reserving freedoms within the copyright regime (5.2). There are also brief discussions about the possibility of “freedom enabled by DRM technologies.”

5.1 Choice (1): Repeal Legal Protection for DRM Technologies when Creating Problems

If some of the DRM implementation diminishes the freedom within the copyright regime, and if anti-circumvention regulations fix the problem by blindly protecting these problematic DRM technologies in the market, one legislative option to help reduce such problems is to repeal the legislation when fixing the problem.

One idea would be to legally protect DRM implementations only when they are

183 Although law can impact the market by in both legislative phase and enforcement phases, the following focuses on the legislative side of the argument. Legislative choices (as well as case law s in the U.S.) primarily set the line between legal and illegal actions. However, in reality, as often pointed out, enforcement policy has a large impact on the actual policy of how free copyright usage is. In fact, one of the problems of DRM technologies is their capacity to enforce the rules privately and thoroughly, which has never been the case in the analog world. See, Lessig, supra note 94 at 127-30 (Minneapolis: Sagebrush Education Resources 1999) See, also, infra note 212 about self-help. However, it will require substantial research to discuss how thorough the enforcement should be and related topics (e.g., privacy issues) and is outside of the scope of this article.
well-balanced with regard to the interests of rights holders and users. In other words, legislators can use anti-circumvention regulations as a tool to create incentives for better-balanced DRM implementations.

Under this scheme, the challenge arises in the problem of drawing a clear line between well-balanced DRM implementations worth protecting and unbalanced implementations not worth protecting. If the line is ambiguous, there will be confusion and chilling effects in the market, which may make regulations very costly in a different sense. However, this problem of how to define a “well-balanced DRM implementation” is not unique to this proposal. Rather, it is a common challenge when legislators try to keep anti-circumvention regulations while also trying to minimize their negative effects.

For example, with regard to the freedom of copyright use based on exceptions, the problem of defining “well-balanced DRM implementations” has many similarities to the problem of creating proper and clear carve-outs within anti-circumvention regulations, as discussed below. If the exceptions or carve-outs for the freedom of copyright can be defined clearly enough to avoid confusion in the course of DRM

184 Suggested by Lawrence Lessig, in a meeting with the Author.
185 For the problems and challenges of setting up a proper exceptions and carve-outs, See, infra Section 5.2.2.2.2.
implementation, there would be no significant additional chilling effect of law that protects only DRM implementations that respect those exceptions and carve-outs.

Still, this legislative choice requires careful study for proper exceptions on the impact on technological research and development, because even a well-balanced DRM implementation may need to be circumvented for legitimate research purposes.

5.2 Choice (2): Try to Keep Balance Within the Anti-Circumvention Regulations

If legislators decide to maintain the main framework of the anti-circumvention regulations as it is now, the next question is to consider any possible means to minimize the negative impact caused by the maintained anti-circumvention regulations. The major legal means is to establish proper statutes of exceptions and carve-outs to the anti-circumvention regulations. In addition, stating some of the copyright exceptions (such as fair use) as an affirmative right instead of a defense may help the interests of copyright users to be better represented in the market of DRM implementations.

In the following, this article first explores the option of creating legal exemptions to give a right to hack when there is a legitimate need (5.2.1). Next, it gets into the
question of how to realize freedom without recognizing a right to hack, which means to respect the freedom within DRM schemes (5.2.2). As a premise to this discussion, this article first analyzes whether the freedom incorporated within the copyright regime can be embodied within DRM schemes (5.2.2.1). It suggests at the end that, barring a higher transaction cost for users, similar freedom could be materialized by combining systems based on computers and human institutions. Given such possibilities, this Section proceeds to describe three possible legal options to help realize balanced DRM systems (5.2.2.2).

5.2.1 A Right to Hack: Legal Exemption to Anti-circumvention Regulations

Although it sounds rather drastic, the idea of giving a right to hack is ready used in the current anti-circumvention regulations.\textsuperscript{186} Exemption statutes in both U.S. and Japanese anti-circumvention regulations allow people to hack DRM technologies or to provide circumvention devices under certain conditions. Therefore, giving a right to hack is an established way of minimizing the negative effect of anti-circumvention regulations. It is a means that can respond to the freedom to use copyrighted materials when allowed under traditional copyright regulations, as well as the freedom of research and development in the field of DRM technologies. In fact, the DMCA has

\textsuperscript{186} See, Bechtold, supra note 3 at 371-74.
exceptions that respond to both of these problems, although narrowly tailored.\textsuperscript{187}

The important question in this approach is the scope and the manner of the exemptions. One of the major criticisms of the DMCA is its narrowness, and the ambiguities and complexities of its statutory exemptions. For example, there is no clear reason why encryption research and other fields of research related to DRM technologies could be reasonably discriminated against in Section 1201 (g).\textsuperscript{188} In Japan, there is no distinction in the exempted area of research.\textsuperscript{189} An equally important issue is the manner of articulating exception rules, i.e., its clearness and simplicity. Complex and unclear manners of exceptions cause chilling effects and eliminate opportunities for legitimate content use and technological research and development.\textsuperscript{190} As the U.S. reviews the proper scope of exemptions to anti-circumvention regulations every four years, there is an opportunity in the future to correct such narrowness, complexities and ambiguities if the government wishes.

The good thing about the right-to-hack approach is the flexibility it provides the

\textsuperscript{187} For example, exemption for reverse engineering, encryption research and security testing are for technological innovation, and exemptions for libraries, archives and educational institutions and government activities are for freedom on content use. See, 17 U.S.C. §1201 (d)(e)(f)(g)(j).
\textsuperscript{189} See, supra Section 3.1.1.1 and 3.1.2.1.
\textsuperscript{190} See, supra Section 3.3.2.
beneficiaries. There is no restriction on how to circumvent the DRM technologies, as opposed to the freedom incorporated within DRM systems approach described below. The transaction costs for users to circumvent DRM systems, and for DRM providers to allow such circumvention, are both generally lower than to incorporate tools for freedom within DRM systems. Users do not need to go through the procedures to achieve freedom incorporated within DRM systems; they have only to look for circumvention tools when they think it is legitimate. On the DRM providers’ side, the costs are also lower, as they do not have to prepare a tool or procedure to allow user freedoms within their DRM systems. They just have to let users make their own decisions, and exercise their rights when they think it is proper. Therefore, this approach might be better than the system described below.

Again, some cultural differences in how comfortable people feel asserting their exceptions and how right-holders feel about trusting the general public may have some impact on the policy decision in this aspect. In any event, it is desirable for legislators to make exemption statutes clear to avoid misjudgment.

There are some downsides in giving a right to hack. Many right-holders are still

---

191 See, infra Section 5.2.2.
192 See, supra Section 3.1.1.2.
afraid of the risk of abuse by broadly authorizing the right to hack, and there should be considerable work to get over such fears. Also, for technologically non-savvy people, a right to hack is not very helpful without authorized circumvention tools. In order to solve this problem, the government could provide some exceptions in anti-device regulations to allow people an opportunity to use circumvention devices for legitimate purposes.

5.2.2 Support Freedom Incorporated within DRM Systems

Another legislative means is to legally support or encourage DRM implementations to be freedom-friendly without giving people an instant right to hack. In other words, under this approach, freedom would be enabled within the usage rules of DRM systems (coded freedom), or freedom would be granted after some procedures with an institution that authorizes circumvention (institutionalized freedom). Coded freedom and institutionalized freedom can be combined to enable a proper and cost-efficient design of freedom within a particular DRM system.

5.2.2.1 Freedom within DRM Systems?

193 For an insightful article proposing the possibility of a coded and an institutionalized approach, and its possible combination, see, Dan L. Burk and Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 Harv. J. L. & Tech 41 (2001). The following description in this article is to elaborate the suggestion made by Burk & Cohen. *See, also*, Bechtold, *supra* note 3 at 374-79 about Key Escrow.

194 See, Burk & Cohen, *Id.* at 65-70.
First, it is necessary to examine the possibility of including within the DRM system some of the freedom defined in the copyright law.

There are two possible ways to incorporate freedom into DRM systems: one is to program it into computer software (or, in some cases, hardware) (coded approach) and the other is via human intervention (institutionalized approach). The bottom line is that one can mimic some of the freedom set forth in the copyright law by combining a coded approach and an institutionalized approach. The following will briefly explain what coded and institutionalized approaches are, their differences, pros, and cons, and an example of how coded and institutionalized approaches can work together.

Because freedom via DRM systems inherently includes monitoring and judgments regarding the use of copyrighted works, this type of freedom-delivery system creates primary concerns about privacy issues. Although privacy issues are outside the scope of this research, it is worth noting that the system design should be privacy-sensitive, and that such privacy concerns can be mitigated to a certain extent by the structure of privacy-related data management.

---

195 See, Id.
196 Privacy concerns regarding the use of copyrighted works first arise when an entity starts to collect data about the subject and object of the use. However, such data collection may be necessary in order to
5.2.2.1.1 Coded Approach

Here, a coded approach is referred to as any kind of automated systems generated by computers and which realize a part of or all the requirements for the free uses of copyrighted works recognized within copyright law.197 Such freedom includes: fair use or other copyright statutory exceptions, freedom to use materials in the public domain, and any part of the requirements for such freedom that can be coded into a computer or a DRM system.

Michael Miron, the CEO of ContentGuard, Inc., thinks that some freedom can be situation-specifically coded:

[Y]ou can use, for example, the MPEG well to create a license grant to mimic fair use for particular domains. And they will be specific to particular types of implementations. An example would be to give a grant for all students registered at an academic institution for a particular time period during a semester, and for professors or librarians to grant certain distribution… rights to any student registered for the academic year. So you can mimic certain uses for academic institutions. But this could be domain specific....

enable transactions regarding copyrighted work, especially over the Internet. Even in such cases, however, privacy concerns can be reduced by avoiding aggregating data beyond what is necessary. This is because privacy concerns increase by relating different kinds of data to each other, especially together with data that allows the identification of people. For example, credit card information, name or other personal identification, and how the copyrighted work is used can all be maintained separately in independent databases, and connected to each other only through an anonymous number and processed separately by different people or departments. Therefore, in this research, the following discussion is based on the assumption that privacy concerns can be reduced to a tolerable level by the system design. For a theory of a system with data confidentiality, see, Adi Shamir, How to Share a Secret, 22 Communications of the ACM, 612 (1979).

197 See, for details of these freedoms, supra Section 5.1.4.1.1. See, also, Burk & Cohen, supra note 193 at 55-56.
The same is true for first sale, where a rights expression involving lending, transfer, and delegation can be created. There is a notion of meta-rights, or rights about rights. I have a right to grant or I have a right to revoke, and so I could construct certain license grants that delegate the right to do all the things, like you mimic first sale. Again, domain specific, and you have to strike a deal with content players for particular distribution models.\(^{198}\)

However, you cannot code every kind of freedom as is stated in law. Generally, coded approach is more suitable to materialize requirements that are defined in a rather specific manner. For example, personal noncommercial recording of TV programs for time-shifting is recognized as one form of fair use in the U.S.\(^{199}\) Article 30 of the Copyright Law of Japan also states that private copying within the home environment is exempt from copyright infringement. Therefore, if you wish, DRM implementers can code into their DRM systems a tool to allow users to make a copy for the purpose of such time-shifting or private copying. Such usage rules may include usage beyond the freedom authorized by copyright law, and thus partly be based on licenses. However, it is clear at the same time that part of it is to materialize the freedom or exemption authorized by copyright law.\(^{200}\)


\(^{200}\) One difficult question in programming the coded freedoms is suggested here: it is sometimes very difficult to draw a clear line between free uses and uses that require licenses. Therefore, under current situation where law does not clearly give carve-out statutes, it is not surprising that a system designer
In order to program certain requirements for freedom within the DRM system, system designers first have to define in rather specific detail what kind of freedom they want to allow within the system. Whether it is based on freedom within the copyright regime or on the license given by right-holders, such freedom or flexibility should be broken down to specific sets of usage rules, such as: Who can make how many copies of what material under what kinds of circumstances and for how long? The major problem here is that the freedom within the copyright law is not written in a manner that can be directly coded into DRM systems. Current statutes are too ambiguous and not well-enough defined in most cases. The fair-use principle in U.S. copyright law is the best example facing this difficulty.²⁰¹ There are a lot of categories of uses that are respected under the fair use doctrine, which can be different in each jurisdiction within the U.S., and which can be changed over time. It can even be hard for a human brain to categorize and specifically define every kind of fair use recognized under the law. It might be possible for computers to do so with a savvy artificial intelligence system; however, even if this were possible, it would be too expensive for mass-market consumer products to include such artificial intelligence in the short run. Therefore, it

²⁰¹ See, Burk & Cohen, supra note 193 at 55-6.
is generally thought very difficult to codify a general principle of fair use.\textsuperscript{202}

It would be relatively easier to code rather specific exemptions with particular requirements and settings. In this sense, Japanese copyright statutory exemptions have an advantage over the U.S. fair use doctrine. However, even Japanese exemptions are not designed to be programmed into DRM systems, and thus leave many uncertainties or ambiguities to be cleared in order to be implemented into DRM systems. Still, such clarification would require less work compared with more general principles such as fair use.

In addition, coded approach has its own limits. Building a computer system can be too costly, and computers are generally not good at identifying the purpose or context of use. Thus, it might be economically feasible to delegate some or all parts of the process to human intelligence, which this article refers to as the institutionalized approach below.

\subsection*{5.2.2.1.2 The Institutionalized Approach}

The institutionalized approach is defined here as a system that uses human judgment (along with some technological assistance, if necessary) to realize freedom
or part of its requirements. This approach to freedom is based on the idea that human judgment can supplement what is too difficult or costly for computers (i.e., the coded approach). A well-known example of this institutionalized freedom would be the key escrow approach that Burk and Cohen propose. They describe a system in which DRM providers would escrow decryption keys or circumvention devices in a trusted third-party organization so that people who want to make fair use can seek the DRM key online.203

The institutionalized approach can also be more limited in scope than is suggested by Burk and Cohen. For example, it can be used to authenticate only one rather than all of the requirements. The Copyright Law of Japan, for example, allows school textbook publishers and educational-television program-producers to use published materials with a fair amount of compensation.204 An institution can handle the authentication process of the beneficiaries of these copyright exceptions (e.g., authorized school-textbook publishers) to hand out circumvention devices to enable their permitted use, but the institution need not necessarily check the actual uses of the copyrighted materials. The review of whether such uses are within the scope of

203 See, Burk & Cohen, supra note 193 at 59-65. For a key escrow system, see, Id. at 63.
204 Articles 34 and 35 of the Copyright Law of Japan.
statutory limitation can be delegated to the normal court procedure, for example. Or, in a different system design, the coded approach might be used to authenticate the beneficiary, and the institutionalized approach for the review of use.

In the following section, this research will compare general differences between coded freedom and institutionalized freedom, and explore how these two can be combined to make copyright exceptions available under DRM and anti-circumvention regulations.

5.2.2.1.3 Choosing between the Coded and Institutionalized Approaches—An Example

When one combines both the coded approach and the institutionalized approach, many forms of copyright limitation can be materialized within the DRM system. Overall, it is true that more transaction costs would be placed on users compared to the analog world, as the de facto starting point is under the DRM control. Still, one can at least claim that it is better to have some system that opens up a legitimate way to secure freedom than none. Therefore, in the following, this article lists several issues to be considered when trying to design a system that enables freedom recognized in the

---

205 See, Burk & Cohen, supra note 193 at 59-60. They point out that such high transaction cost would reduce spontaneous uses that are often beneficial to the societies. Id. See, also, Bechtold, supra note 3 at 375.
copyright law.

Choosing between the coded approach using computers and the institutionalized approach using human powers, or deciding how to combine these two, can be done by comparing the efficiencies and costs of each approach.206

The first step in determining which approach to use is to break down the exemption rules into a set of relatively clear requirements. As previously stated, system designers would face great difficulties when they tried to break down the U.S. fair use principle into a set of clearer rules. More specific statutory exemptions, however, such as some of those in the Copyright Law of Japan, are relatively easier to analyze and program.

For example, Article 33 of the Copyright Law of Japan allows school textbook publishers to quote published works “to the extent deemed necessary for the purpose of school education,” along with a reasonable compensation, the amount of which is fixed by the Commissioner of the Agency for Cultural Affairs (a governmental body in charge of copyright regulation). This Article can be broken down to four requirements:

(i) the subject of the use should be publishers of textbooks authorized by the

---

206 In addition to the factors described below, there is another question of privacy or anonymity of uses, especially when one thinks of the institutionalized approach. See, Burk & Cohen, Id. at 60-1.
Ministry of Education and Science;

(ii) the object of the use should be works already made public;

(iii) the purpose and manner should be deemed necessary for school education;

and

(iv) the quoting publishers should pay the amount of compensation designated by the Commissioner of the Agency of Cultural Affairs.

The next step is to ask whether computers can process each of the requirements set forth in the above process. This is because, if a requirement is practically very difficult or too costly for computers to clear, there is no choice left for system designers but to leave the requirement to human institutions.

To elaborate more, computers are generally good at processing a large amount of data, if such data can be properly prepared and the rules of processing are properly programmed. However, computers have some limits on their capacities: they are usually not good at processing the purposes of uses that people have in their minds, or usage contexts that require complex judgments. Of the four requirements set forth in Article 33, for example, the purpose and manner of the use in requirement (iii) would be very costly or nearly impossible for computers to decide. Therefore, a reasonable
choice is to leave this part of requirement to some human institution.

On the other hand, other requirements under Article 33 can be processed by both computers and by human institutions. In such cases, the next question is which approach, coded or institutionalized, will cost less. There are two kinds of costs involved when the systems are designed: costs of regular processing and costs of irregular results. There are also two or three parties involved: system providers (and right-holders) and system users. The ideal choices should be the ones in which costs are affordable and preferably low for every party involved. However, in some cases, one choice would put more burden on one party while benefiting the other party more. In such a case, the choice is more of a policy question, which legislators have to decide.

The regular costs for running each system may include costs such as the following:

(a) Initial cost for building and installing the system. For example, authentication or validation of the qualified textbook publishers can be done by matching a user ID and the data of qualified publishers. The cost of handing out the user IDs and building the database of qualified publishers, and the cost of matching these two, should be calculated and compared between the computer-based process and the
human-based process.

(b) Running cost of the system: for the coded approach, the maintenance and update fee, and for the institutionalized approach, the labor cost of running and updating the institution.

(c) The cost related to system changes in the long run: flexibility of changes that could be made according to the possible change in rules in the future, or in order to make improvements in the system. For larger and more drastic changes, the computer system might cost more than in human institutions, which could respond by revising the working manuals and retraining the human resources.

(d) The cost on the user’s side: ease and clarity of the user interface or its process, availability of the system, and consistency or accuracy of rule application and judgment. Generally, if programmed properly with accurate data, computers are good at giving consistent and accurate application with more availability. However, the ease of use greatly depends upon the user interfaces, which varies between the systems. Also, the access cost may depend upon the system design: if access to a coded system is made easily available over the Internet, for example, it may be lower than access costs to human institutions, which often has time restraints as
well as stricter capacity restraints. However, if the coded system is poorly designed, again, the system would end up having a human-based customer-support system. In such a case, it may be less expensive in the end for both the users and the system to provide only the institutionalized system.

The next group of costs to be considered is the irregular cost, or risk, of running the system. For example, such costs may include issues such as:

(a) Risk of making errors when building the system: This can also be viewed as the flip side of costs in breaking down the statutory requirements into a programmable form. Thus, there would be a role for legislators or the government, as described below, to clearly state the requirements in a more programmable way to avoid this risk and cost.

(b) Risk of misapplying the system to each case: both humans and computers can be tricked by potential infringers; and the system can malfunction. In addition, human judgment is more vulnerable to bias than the binary judgments of computers.

(c) Cost of correcting the abovementioned errors.

Apart from how easily mistakes can be made, there is always a question of which party takes primary responsibility when talking about designing the type of system that
Burk and Cohen suggest.\textsuperscript{207} The players can be right-holders, users, or third parties. This question involves two issues. One is the problem of the potential bias of the system designer. This is more prominent in the institutionalized approach: however, the same problem exists for the coded approach. The other is the transaction costs of achieving exempted uses.

For example, if users have the primary responsibility in designing or using the system for exempted uses, there is always a risk of users biasing the system in their favor, which may result in infringement and damage to right-holders. However, such risk involves a trade-off regarding transaction costs. The transaction costs of getting an exemption borne by users are, in many cases, much lower compared to other system designs for which the primary decision makers are other parties and thus may require additional steps by users to seek decisions from those responsible for it. The \textit{right-to-hack} approach\textsuperscript{208} taken by the DMCA and Japanese anti-circumvention regulations can be viewed as an extreme example of a design in which users exercise the power of primary judgment, because they both allow users to create and use circumvention devices based on their own judgment.

\textsuperscript{207} See, Burk & Cohen, supra note 193 at 59.
\textsuperscript{208} See, supra Section 5.4.2.1.
On the other hand, there can be a system design in which the primary responsibility for making decisions within the system (such as rule design and application) rests with right-holders. In this case, the risk of infringement would be low. Rather, there is a risk that right-holders will disrespect the exempted freedoms of users. For example, the EU Copyright Directive of 2001 takes this approach in several cases, especially with content distribution in on-demand download services along with a contract. As Article 6 Section 4 Subsection 4 of the EU Copyright Directive makes clear, Member States cannot take any legislative means to secure copyright limitation when right-holders decide to take that particular business model.209 This means that the EU Copyright Directive leaves to right-holders the decision of whether they will provide a system that recognizes copyright limitations.

The least biased design is to give primary responsibility to a neutral third party. It could be an existing institution such as the courts, or it could be new organizations with simpler procedures and lower costs.210 Thus, freedom might be better secured while lowering the risk of infringement. However, this could be the choice with higher

210 Such third-party organizations are suggested by several scholars. See, Burk & Cohen, supra note 193 at 61-65, Bechtold, supra note 3 at 375.
transaction costs for both users and right-holders, because both must be involved in some process to deal with the parties making decisions. These costs can be lowered to a certain extent, and should be made as low as possible, but they would not be zero. Also, the problem of how to finance the institution would become a more urgent issue than whom to delegate the decision to, right-holders or users.

Another issue to be considered in the course of system design is: when to make the screening and judgment of each requirement. Taking the example of the quotation again, there can be four phases to making judgments and screenings for each requirement. The first is before the decoding of applied DRM on the work to be quoted; the second is after the decoding and before the actual editing such as copying and pasting; the third is after the editing and before publishing; and the fourth is after the publication of the quoting works.

The earlier the filtering judgment, the safer right-holders may feel, because it minimizes the chance of abuse. However, it also means that, from the viewpoint of freedom and creativity, early filtering activities reduce the chance of experiment, learning, and innovation, and thus reduce their benefits. Again, the risk of infringement.

\[211\] See, Burk & Cohen, Id. at 61-62.
and the chance of new innovation involve many common processes, and the difference largely depends upon issues such as context, intention of the editors, and the manner of use or publication, which is sometimes difficult to decide before it is finally published.

Generally speaking, possible damage to right-holders is caused by publication and dissemination of the infringing works. Therefore, before the quoting works are published and disseminated, it might be better to do the filtering as late as possible in order to respect the possibilities for experimenting, learning, and innovating. There could be even a system design in which all the filtering and judgment were done at the very end, i.e., after publication, which has been the rule in the analog world.\(^{212}\)

If the system integrators opt for review after publication, such ex ante review could possibly be done using a coded system, an institutionalized system, or a combination of the two. For example, if a DRM provider decided to allow editing and quoting using an editing software program that decodes the DRM but integrates an anonymous ID number with a watermark,\(^ {213}\) a pilot program could be developed to search for cases

\(^{212}\) The timing of judgment or filtering by technologies is closely related to the issue of private enforcement, which is generally prohibited by law. The de facto enforcement by private parties using technologies (or self-help) has been an issue for debate. See, e.g., Yochai Benkler, *An unhurried view of private ordering in information transactions*, 53 Vand. L. Rev. 2063 (2000); Julie E. Cohen, *Copyright and the jurisprudence of self-help*, 13 Berkeley Tech. L.J. 1089 (1998). From this standpoint, it can also be said that delaying the judgment is more consistent with legal enforcement systems. Except for a very clear violation, such as mass reproduction, there should be some policy to avoid too strict private enforcement and its chilling effects.

\(^{213}\) The system has to be privacy-friendly, too. Therefore, in designing a review program, the
of clear violation for works already published.\textsuperscript{214} Still, such a pilot program could not understand and make decisions regarding the context or content of the work, which might need to be supplemented by human judgment in institutions, such as courts or alternative dispute resolution systems, or even preliminarily by legal staff hired by right-holders.

In sum, it is possible to incorporate the freedoms extant within the copyright regime by combining coded and institutionalized systems even though the resulting freedoms would not be exactly the same as in the non-DRM world. Both the coded and institutionalized systems have their pros and cons, and the system designer should pay attention to the characteristics of each system to design a system with lower costs for users, right-holders, and system providers.

However, the ability to provide such systemized freedom does not guarantee that it will be provided in the real world. System integrators, most of whose primary customers are right-holders and content providers, may not have an instant market

---

\textsuperscript{214} There is also a problem of who would design the protocol of the pilot and review programs, because it would function as a primary alternative to court decisions. If the protocol is not appropriate, it will cause large chilling effects. It could be an area where government intervention is worth considering.
incentive to design DRM systems with any integrated freedoms. Therefore, the next Section discusses the government’s possible choices to help DRM systems be more balanced by supporting the integration of coded and institutionalized freedoms.

5.2.2.2 Legal Option supporting Coded and Institutionalized Approach for Freedom

When thinking about the role of the government in helping system integrators keep a better balance in DRM systems, decisions should be made, again, by comparing the pros and cons caused by such government intervention. The following generally describes what the government can do to help create balanced DRM systems, as well as what it ought to avoid.

5.2.2.2.1 Make Freedoms the Affirmative Rights of Copyright Users

Probably the least intervening option to the market is to state user freedoms as affirmative rights rather than defenses, and leave all implementation issues to the market. One reason why market negotiation between right-holders and users (or their representatives) cannot effectively incorporate the freedom within DRM systems is because the freedom is recognized as a defense, while the interests of copyright
holders are protected as rights, as mentioned above. This first option gives both parties equal legal standing in order to help enable more balanced negotiations between the interested parties, which would result in a more balanced implementation of DRM usage rules. This option may or may not include changes of rules for free uses.

In some cases, government should clear up some vagueness or fuzziness in the rules of freedom in order to reduce the transaction costs of judging the borders.

For example, Masaya Otsuka at Sony thinks that such a legislative change might be helpful.

If you ask me the questions of whether such “authorization of freedom as rights” will influence our negotiations with content owners, or influence the design of DRM systems or devices, I would say it is possible. If the rights are clearly stated as enforceable mandatory rights (and agreements against these rights are invalid), it would definitely have an impact. This is because we cannot sell products that infringe consumers’ rights…

However, Otsuka mentions that such user-friendly DRM may add some additional cost to the device makers’ side. In this regard, he mentions the importance of the rules of users’ rights being clear and relatively easy to implement.

From the viewpoint of technologists and device makers, we would weigh (1) the amount of increased users’ merit against (2) increased production costs. The problem of a cost increase can be solved if we use simple and clear rules. If so, as a device maker, [stating exemptions as

---

215 See, supra Section 5.3.2.
216 Interview with Masaya Otsuka, Senior Patent Manager, Sony, in Tokyo, Japan (Apr. 8, 2004).
The difficult part would be to determine the rules. For example, if we take the example of private copying, how broad should it be, and what criteria should we use? Is it OK to give the copies you personally made to your grandparents? How about friends? What kind of information should we use to make decisions?217

On the other hand, Otsuka is a little skeptical when users’ rights are voluntary.

[I]f the rights are voluntary and waivable (or, when the nature or rights are not clear), the impact could be subtle. Content owners can choose not to use [user-friendly] DRM if they don’t like the offered terms…. In such a case, device makers would develop their products with careful attention to the expression of their advertisements and specifications (to make sure that consumers understand the devices don’t respect the freedoms stated as rights. If they understand and still buy them, could we argue that they agreed to waive the rights?). However, situations could be improved by business norms and free competition. Therefore, even waivable rights may push the trend of user-friendly DRM.218

This concern that freedom is not being respected as much as expected is partly experienced in Europe, where the 2001 EU Copyright Directive took a mixed mandatory and voluntary approach to copyright exemptions with regard to anti-circumvention regulations. Even though Article 5 of the EU Copyright Directive clearly sets forth some exemptions that the member states are mandated to grant to copyright users, it does not clearly state whether they are users’ rights or defenses. In addition, Article 6 Paragraph 4 mandates member states to take “appropriate measures” to ensure some of the exemptions for users set forth in Article 5 (which

217 Id.
218 Id.
makes it sound as if they are rights).\textsuperscript{219} On the other hand, Article 6 also provides several significant loopholes to right-holders: for example, if there is an agreement between users and right-holders, such agreement takes precedence over stated exemptions.\textsuperscript{220} This means that the possible rights stated in Article 5 are, in practice, not considered mandatory but voluntary rights, or waivable rights by agreements. Also, by choosing on-demand online download services with agreements, content distributors are totally exempted from the obligation to pay attention to users’ rights.\textsuperscript{221} These escape routes in Article 6 have been criticized for significantly undermining the meaning of Article 5.\textsuperscript{222} Therefore, making users’ rights optional may not be as powerful to help balance the interests between right-holders and copyright users.

Therefore, it can be said that declaring some rights mandatory would help more in guiding the market toward more-balanced DRM systems. However, a different concern is raised by this idea of mandating users’ rights, mainly from the viewpoint of protecting privacy and confidential information. As Michael Miron explains:

\begin{quote}
Someone suggested to us that we ought to build in, including into the standards, a set of mandatory [users’] rights. You must have an
\end{quote}

\textsuperscript{219} See, Article 6 (4)(1) of the EU Copyright Directive of 2001. The limitations that are required to be protected here are: copying privileges for libraries, researchers, museums, hospitals and disabled persons. See, Bechtold, supra note 209.

\textsuperscript{220} See, Id.

\textsuperscript{221} See, Article 6 (4)(4) of the EU Copyright Directive of 2001.

\textsuperscript{222} See, Bechtold, supra note 209.
involuntary grant that is available to anybody anytime. But as we thought about it, we started to think “Well, gee, I have a document called a PDF file. Do I really want to say that I have an involuntary grant to read that? What happens … if the PDF carries my medical records as if it is a novel?”  

This concern is surely legitimate. The question, however, is not about whether any of the ‘free uses’ recognized by copyright law should be a right; it is rather about the scope of rights, or how to deal with conflicts with other rights such as privacy. As can be seen below, even Miron agrees that some kind of freedoms, such as back-up copies of purchased entertainment content, can be a right.

5.2.2.2.2 More Specific Carve-Out Provisions for Coded or Institutionalized Approaches to Freedom

The more difficult question is: What kind of uses should be qualified as mandatory rights and how detailed should the statute be? If the market took the institutionalized approach rather than the coded approach, the rules of users’ rights could be stated relatively generally, because the judgment would be made by human intelligence. In fact, if the government decided to leave the rules as flexible as they are now, there would be no other choice for the market but to opt for some form of institutionalized

---

224 See, infra Section 5.2.2.2.2.
system to realize users’ rights. However, leaving all decisions to an institutionalized system is relatively costly, as has been pointed out. This is because the institution must make decisions similar to those made by the courts, and because users must take extra steps to seek judgments, which will chill spontaneous uses and small-value uses.

Therefore, if the government wants to help ensure more voluntary freedoms within DRM technologies that impose lower transaction costs on users, especially for systems using the coded approach, it would be helpful either to have more detailed rules that are easily coded or to delegate judgments.

Michael Miron explains this point:

Fair use is a situation-specific defense against copyright infringement: it is not a pre-determined set of rights as one normally thinks about rights. As such, you cannot precisely define them in advance, although there have been some carve-outs in Europe to define some things. I’ve suggested to the U.S. government that they do the same thing. [They] said it’s kind of hard to do, so I don’t see a safe harbor anytime soon, although that’s more of the possibilities to assist systems implementers.

Miron elaborates the idea of providing carve-outs, using an example of making

---

225 See, supra note 205.
226 See, Id.
227 See, supra Section 5.4.2.2.1.1.
228 See, the EU Copyright Directive of 2001, Article 5.
back-up copies in the U.S.

[T]he government could assist system implementers by carving out specific uses. For example, if the government said “it is legal to make one backup copy.”… you just now gave a safe harbor to systems designers, who could put a copy counted one in a backup mode, maybe tied to domains. [There are] a lot of different ways to implement it depending on devices. But if they said “That is an appropriate fair use, so go ahead,” then, that’s an example…. Is a backup a violation? Unknown. It clearly is an expectation by a lot of consumers, but under the law it is not clear whether it passes the test [of fair use]. So that is an example of something that the government, if they wanted to, could carve out and say that’s a safe harbor.230

Tom Jacobs, Director of Research, Voodoo Sciences, Vanguard: Media Architecture & Technology Project at Sun Microsystems Laboratories agrees that the government may need to make the balanced rules clear. As Jacobs states:

I hate to say we need more government, and you probably don’t want [the government to mandate technologies]. I think probably what you want are more defined guidelines as to what is inbounds and what’s out of bounds. What would be considered breaking copyright, and what would be considered fair use….231

Another issue to be considered by the government is how finely the government defines users’ freedoms. The fineness of the rules might bias the market’s choice of the manner of implementation. This is because of the limits of computer abilities and costs

---

230 Id.
231 Interview with Tom Jacobs, Director, Sun Microsystems Laboratories, in Menlo Park, Cal. (Aug. 3, 2005).
with the coded approach, as explained above.232 The more general, the more situation-dependent, or the more context-dependent the rules become, the more likely it is that the market would opt for the institutionalized approach. On the other hand, if the rules are relatively specific without any substantial decisions about the context or substance of the use, the market can take the coded approach, too.

5.2.2.2.3 Specify Coded or Institutionalized Approaches to Freedom by Law

In addition to more finely defining the rules of users’ rights for the market to explore the opportunities for coded or institutionalized freedom, the government can step further into the manner of implementation to mandate specific coded or institutionalized freedom. While the previous option is just to make clear what the requirements for mandatory users’ rights are and leave the concrete implementation of the market (i.e., what part should be realized by the coded approach, and what others by the institutionalized approach, for example), this option is to specify what should be coded and what should be institutionalized.

Even though this sounds as if the government is intervening significantly, and it probably is, there is already legislation that has taken this approach. For example, the U.S. Audio Home Recording Act is an example that clearly states that devices should

232 See, supra Section 5.2.2.1.3.
take the coded approach for back-up copies. On the other hand, the EU Copyright Directive of 2001 is said to take a modified key-escrow approach, which is one form of the institutionalized approach. Article 6 Paragraph 4 of the EU Copyright Directive mandates Member States as follows:

… in the absence of voluntary measures taken by right-holders, including agreements between right-holders and other parties concerned, Member States shall take appropriate measures to ensure that right-holders make available to the beneficiary of an exception or limitation provided for in national law … the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

According to the Commentary on European Copyright Law, the above Article is interpreted to allow, in certain cases, that Member States can require content providers to provide content users with circumvention devices or services.

Because the government intervention always gives some bias to the market, the government should avoid as much as possible mandating anything harmful or costly to technological innovation when government decides to take this approach. For example, legislation that requires system integrators to integrate “all the freedoms that are

---

234 See, Bechtold, supra note 3 at 376.
236 See, Bechtold, supra note 3 at 376. See, also, Bechtold, supra note 209.
available under the copyright law’’ into their DRM systems may be harmful rather than helpful, because it may be unclear and thus prohibitively costly to decide what ‘‘all the freedoms’’ means. Rather, the government should make more of an effort to specify or list the freedoms that should be respected even within the DRM world.

Another thing that many technologists want the government to avoid, when stepping into a coded approach to freedom (or codes in general) is to mandate implementation of specific technology specifications. For example, Noboru Tohyama at Fujitsu, among others, clearly states this problem from two different directions:

I don’t want the government to mandate technological standards, because that would trouble the department of technological research and development. It would also be problematic to regulate devices that would not react to DRM systems. There are only two ways to do so: either they specify the technologies and mandate to incorporate them; or you have to make your devices respond to every possible DRM system available, which would require unlimited effort. Either way, I don’t want to see it happen.237

It might be possible under some circumstances that government would specify the freedom to be coded, but without determining the actual specifications of the technologies. Determining the actual specifications should be left to the market, as many have already pointed out.238

237 Interview with Noboru Tohyama, Fujitsu, in Tokyo, Japan (Nov. 22, 2002).
238 See, Burk & Cohen, supra note 193 at 55-57; Bechtold, supra note 3 at 368-71,
With regard to institutionalized freedom, there could be a diversity of levels of government intervention. The government could set guidelines of what should be followed by institutions and leave their formation and governance to the market. The other extreme example would be that the government itself run the institution.

Or, alternatively, the government could seek applications from private entities to handle the processes in question, designate or approve appropriate groups, and supervise their operation. Also, as discussed above, it is important to notice that the issue of who takes control over the organization would impact the fairness of the judgment.

As described above, the government would always bias the market by how detailed its requirements for the freedoms incorporated into DRM systems were. Whether further government involvement in system implementation is necessary or desirable should be left for later research, with more study on how the market can properly

---

239 A close example is Internet Corporation For Assigned Names and Numbers (ICANN), which coordinates the management of the technical elements of the Domain Name System to ensure universal resolvability. The actual implementation are delegated to local representatives. See, ICANN home page, http://www.icann.org/general/ (last visited April 27, 2006). Note, however, that the highly-centralized structure of rule making by ICANN calls attention regarding antitrust law in the U.S. See, A. Michael Froomkin and Mark A. Lemley, ICANN and Antitrust, 2003 U. Ill. L. Rev. 1 (2001).

240 An example is the U.S. copyright registration system by the U.S. Copyright Office.

241 An example is the Japanese copyright registration for software programs. See, Law on Exceptional Provisions for the Registration of Program Works, Chapter III.

242 See, supra Section 5.2.2.1.3.

243 See, supra Section 5.2.2.2.2.
realize the rules of users’ rights set by the government, as well as the possible negative impacts of government’s imposing specific system designs.

6. Conclusion

This article has shown that the problem of DRM systems overriding freedoms of copyright uses incorporated within the copyright regime are largely coming from the unbalanced implementation of DRM technologies, and that the current anti-circumvention regulations have fixed this problem by blindly prohibiting one means of solution: i.e., circumvention of DRM technologies that cause the problems. This research also shows that the anti-circumvention regulations are causing chilling effects and other negative impacts on scientific research regarding DRM technologies. By comparing anti-circumvention regulations between the U.S. and Japan, this research shows that the implementation made in the DMCA is not the only solution: rather, it shows that a more modest implementation like in Japan can be possible and desirable. In order to support such limited implementation, this research also revisits the rationale behind anti-circumvention regulations and shows that legally prohibiting the circumvention of DRM systems may not be important to stop piracy and to support content business as it first appears.
This research also shows, based on actual voices of key players in the market, that
the market would not function efficiently to implement within the DRM systems the
freedom of copyright use incorporated within the copyright law. This is because there
is imbalance in legal standings between right-holders and users; the mindset and/or
ability of the right-holders who have the power to decide the implementation rules are
not ready to respect the freedoms; and also because the voices of users are currently
not well represented in the market. After such extensive market analysis, this research
tends to see what law can do to help to bring DRM systems more balanced. It suggests
two solutions: repeal anti-circumvention regulations when DRM systems are
imbalanced, and keep proper balance within the framework of anti-circumvention
regulations. The latter choice can be broken down to two options. One is to give a
properly-tailored “right to hack” when there is legitimate reason to do so. The other is
to incorporate tools to embody freedom within the DRM system without giving a right
to hack. This research shows by using a concrete example that many of the freedoms
can be incorporated into DRM systems by combining coded approach using computer
systems and institutionalized approach using human intelligence. At the end, this
research provides three legal option to support freedom to be incorporated within the
DRM system: to declare the freedoms as affirmative (and preferably mandatory) rights of users to give users equal legal standings; to establish more detailed and clear carve out provisions to make it easy for DRM systems to implement; and to specify the actual manner of implementation by law. It also points out what the government has to pay attention in order to avoid market confusion when taking these steps: the most important one is to make the rule clear enough, as well as to avoid mandating particular technological specifications.

A decade has passed since the 1996 WIPO treaties has brought a significant change to the world of copyright. And we have seen more than enough problems in these new technologies and regulations. Hopefully this research has provided an opportunity to understand why the efforts in the DRM technologies have been rather painful for both right-holders and copyright users, and to show some steps to improve the current legal and market situation to realize a better-balanced world of copyright with DRM technologies.