

**THE DRM DILEMMA:  
RE-ALIGNING RIGHTS UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT**

**JACQUELINE LIPTON\***

**ABSTRACT**

*The Digital Millennium Copyright Act ('DMCA') prevents unauthorized copying and distribution of digital copyright works by regulating devices that can be used to circumvent Digital Rights Management ('DRM') measures that are used to restrict access to those works. A significant problem is that those devices, like many new technologies, have the potential to be used for both socially harmful and socially beneficial purposes. There is no obvious way for Congress to regulate circumvention devices to prevent the social harms, while at the same time facilitating the social benefits they might provide. Recent judicial interpretations of the DMCA have unsurprisingly erred on the side of harm-prevention to the detriment of potentially legitimate uses of circumvention devices. Unlike previous scholarship, this article suggests that the answer to this dilemma is not necessarily to amend the DMCA to bolster legitimate use exceptions to the anti-circumvention provisions. Instead, this article advocates resolving the problem through a new approach that takes socially beneficial uses of circumvention technologies outside the scope of the DMCA altogether. The idea is to create a new administrative complaints mechanism that would support those seeking to make such uses of digitally encrypted copyright works by imposing legal obligations on copyright holders to facilitate those uses. This approach has the added benefit of generating a significant amount of data about emerging social norms relating to the boundaries of the fair use doctrine that could be fed back into legislative and judicial processes as copyright law develops in the future.*

**TABLE OF CONTENTS**

INTRODUCTION .....	
I. FAIR USE UNDER THE DMCA .....	
A. The Legislative Framework .....	
B. The Role of Fair Use in Copyright Law .....	
C. Criticisms of Fair Use Protection Under the DMCA .....	
1. General Criticisms of the Anti-Circumvention Provisions with Respect to Fair Use .....	
a. <i>Universal City Studios v Reimerdes</i> .....	

---

\* Associate Professor and Associate Director, Frederick K Cox International Law Center, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, Ohio 44106, USA, (Email: JDL14@case.edu). For various useful comments and observations on earlier drafts of this paper, the author would like to thank participants in "Real Law and Online Rights", University of Virginia School of Law on February 19, 2005, as well as participants in the Inaugural International Symposium: "The Law and Information Interface in the Digitally Networked Society: Is a Conceptual Rethink Imperative?" held on February 4, 2005, at the University of Wolverhampton in the United Kingdom, sponsored by the History and Governance Research Institute. Thanks are also due to Professors Mark Lemley, Thomas Nachbar, and Craig Nard for comments on an earlier draft of this paper. All mistakes and omissions are those of the author.

## THE DRM DILEMMA

	<i>b. United States v ElcomSoft Ltd</i> .....	
	<i>c. 321 Studios v MGM Studios</i> .....	
	2. Critique of the Triennial Administrative Review Procedure.....	
II.	RE-ALIGNING COMPETING INTERESTS IN DIGITAL COPYRIGHT WORKS: THE GLOBAL DIMENSION .....	
	A. DRM Legislation in Australia.....	
	1. The Framework of the Australian Legislation .....	
	2. Judicial Interpretations of the Australian Legislation .....	
	B. DRM Legislation in the United Kingdom.....	
	1. The European Union Copyright Directive .....	
	2. The British Copyright and Related Rights Regulations .....	
	<i>a. Software Copyrights: Anti-Device Provisions</i> .....	
	<i>b. Works Other than Software: Anti-Circumvention and Anti-Device Provisions</i> .....	
III.	DIGITAL ENCRYPTION AND THE PRESERVATION OF FAIR USE .....	
	A. Crafting a Fair Use Mechanism for Digital Copyright Anti-Piracy Law.....	
	B. Determining Protected Uses.....	
	C. The Administrative Agency and Its Procedures.....	
IV.	CONCLUSIONS.....	

## INTRODUCTION

“While it may be too early to draw final conclusions, it is plain that DRM technologies, backed by laws like the DMCA, pose a serious potential threat to fair use. While technical refinements may address or minimize some of the social costs that stem from an erosion of fair use, it is unlikely that they will entirely resolve the tension.”<sup>1</sup>

Imagine that you are a student of musicology. Your professor has asked you to research Alban Berg’s Violin Concerto for a term paper on atonal musical forms. You are not remotely interested in Berg, violin concerti, or the atonal music movement. In fact, you enrolled in the musicology course mainly because you were interested in meeting an attractive sophomore who you heard was taking the class. However, you have to write the paper to complete the course.

During a Google search on the topic, you notice an advertisement for a new online service that will allow you to listen to samples of recent recordings of various musical works, as well as to access recent commentaries on those works by leading musicologists. You are extremely interested in this service as you figure that it will probably cut your research time in half. However, when you investigate further, you discover that the cost to access it is prohibitive on a student budget. You mention the service to the professor and ask if there is some way she can get you free or discounted access to the service through the music department. She tells you that she has been aware of this service for some time and she highly recommends it, but that the operators of the service do not

---

<sup>1</sup> Fred von Lohmann, *Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension Between Them*, available at: [http://www.eff.org/IP/DRM/fair\\_use\\_and\\_drm.php](http://www.eff.org/IP/DRM/fair_use_and_drm.php), last viewed on April 8, 2005.

currently provide academic or student discounts. She herself has had to spend a sizeable chunk of her own faculty budget on a subscription to the service.

This is obviously good news for you. If the professor has access, presumably she can make copies for you and your classmates. This is no different to her owning a vinyl record or audio cassette of a relevant music recording, and a hard copy book or journal of the expert commentaries in the good old days. Surely she could have copied relevant portions of those things for her students, so presumably she can make digital copies from the online service today. Unfortunately, it's not that simple.

For one thing, even before digital technology hit the scene, the extent of your professor's ability to make students copies of old fashioned media was not particularly clear cut.<sup>2</sup> Over the years, laws<sup>3</sup> and guidelines<sup>4</sup> developed on this issue, but some student copying may always have amounted to copyright infringement. It may merely have been tolerated by content industries as a necessary inconvenience that could not be effectively policed.<sup>5</sup> This is because it has traditionally been too difficult for content owners to police and enforce their copyrights in an aggressive way in all classrooms and private homes around the world. However, DRM technologies<sup>6</sup> now allow content owners to exercise more control over all unauthorized reproductions of their works.

Imagine, then, that the owner of the online service described above has imposed DRM measures to restrict access to, and copying of, the relevant music and commentaries unless the appropriate fee has been paid. Thus, your professor can access the relevant material provided that she maintains payment of her subscription fees, but she is physically unable to make a digital copy of the music or the commentary. Imagine further that the law does not technically prevent her from cracking the DRM measure and

---

<sup>2</sup> See RALPH S. BROWN and ROBERT C. DENICOLA, COPYRIGHT: UNFAIR COMPETITION, AND RELATED TOPICS BEARING ON THE PROTECTION OF WORKS OF AUTHORSHIP (8 ed, 2002), 436-443 (on classroom copying generally and the guidelines for classroom reproductions).

<sup>3</sup> 17 U.S.C. § 107 (fair use in copyright law).

<sup>4</sup> Agreement on Guidelines for Classroom Copying in Not-For-Profit Educational Institutions with respect to books and periodicals, March 19, 1967 (between Ad Hoc Committee on Copyright Law Revision, Author-Publisher Group, Authors League of America, Association of American Publishers Inc.), reproduced in Brown, *supra* note \_\_\_, 438-440; Guidelines for Educational Uses of Music, April 1976 (between the Music Publishers' Association of the United States, Inc., the National Music Publishers' Association, Inc., the Music Teachers National Association, the Music Educators National Conference, the National Association of Schools of Music, and the Ad Hoc Committee on Copyright Law Revision).

<sup>5</sup> See RALPH S. BROWN and ROBERT C. DENICOLA, COPYRIGHT: UNFAIR COMPETITION, AND RELATED TOPICS BEARING ON THE PROTECTION OF WORKS OF AUTHORSHIP (8 ed, 2002), 436-443 (on classroom copying generally and the guidelines for classroom reproductions); See also *Princeton University Press v Michigan Document Service*, 99 F 3d 1381 (6<sup>th</sup> Cir. 1996) (finding copyright infringement for much larger scale university photocopying of 'coursepacks' than contemplated in the example here).

<sup>6</sup> One generally accepted definition of DRM systems is the 'secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works': Dan Burk and Julie Cohen, *Fair Use Infra-Structure for Rights Management*, 15 HARVARD JOURNAL OF LAW AND TECHNOLOGY 41, 48 (2001).

make copies of the relevant material for students, assuming that she could establish the copying was for a 'fair use' purpose.<sup>7</sup> Nevertheless, having devoted her life to musicology, she is no expert on decryption technology and is unable herself to crack the relevant code. She needs some device or service that would help her to do so. However, the aggressive enforcement of a new digital anti-piracy law has effectively put most companies out of business that used to manufacture and distribute the kind of technology she would need. The unavailability of these technologies also prevents you from cracking the code yourself in order to *access* the material you want without paying for it, again assuming you could establish a fair use purpose. In any event, the new law would prohibit you from making unauthorized *access* even for a fair use purpose.<sup>8</sup>

Your professor therefore suggests that you buy or borrow a recoding of the violin concerto, and that you go to the library and find some commentaries on the concerto. They may not be as good or as up-to-date as the online commentaries, but short of paying a large fee to subscribe to the online service for the purposes of writing one term paper, they are the best you can do.

In one sense, you are pretty annoyed with this outcome, particularly because you were trying to win a bet with your best friend to get through a whole semester without physically setting foot in the library. On the other hand, you understand the reason why the online music service chose to restrict access to, and use of, its works in this way. If it was not so restrictive, it could not protect its work and its business model against digital copyright pirates who could utilize digital media to make fast, cheap, and near perfect copies of its materials, and to distribute them globally at the push of a button with no compensation to the online music service.<sup>9</sup>

Hence, the DRM dilemma: the question of how effectively digital technology might be regulated to prevent digital copyright piracy, while at the same time facilitating fair uses of digital copyright works.<sup>10</sup> This is a fundamental issue in digital copyright law which has serious implications for the balance of information access and use in many different fields and across national borders. This article suggests that the issue needs to be addressed head on before a serious information imbalance arises in the global information society, to the extent that this is not already happening. In so doing, it advocates a novel approach to protecting fair uses of digital copyright works by taking them outside the scope of digital copyright anti-piracy laws like the Digital Millennium

---

<sup>7</sup> See 17 U.S.C. § 107.

<sup>8</sup> 17 U.S.C. § 1201(a)(1)(A).

<sup>9</sup> The DMCA mirrors the content industries' concerns here: Dan Burk, *Anticircumvention Misuse*, 50 UCLA L REV 1095, 1135 (2003) (legislative aims behind the drafting of the DMCA were to prevent 'piracy' in digital works); Electronic Frontier Foundation, *Unintended Consequences: Five Years Under the DMCA*, available at [http://www.eff.org/IP/DMCA/unintended\\_consequences.php](http://www.eff.org/IP/DMCA/unintended_consequences.php), last viewed on March 21, 2004 and on file with the author.

<sup>10</sup> Again, assuming that we have at least a vague idea of the boundaries and scope of the fair use doctrine. This issue is discussed in more detail *infra*.

Copyright Act (“DMCA”) and supporting them instead through a new administrative complaints mechanism.

These questions are separate to those recently addressed by the Supreme Court in *MGM Studios v Grokster*,<sup>11</sup> although both problems are created by recent developments in digital technology, and both situations share some similar dynamics. The *Grokster* litigation involved attempts by digital content industries to combat copyright infringements by unauthorized peer-to-peer file sharing.<sup>12</sup> The plaintiffs in that litigation, and other similar litigation,<sup>13</sup> have sought to hold manufacturers and distributors of file sharing services secondarily liable for direct copyright infringements committed by the users of those services.

The DRM dilemma addressed in this article, on the other hand, deals with something even more fundamental: attempts by digital content industries to utilize technological encryption measures to control initial *access* to, as well as copying of, digital works. As with the digital file sharing situation, these industries have employed a secondary liability strategy focused on third parties not directly involved in specific acts of copyright infringement. In the case of the DRM dilemma, the third parties are those who manufacture and distribute ‘circumvention’ devices: that is, devices that can be used to circumvent technological encryption measures utilized by content industries to control access to, and use of, their works. Unlike file sharing situations, the content industries required legislative support to create a new regime to hold these third parties responsible for the manufacture and distribution of such circumvention technologies.<sup>14</sup>

Although much recent digital copyright literature understandably focuses on *Grokster*, and the digital file sharing problem more generally, the DRM dilemma has much more serious implications for society, both nationally and globally, than the resolution of the digital file sharing issue. This is because DRM technologies, bolstered by DRM-supporting legislation, pose a very serious threat to fair use because of their implications for *accessing* protected works. They effectively prevent many fair uses from ever taking place. Even though the aims of the DMCA are laudable, the regulation of circumvention technologies in this way seriously threatens to damage the pre-existing balance of interests in copyright works.

---

<sup>11</sup> *MGM Studios v Grokster*, 380 F.3d 1154 (2004), appealed to the United States Supreme Court.

<sup>12</sup> Alfred Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, forthcoming CASE WESTERN RESERVE UNIVERSITY LAW REVIEW, 2005 (detailed discussion of peer to peer file sharing and associated legal issues).

<sup>13</sup> See, for example, *A&M v Napster*, 239 F 3d 1004 (9<sup>th</sup> Cir, 2001); *In re Aimster Copyright Litigation*, 334 F 3d 643 (7<sup>th</sup> Cir. 2003).

<sup>14</sup> Legislative support was also required to sanction individual acts of circumvention. This support came in the form of a new Chapter 12 inserted into Title 17 of the United States Code in 1998 as part of the Digital Millennium Copyright Act (‘DMCA’). Unlike traditional copyright law, this legislation prohibits unauthorized *access to* digitally encrypted copyright works amongst other things.

This is the heart of the DRM dilemma. If circumvention devices are regulated in this way, fair use is under threat. This means that the previously existing societal balance in relation to access and use of copyright works potentially falls apart. However, if circumvention devices are not effectively regulated, digital content industries may be unable, or less able, to rely on encryption technologies that could protect their works against digital copyright piracy.<sup>15</sup> This ultimately affects their business models and the prices for which, and contractual terms on which, they will be prepared to make digital works available to the public.

To date, the dilemma has been addressed in various ways. The DMCA itself evidences a legislative intention to protect fair use. The legislation expressly states that fair use rights are not intended to be affected by the operation of the DMCA.<sup>16</sup> The DMCA also incorporates a triennial review to be conducted by the Librarian of Congress on the advice of the Register of Copyrights with a view to creating necessary exemptions for particular classes of works from the operation of certain aspects of the anti-circumvention provisions of the DMCA.<sup>17</sup> None of these measures has proved particularly effective in practice to date as demonstrated *infra*.

By contrast to the current approaches, this article suggests a new approach to the DRM dilemma. It advocates preserving the current system with its emphasis on restricting trafficking in circumvention devices, while at the same time developing a separate administrative complaints mechanism for individual fair users to preserve particular fair uses of given works. This would be different from the current approaches because it could be individually tailored to specific fair use complaints. It would accommodate the timescale of individual fair users and their specific fair use needs. Unlike the triennial review, it would not be based on identifying classes of works that may be exempted from the anti-circumvention provisions of the DMCA, nor would there be three year time lags between determinations. This would prevent the balance of interests in digital copyright works from becoming too skewed against fair users while awaiting the next set of administrative determinations. The new system would also impose affirmative legal duties on copyright holders to make *access* to given works available to those seeking to make a fair use of a relevant work.

Copyright holders would still be able to proceed against those trafficking in anti-circumvention devices under the existing provisions of the DMCA. The assumption here is that if a simple, inexpensive, individually tailored complaints procedure could be put in place to preserve fair use, there would be much less cause for concern about aggressive enforcement of the DMCA's anti-trafficking provisions against those who manufacture and distribute circumvention devices. If fair use could be protected in other ways without

---

<sup>15</sup> This is because all good encryption measures can ultimately be hacked even if it takes some time to do so. At least legal sanctions against decryption provide some additional comfort to content industries who want to rely on digital encryption measures.

<sup>16</sup> 17 U.S.C. § 1201(c)(1) (“Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.”).

<sup>17</sup> 17 U.S.C. § 1201(a)(1)(B) – (D).

the potential fair user having to avail herself of such a device in the open market, there would be no reason to object to stringent enforcement of the anti-trafficking provisions. It would be reasonable to assume that much of the market for such devices would be to promote illegal digital piracy, provided that legitimate users of copyright works could effectively gain access to the works through the administrative procedure.

Another benefit of such a system is that it would generate data about emerging social norms relating to the boundaries of fair use in the digital age. This data could be fed into the law reform process in catering to new challenges posed by digital technology that might threaten the existing balance of interests in digital copyright works. Additionally, such a system might ultimately encourage private settlement of complaints about lack of fair use to digital copyright works. This is because one of the underlying assumptions of the system would be that fair use has to be accepted as an important part of the copyright structure and of the social bargain underlying the grant of a copyright. If fair use was clearly accepted as a legal right, rather than as a mere defense to a copyright infringement action, it might create incentives for copyright holders to better accommodate fair users privately. This may lead the market to create its own solutions to balancing these rights in due course, particularly after some data was generated by the administrative mechanism as to the boundaries of the fair use right in the digital age.

Part I sets out the relevant background to the enactment of the DMCA, including the legislative intentions in relation to fair use and judicial interpretations of the DMCA with respect to fair use. Part II situates the problem in a broader global context and surveys similar legislation in other jurisdictions. Given that the imbalance of rights under the DMCA is now being mirrored in other countries, it is imperative that law-makers globally start trying to re-align the balance of rights in digital copyright law as a matter of the highest priority. If the United States Congress acts now, it can be a world leader in implementing such re-alignment strategies and will not be relegated to either following the lead of strategies gradually being developed in other jurisdictions,<sup>18</sup> or creating approaches that do not sit well with those in other countries. It is particularly important to address this problem with an eye to global harmonization because of the ease with which digital information can cross national borders. Part III develops the contours of the new administrative complaints procedure in more detail, including the suggestion that the nature and scope of the fair use doctrine need to be more fully developed for the doctrine to be a meaningful part of copyright law in the digital age. Part IV then draws conclusions from the observations made in the previous sections and sets out some ideas for future legal developments in aligning rights and interests in digital copyright works.

## I. FAIR USE UNDER THE DMCA

### A. THE LEGISLATIVE FRAMEWORK

---

<sup>18</sup> For example, the new administrative complaints procedure adopted in 2003 in the United Kingdom – *see infra*.

Concerned about the possibility that the advent of digital technology and its use in digital content industries could stifle, rather than promote, innovation, the World Intellectual Property Organization ('WIPO') adopted provisions in two 1996 treaties to protect content industries against digital piracy.<sup>19</sup> The aim was to encourage treaty signatories to provide legal sanctions for unauthorized circumvention of DRM measures that encrypted a copyright work.<sup>20</sup> The rationale was to bolster DRM measures protecting a copyright work with legal sanctions for unauthorized interference. DRM measures did not have to be *foolproof* or *unbreakable* to attract legal protection. Provided that the measure was *sufficiently effective*<sup>21</sup> in operation to be categorized as an 'effective technological protection measure' under the relevant legislation, a legal remedy would be available to a content owner who claimed unauthorized access to, or use of, the work as a result of someone cracking a DRM system.

This seems simple enough. However, with the clear legislative focus on preventing unauthorized access to, and use of, digitally encrypted copyright works, the idea of protecting legitimate interests in copyright works against restrictive DRM measures seemed to be inadvertently sidelined. This has meant that the protection of some legitimate interests in accessing and using digital copyright works has, to a significant extent, been lost in translation. The ability of individuals to make fair uses of a digital copyright work, for example, has received inadequate protection under legislation that has been enacted to give effect to the relevant articles of the WIPO treaties.

Part of the reason for this, as demonstrated *infra*, is that unless fair use is accepted as a clear legal right to access and use a work, rather than as a mere defense to an act of copyright infringement, there is no way to effectively regulate circumvention technologies without encroaching on fair use. Any legislation that prevents acts of circumvention or trafficking in circumvention devices will encroach on fair use if it does not additionally place affirmative obligations on copyright holders to make access and use of copyright works available to potential fair users for fair use purposes. The only realistic way to place such affirmative obligations on copyright holders is to accept that fair use is a legally guaranteed right and not a mere tolerated convenience. Otherwise, there is no legal basis for imposing affirmative obligations on copyright holders to facilitate fair use.

Although the imposition of such duties on copyright holders may seem like a new concept in copyright law that unfairly shifts the balance of interests away from copyright holders by lessening their power to control their works, it is, in fact, not such a conceptual

---

<sup>19</sup> The Copyright Treaty of 1996, and the Performances and Phonograms Treaty of 1996.

<sup>20</sup> WIPO Copyright Treaty of 1996, Art. 11; WIPO Performances and Phonograms Treaty of 1996, Art. 18.

<sup>21</sup> See, for example, 17 U.S.C. § 1201(a)(3)(B), providing that: "a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."

stretch from the current law. It has never been clear that fair use is not a guaranteed legal right,<sup>22</sup> although admittedly it has never been clear that it is such a right.<sup>23</sup> However, it has always been assumed that fair use is an integral part of the social bargain under copyright law. Along with the idea-expression dichotomy,<sup>24</sup> fair use is an essential part of the balance of rights and interests to ensure an appropriate flow of information and ideas throughout society. Thus, even if there were good reasons in the past for relegating fair use to the status of a defense to copyright infringement, the advent of digital technology that can be used to restrict access to copyright works, may require a shift in the thinking and an elevation of the defense to an independent right of action. In other words, perhaps digital technology necessitates transforming fair use from a shield into a sword. These ideas are taken up in more detail *infra*.

Following the requirements of the 1996 WIPO treaties, Congress drafted the DMCA which, amongst other things, inserted a new Chapter 12 into Title 17 of the U.S.C., giving effect to the relevant WIPO treaty requirements. The WIPO Copyright Treaty of 1996 requires that:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.<sup>25</sup>

The WIPO Performances and Phonograms treaty makes similar provision in the context of relevant works.<sup>26</sup> These treaties do not say anything more about the effect

---

<sup>22</sup> WILLIAM CORNISH and DAVID LLEWELYN, *INTELLECTUAL PROPERTY: PATENTS, COPYRIGHTS, TRADE MARKS AND ALLIED RIGHTS* (5 ed, 2003) 808 (noting that British law has generally assumed that fair dealing exceptions to copyright infringement, the British equivalent to fair use, have generally been assumed to be constitutionally guaranteed rights of access and use, although there has historically been little actual debate about it); *Sony Corporation v Universal City Studios*, 464 U.S. 417 (1984) (majority and minority judges disagreed over the extent of transformative use necessary for finding of fair use).

<sup>23</sup> *321 Studios v MGM Studios*, 307 F Supp 2d 1085, 1011 (2004) (despite obiter comments in Supreme Court cases, it is not clear that fair use is a constitutionally guaranteed right).

<sup>24</sup> Nimmer on Copyright, §2.03[D] (copyright may be claimed in the ‘expression’ of a work but not in its underlying ‘idea’; this protects freedom of speech).

<sup>25</sup> WIPO Copyright Treaty of 1996, Art. 11. See also WIPO Performances and Phonograms Treaty of 1996, Art. 18, providing that: “Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.”

<sup>26</sup> Art. 18: “Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect

these requirements might have on interests in copyright works such as fair use, other than the above statement that legal protection shall be available for DRM measures used to restrict activities that are not ‘permitted by law’. Thus, the drafters of the treaties seem to have implicitly assumed that the domestic implementation of the relevant treaty terms would not adversely impact activities that are permitted by law, such as fair use.

The new Chapter 12 of Title 17, hereinafter referred to somewhat generically as the ‘DMCA’, contains prohibitions on *circumventing* access-control measures,<sup>27</sup> as well as *trafficking* in devices that can circumvent access-control<sup>28</sup> and copy-control measures.<sup>29</sup> These prohibitions attract both civil remedies<sup>30</sup> and criminal penalties.<sup>31</sup> There is, however, no specific restriction on circumventing a *copy-control measure*, because of the Congressional intention to preserve fair use in relation to copyright works.<sup>32</sup> In fact, Congress inserted a provision into the DMCA to make this clear. Sub-section 1201(c)(1) of Title 17 provides that: “Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, *including fair use*, under this title.”<sup>33</sup>

Additionally, Sections 1201(a)(1)(B) to (D) of Title 17 set out an administrative procedure to exempt circumventions of *access-control* measures applied to certain classes of works from the provisions of § 1201(a)(1)(A). This procedure requires the Librarian of Congress to make triennial determinations of relevant classes of works based on the advice of the Register of Copyrights.<sup>34</sup> In particular, such determinations are intended to be made, taking into account some of the classic ‘fair use factors’<sup>35</sup> as well as other

---

of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.”

<sup>27</sup> 17 U.S.C. § 1201(a)(1)(A).

<sup>28</sup> 17 U.S.C. § 1201(a)(2).

<sup>29</sup> 17 U.S.C. § 1201(b).

<sup>30</sup> 17 U.S.C. § 1203.

<sup>31</sup> 17 U.S.C. § 1204.

<sup>32</sup> *United States v Elcom Ltd*, 203 F Supp 2d 1111, 1120-1121 (2002) (Congress did not ban the act of circumventing *use* restrictions – as compared with *access* restrictions – because it sought to preserve the fair use rights of persons who had lawfully acquired a work).

<sup>33</sup> 17 U.S.C. § 1204 (emphasis added).

<sup>34</sup> 17 U.S.C. § 1201(a)(1)(C).

<sup>35</sup> 17 U.S.C. § 1201(a)(1)(C)(ii), (iii) and (iv) (requiring the Librarian of Congress to take into account, amongst other things: (a) the availability for use of works for nonprofit archival, preservation, and educational purposes; (b) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; and, (c) the effect of circumvention of technological measures on the market for or value of copyrighted works.)

relevant issues.<sup>36</sup> The first set of determinations was published in October, 2003 and exempted four classes of works from the *access-control* prohibitions.<sup>37</sup> The limited nature of the determination ultimately made could be regarded as somewhat disappointing from the perspective of seriously protecting legitimate interests in copyright works from restrictive DRM measures bolstered by the DMCA. Additionally, as the following discussion will evidence, the current triennial administrative mechanism has many other deficiencies in terms of its ability effectively to protect fair use in copyright works.

## B. THE ROLE OF FAIR USE IN COPYRIGHT LAW

Fair use has always been a problematic concept within copyright law. Although it is clearly the most important defense for an action for copyright infringement,<sup>38</sup> its precise boundaries have never been clear. This is largely because it is historically an equitable defense<sup>39</sup> that benefits from flexibility.<sup>40</sup> Judicially created, it has now been codified in the United States in § 107 of Title 17. This section does not provide a clear definition of what a fair use is, nor how the doctrine operates in practice. Rather, it mentions classes of uses that might typically be thought of as ‘fair use’ in an inclusive, rather than an exclusive, manner.<sup>41</sup>

---

<sup>36</sup> 17 U.S.C. § 1201(a)(1)(C)(v) (in making a determination the Librarian of Congress should consider ‘such other factors as the Librarian thinks appropriate).

<sup>37</sup> Library of Congress, *Copyright Office; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, available at <http://www.copyright.gov/fedreg/2003/68fr2011.html>, last viewed on April 13, 2005 (exempting the following classes of works from the access control provisions: (a) Compilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of e-mail; (b) Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete; (c) Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace; and, (d) Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format.)

<sup>38</sup> MARSHALL LEAFFER, *UNDERSTANDING COPYRIGHT LAW* (3ed, 1999), 427.

<sup>39</sup> *id.*

<sup>40</sup> *id.*, 429.

<sup>41</sup> The list of fair use purposes set out in 17 U.S.C. § 107 includes: “...purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research...”.

Section 107 lists four ‘fair use factors’ that courts can use in determining whether a particular use is a fair use. Again, these factors are not decisive, but are intended to allow courts the flexibility to develop the doctrine appropriately in the face of new factual circumstances. The idea of this drafting is to allow the continued development of the fair use doctrine in the face of new technologies and new practical circumstances.<sup>42</sup> The four factors are: (1) the purpose and character of the use, including whether the use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyright work; (3) the amount and substantiality of the portion used in relation to the copyright work as a whole; and, (4) the effect of the use upon the potential market for or value of the copyright work.

Obviously, nothing in § 107 defines clear boundaries for the fair use doctrine. This is a matter for incremental judicial determinations. However, two additional questions have come to plague the fair use doctrine in recent years because of the challenges posed to copyright law by new digital technologies. These questions are:

- (a) How should fair use be characterized in terms of its legal basis? In other words, is fair use a legally guaranteed right, a privilege, or a mere tolerated inconvenience for the copyright holder?
- (b) How productive/transformational does a use have to be in order to qualify as a fair use? Productive or transformational uses might be described as uses that “build on the works of others by adding their own socially valuable creative element”.<sup>43</sup>

Courts and commentators have differed on these questions.<sup>44</sup> Although in the past they may have seemed somewhat academic, they both become extremely important in the face of digital technologies that can easily restrict access to, and unauthorized uses of, copyright works. The first question is the most important for the purposes of this discussion. If fair use is a legally guaranteed right, technological measures should not be employed by copyright holders to the extent that they curtail such rights. If the only way to prevent digital copyright piracy is to employ such measures, it should be incumbent on copyright holders to facilitate fair use accesses to, and uses of, their works. However, if, on the other hand, fair use is only a tolerated inconvenience, then arguably a copyright

---

<sup>42</sup> MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW (3ed, 1999), 429.

<sup>43</sup> *id.*, 430.

<sup>44</sup> See, for example, MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW (3ed, 1999), 428 (citing *Rosemont Enters Inc v Random House Inc*, 366 F 2d 303, 306 (2d Cir 1966), *cert denied*, 385 U.S. 1009 (1967) describing fair use as a ‘privilege’); WILLIAM CORNISH and DAVID LLEWELYN, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHTS, TRADE MARKS AND ALLIED RIGHTS (5 ed, 2003) 808 (noting that British law has generally assumed that fair dealing exceptions to copyright infringement, the British equivalent to fair use, have generally been assumed to be constitutionally guaranteed rights of access and use, although there has historically been little actual debate about it); *Sony Corporation v Universal City Studios*, 464 U.S. 417 (1984) (majority and minority judges disagreed over the extent of transformative use necessary for finding of fair use).

holder has every right to utilize whatever technology and contractual measures<sup>45</sup> possible to prevent digital piracy, and if fair use is a casualty in this battle, so be it.

It is therefore important in the digital age to answer this question about the nature of fair use. As noted above, this article takes the stance that developments in digital technology require fair use to be accepted as a legally guaranteed right capable of forming the basis of a legal action to impose a duty on a copyright holder to facilitate a relevant use. Even if fair use has not been characterized in this way in pre-digital copyright law, the time has come to elevate its status to combat the imbalances created by digital technology, now bolstered by legislation such as the DMCA.

As to the second question about productive/transformational uses, this issue attains a great significance in the digital age because of the abundance of personal copying that is enabled by such technologies as mp3 file sharing software. It may seem more immediately relevant in situations like the *Napster*<sup>46</sup> and *Grokster*<sup>47</sup> file sharing scenarios than in the DRM context. However, if fair use is to be acknowledged as, or elevated to the status of, a legally guaranteed right, it is important to have some idea of its scope. These file sharing technologies raise the issue previously considered by the Supreme Court in the well known *Sony Betamax* litigation,<sup>48</sup> about the scope of fair use in terms of personal copying. If fair use is a legal right, it will be important for decisions to be made as to whether even small scale copying of digital works for personal uses will fall within the scope of the concept. Are these uses sufficiently productive/transformational to be regarded as fair uses and, indeed, do they have to be?

This question does not necessarily need to be answered for the purposes of the discussion here about protecting fair use in light of DRM measures restricting access to, and use of, copyright works. However, it is worth noting that an administrative fair use facilitation mechanism such as that presented in this article may generate important and useful data about emerging social norms relating to fair use, including in the digital file sharing context. This is not to say that everything claimed by potential users of copyright works will necessarily be deemed a fair use by an administrative agency or a court. However, the procedures advocated here will at least have the potential to generate significant volumes of data about what segments of society regard as fair use, and why. This will be helpful in future developments in copyright law as new technologies emerge that may again affect the social bargain with respect to competing interests in copyright works.

---

<sup>45</sup> Most of the discussion in this article focuses on the use of DRM measures to prevent unauthorized access to, and use of, digital copyright works. However, contractual restrictions obviously also have an important role to play here and are mentioned throughout the following discussion where appropriate.

<sup>46</sup> *A&M Records v Napster Inc*, 239 F.3d 1004 (2001).

<sup>47</sup> *MGM Studios v Grokster*, 380 F.3d 1154 (2004), appealed to the United States Supreme Court.

<sup>48</sup> *Sony Corp. of America v Universal City Studios, Inc*, 464 U.S. 417 (1984).

The administrative procedure advocated here has a significant advantage over waiting for legislative and judicial determinations on the questions raised above. This is because a fast and inexpensive administrative procedure can generate more data more quickly than typical judicial proceedings or Congressional hearings. This, in turn, can inform future legal developments at the legislative and the judicial level, thus creating an evolving system where administrative decisions and data feed into judicial and legislative processes, whose determinations ultimately feed back into the administrative procedure. This would help to guide administrators in everyday decisions about legitimate uses of digital copyright works. After some years of this system, a much more sophisticated picture of socially and economically appropriate norms relating to competing uses of digital copyright works could be generated and applied within the legal process.

The other obvious advantage of the administrative procedure advocated here is that it would help to strengthen and preserve legitimate, if unauthorized, uses of copyright works outside DRM-protection legislation, such as the DMCA. Thus, applications of DMCA style laws could be more easily limited to digital copyright piracy cases – the area in which they were intended to operate – while fair uses could be separately protected outside the scope of that legislation. If fair use was protected in this way, rather than as a vague exception or possible defense to a DMCA claim,<sup>49</sup> there may be less objection to aggressive enforcement of the DMCA in circumstances involving a serious potential for digital copyright piracy. This is because there would be less chance of a successful DMCA claim adversely affecting legitimate uses of copyright works by stifling the availability of a decryption technology that has both legitimate and illegitimate possible uses. If legitimate uses are preserved under a stand-alone system, such DMCA-based incursions into marketing decryption technologies may not matter so much to potential legitimate users of an encrypted work.

## C. CRITICISMS OF FAIR USE PROTECTION UNDER THE DMCA

### 1. GENERAL CRITICISMS OF THE ANTI-CIRCUMVENTION PROVISIONS WITH RESPECT TO FAIR USE

The DMCA's anti-circumvention and anti-trafficking provisions have attracted a great deal of criticism over the years, notably for their failure to maintain an adequate balance of interests in digital copyright works.<sup>50</sup> Professor Samuelson has noted that even

---

<sup>49</sup> It is not currently clear that fair use is, in fact, a defense to a DMCA claim: Dan Burk, *Anticircumvention Misuse*, 50 UCLA L REV 1095, 1137-1138 (2003) (DMCA makes no explicit provision for fair use with regard to the anticircumvention right itself, as distinct from the copyright in the underlying work); *Universal City Studios, Inc v Reimerdes*, 111 F Supp 2d 292, 322, 323-324 (S.D.N.Y. 2000); *aff'd* 273 F 3d 429 (2d Cir 2001) (fair use is not a defense to DMCA infringement); Pamela Samuelson, *Intellectual Property in the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Tech LJ 519, 539 n. 108 (1999). But now see also *Chamberlain v Skylink*, 381 F.3d 1178, 1200, 1201; 2004 U.S. App. LEXIS 18513, 59, 65 (2004) (suggesting there must be a link between fair use and copyright infringement for the DMCA anti-circumvention provisions to apply in a given case).

<sup>50</sup> Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14(3) BERKELEY TECH L J 519 (1999); David Nimmer, *A Riff on Fair Use*

though the DMCA appears to protect fair use rights by not prohibiting circumventions of copy control measures *per se*,<sup>51</sup> the legislation really does little to support fair uses of protected works. This is because most potential fair users do not have the technological know-how to *access* protected works in order to make a fair use of them,<sup>52</sup> and because there is no provision in the DMCA to permit the distribution of circumvention tools to enable fair use.<sup>53</sup> The DMCA should perhaps contain an exemption for *accessing* a protected work in order to make a fair use of it.<sup>54</sup>

More recently, Professor Reese has argued that the distinction between *access* prohibitions and *use* prohibitions under the DMCA makes little sense with respect to modern DRM measures.<sup>55</sup> He has pointed out that access and copy control measures are increasingly merged in practice.<sup>56</sup> Thus, a legislative prohibition on unauthorized *access* is tantamount to a prohibition on *use* even if the use in question would otherwise be preserved under the legislation.<sup>57</sup>

---

*in the Digital Millennium Copyright Act*, 148 U PA L REV 673 (2000); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 NYUL REV 354 (1999); John R. Therien, *Exorcising the Specter of a "Pay-Per-Use" Society: Toward Preserving Fair Use and the Public Domain in the Digital Age*, 16 BERKELEY TECH. L.J. 979 (2001) (on concerns that the DMCA will over-propertize digital information if courts do not take an adequate stance on protecting 'fair uses'), Tricia J. Sadd, *Fair Use as a Defense Under the Digital Millennium Copyright Act's Anti-Circumvention Provisions*, 10 GEO. MASON L. REV. 321 (2001); Harry Mihet, *iBRIEF: COPYRIGHTS & TRADEMARKS: Universal City Studios, Inc. v. Corley: The Constitutional Underpinnings of Fair Use Remain an Open Question*, 2002 DUKE L. & TECH. REV. 3 (2002).

<sup>51</sup> 17 U.S.C. § 1201(b)(1) (prohibits trafficking in a device that can circumvent a copy control measure, but not circumvention of a copy control measure *per se*); 17 U.S.C. § 1201(1)(c) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."); Samuelson, *supra* note \_\_\_\_, at 539-557.

<sup>52</sup> Samuelson, *supra* note \_\_\_\_, at 551 ("It is unclear whether Congress intended for the technologically savvy who could "do it themselves" to be the only ones who could engage in privileged acts of circumvention.")

<sup>53</sup> *id.*, at 548 ("section 1201 contains no provision enabling the development or distribution of circumvention tools to enable fair use or other privileged uses in terrain which section 1201(a)(1)(A) doesn't reach (i.e., making fair uses of lawfully acquired copies)").

<sup>54</sup> There are several bills currently before Congress that attempt to clarify this situation: Digital Choice and Freedom Act of 2003, H.R. 1066, 108<sup>th</sup> Cong. (2003); Digital Media Consumers' Rights Act of 2003, H.R. 107, 108<sup>th</sup> Cong (2003). See *infra*.

<sup>55</sup> R Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH LJ 619 (2003).

<sup>56</sup> *id.*, at 621 ("Copyright owners may ... be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such "merged" control measures as entitled to the legal protections of both access-and rights-control measures, even when the system was essentially directed only at preventing copying and distribution, rather than at controlling access. If courts continue to treat merged control measures in this manner, copyright owners may have an incentive to use such merged controls in order to maximize their legal protection.")

<sup>57</sup> *id.*

The DMCA thus clearly has the potential to powerfully enhance the rights of copyright holders in digital works. Indeed, this is the legislative intention. Governments around the world have been concerned to promote digital commerce,<sup>58</sup> and to prevent digital piracy.<sup>59</sup> These are difficult tasks to achieve in a borderless digital world. In particular, it is difficult to strike a legislative balance that promotes the interests of content holders against the very real threat of digital piracy, without at the same time compromising other legitimate interests in digital content, such as fair use.

Outside the nominal attempt to protect fair use interests in digital copyright works, the drafting of the DMCA evidences Congressional intent to protect some other legitimate interests in digital copyright works. The legislation contains provisions that exempt persons from DMCA liability in situations involving: (a) non-profit libraries, archives, and educational institutions making copies of works for the purposes of evaluating their suitability for activities permitted by copyright law;<sup>60</sup> (b) law enforcement and other government activities;<sup>61</sup> (c) reverse engineering;<sup>62</sup> (d) encryption research;<sup>63</sup> (e) protecting personally identifying information;<sup>64</sup> and, (f) security testing.<sup>65</sup> There are also

---

<sup>58</sup> *United States v Elcom Ltd*, 203 F Supp 2d 1111, 1129 (2002).

<sup>59</sup> Electronic Frontier Foundation, *Unintended Consequences: Five Years Under the DMCA*, available at [http://www EFF.org/IP/DMCA/unintended\\_consequences.php](http://www EFF.org/IP/DMCA/unintended_consequences.php), last viewed on March 21, 2004 and on file with the author; Dan Burk, *Anticircumvention Misuse*, 50 UNIVERSITY OF CALIFORNIA LOS ANGELES LAW REVIEW 1095, 1135 (2003) (legislative aims behind the drafting of the DMCA were to prevent 'piracy' in digital works).

<sup>60</sup> 17 U.S.C. § 1201(d).

<sup>61</sup> 17 U.S.C. § 1201(e).

<sup>62</sup> 17 U.S.C. § 1201(f). Reverse engineering has been associated with fair use doctrine prior to the enactment of the DMCA, at least in American jurisprudence: *Sega Enterprises v Accolade, Inc*, 977 F 2d 1510 (9<sup>th</sup> Cir. 1993) (decompilation of a computer program to create a compatible non-infringing program is a fair use); *Atari Games v Nintendo of Am.*, 975 F 2d 832, 842 (Fed. Cir. 1992) (decompilation to produce a non-infringing game would be a fair use, but in this case the program created was 'substantially similar' to the defendant's program); LEAFFER, *supra* note \_\_\_, 450-452 (general discussion of reverse engineering and fair use in the software context). However, as demonstrated *infra*, it is not clear that fair use is a defense to a DMCA infringement claim, as distinct from a copyright infringement claim, so the 'reverse engineering' defense under the DMCA potentially has some real work to do on the face of the legislation as currently drafted: Dan Burk, *Anticircumvention Misuse*, 50 UCLA L REV 1095, 1137-1138 (2003) (DMCA makes no explicit provision for fair use with regard to the anticircumvention right itself, as distinct from the copyright in the underlying work); *Universal City Studios, Inc v Reimerdes*, 111 F Supp 2d 292, 322, 323-324 (S.D.N.Y. 2000); *aff'd* 273 F 3d 429 (2d Cir 2001) (fair use is not a defense to DMCA infringement).

<sup>63</sup> 17 U.S.C. § 1201(g).

<sup>64</sup> 17 U.S.C. § 1201(i).

<sup>65</sup> 17 U.S.C. § 1201(j).

the limitations on the access-control circumvention prohibition set out in the Librarian of Congress' triennial review of the operation of § 1201(a)(1) noted *supra*.<sup>66</sup>

Some of the activities protected here may overlap with fair use: for example, reverse engineering has been held to constitute a fair use in a number of copyright cases.<sup>67</sup> Most of the specific DMCA defenses are, as yet, judicially untested. There have been some concerns about their likely efficacy in practice.<sup>68</sup> However, regardless of their efficacy, the list of protected purposes does give some indication as to what Congress felt were legitimate uses of a copyright work in the digital age.

Despite the express intentions of the drafters of the DMCA to preserve such legitimate interests in accessing and using otherwise protected works, the legislation has been judicially interpreted in a manner that chills innovation and stifles certain legitimate interests in copyright works. The best way to illustrate the tensions currently arising in American law in relation to the balance of rights and interests in digital content is to examine some of the case law interpreting the DRM-related provisions of the DMCA. The focus is on some of the more 'straightforward' applications of the DMCA's anti-circumvention and anti-trafficking provisions in cases involving obvious use of a DRM measure to prevent unauthorized access to, and use of, a digitally stored copyright work. In particular, these cases illustrate the attitude courts have taken to the preservation of fair use rights under the DMCA.

These cases, along with the drafting of the DMCA, have not gone without their critics. Most of the criticism has been directed at the overly restrictive approach taken to the protection of digital content *within the United States*. In this article, the argument is made that an overly restrictive attitude of this kind reflected in American legislation and jurisprudence can have wider ranging implications than just on the domestic copyright scene. Because we live in an increasingly globalized society, and the United States is often a first mover on issues such as the protection of digital content, American courts and legislatures need to be aware of the effect of their determinations in a broader global context. This is not necessarily a bad thing, and the United States certainly should not be blamed for bad policies voluntarily adopted by other nations. However, it is all the more

---

<sup>66</sup> 17 U.S.C. §§ 1201(a)(1)(B) - (D).

<sup>67</sup> Reverse engineering has been associated with fair use doctrine prior to the enactment of the DMCA, at least in American jurisprudence: *Sega Enterprises v Accolade, Inc*, 977 F 2d 1510 (9<sup>th</sup> Cir. 1993) (decompilation of a computer program to create a compatible non-infringing program is a fair use); *Atari Games v Nintendo of Am.*, 975 F 2d 832, 842 (Fed. Cir. 1992) (decompilation to produce a non-infringing game would be a fair use, but in this case the program created was 'substantially similar' to the defendant's program); LEAFFER, *supra* note \_\_\_, 450-452 (general discussion of reverse engineering and fair use in the software context).

<sup>68</sup> Dan Burk, *Anticircumvention Misuse*, 50 UCLA L REV 1095, 1139 (2003) (suggesting that the § 1201(f) exemption to anticircumvention liability only applies to the creation of *interoperable software* and does not extend to reverse engineering hardware or data; presumably this implies that the exemption will not save reverse engineering undertaken for the purpose of creating an interoperable tangible good that incidentally incorporates the software in question).

reason for Congress and American courts to reflect carefully on the potential long term effects of their actions both on a national level and ultimately also on a global scale.

*a. Universal City Studios v Reimerdes*

The first significant judicial interpretation of the DMCA's anti-trafficking provisions was the case of *Universal City Studios v Reimerdes*.<sup>69</sup> The major American motion picture studios had begun to market movies in DVD format. They were concerned about the ease with which this digital content could be cheaply, quickly, and near-perfectly copied by digital pirates. They thus employed a DRM measure called 'CSS' code (short for 'Content Scrambling System') to encrypt DVDs and protect them against unauthorized copying. CSS code can also be used to regionally encode digital works such as movies in DVD formats and digital video game cartridges, a fact that has some significance in the Australian case of *Sony v Stevens*<sup>70</sup> –*infra*.

Prior to the *Reimerdes* litigation, the movie studios had made agreements with manufacturers of DVD players for those manufacturers to incorporate software code into DVD players that would enable them to decrypt the CSS code and play a protected DVD. However, the decryption software would not allow copying of DVD content, only playing a DVD. Shortly after releasing DVDs into the market, a decryption algorithm for the CSS code was invented by a Norwegian teenager as part of a high school science project. The decryption code was called 'DeCSS'. Eventually, the DeCSS code made its way to the United States via the Internet, and became widely available to those who wished to be able to decrypt, and therefore copy, DVDs marketed by motion picture studios in the United States.

The movie studios were obviously concerned about the impact this would have on their ability to profit from marketing DVDs. They were unable to take direct action against the student in Norway who invented DeCSS because he was not within the jurisdiction of the United States and, in any event, the decryption activities he engaged in took place before the effective date of the DMCA.<sup>71</sup> It was also unwieldy for the motion

---

<sup>69</sup> 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd Universal City Studios v Corley*, 273 F.3d 429 (2nd Cir. 2001).

<sup>70</sup> [2002] FCA 906 (26 July 2002), available at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 14, 2004. This decision was overturned in part on appeal to the full federal court: see *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003), available at <http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/157.html>, last viewed on July 14, 2004.

<sup>71</sup> However, the Motion Picture Associate of America ("MPAA") later apparently brought pressure to bear on Norwegian authorities to prosecute Jan Johansen who decrypted CSS under Norwegian criminal law upon attaining the age of majority in Norway. He was eventually acquitted of all criminal charges. See discussion in Electronic Frontier Foundation, "Norwegian Teenager Jon Johansen Acquitted in DVD Case: Legal to Descramble his DVDs on Linux Computer in Norway", available at [http://www.eff.org/IP/Video/DeCSS\\_prosecutions/Johansen\\_DeCSS\\_case/20030107\\_eff\\_pr.html](http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20030107_eff_pr.html), last viewed on July 23, 2004. This is direct evidence of the impact United States digital copyright policy can have on the international scale.

picture studios to attempt to proceed against individuals who may have downloaded the DeCSS code from the Internet and used it to decrypt and copy DVDs. It would be difficult to identify such prospective defendants, and to gather necessary evidence against each of them individually. In any event, it may have been assumed that much of the individual private copying of DVDs could be justified under the fair use doctrine.

Thus, the studios proceeded against the operators of a computer hackers' website that both posted the DeCSS code and encouraged others to download and use it, as well as providing links to other websites that contained copies of the DeCSS code for download. The case proceeded on the basis that the operators of the website had trafficked in a device (the DeCSS code) that had no significant purpose other than to circumvent a copy-protection measure. The movie studios were successful in obtaining injunctions against the operators of the hackers' website containing the DeCSS code. The injunctions prevented the website operators from including the code on their website. It also required them to remove hyperlinks to other websites where the DeCSS code was available for download.

The defendants raised arguments based on the First Amendment to the effect that software code (such as the DeCSS code) is protected speech, and any legislation impeding the dissemination of this code is an unjustified restriction on speech. They also argued that the fair use doctrine from copyright law is a constitutionally protected right based on the First Amendment. They were unsuccessful on both counts. The court, both at first instance and on appeal, held that although software code does have an expressive component that may be protected as First Amendment speech,<sup>72</sup> the DMCA satisfied the 'intermediate scrutiny' test developed for content-neutral regulation of such expression.<sup>73</sup> Further, and more importantly for the purposes of this discussion, the appeal court noted that the Supreme Court has never held that the fair use doctrine is constitutionally guaranteed, even though previous cases have referred to it as being part of the balance between copyright law and free speech.<sup>74</sup>

In respect of fair use, the court also made the point that the defendants could not, in any event, avail themselves of the defense because they were not engaging in fair uses of copyright works, even if their conduct involved in part the dissemination of circumvention tools to enable others to make fair use of works. The court noted that the express legislative preservation of the fair use defense in the DMCA<sup>75</sup> said nothing about

---

<sup>72</sup> *Universal City Studios v Corley*, 273 F.3d 429, 447 (2nd Cir. 2001) ("Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance on an electric guitar").

<sup>73</sup> *id.*, at 455 ("a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective . . . . It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests"); 459-460 (affirming lower court judgment, including injunctions on dissemination via linking of DeCSS code).

<sup>74</sup> *id.*, at 458 ("the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement.")

<sup>75</sup> 17 U.S.C. § 1201(c)(1).

rights to circumvent a digital lock, or to traffic in a device that could circumvent a digital lock for the purposes of making a fair use. In this context, the appeal court noted that § 1201(c)(1): “simply clarifies that the DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred.”<sup>76</sup> In other words, the DMCA should be read to ensure that fair uses of a copyright work are not prohibited just because the information was originally obtained in a manner made illegal by the DMCA.<sup>77</sup>

Judge Kaplan at first instance had responded to the suggestion that he should not grant an injunction because it would be like ‘locking the barn door after the horse has bolted’.<sup>78</sup> He took the view that to conclude that an injunction should not be granted on this basis would effectively: “create all the wrong incentives by allowing defendants to continue violating the DMCA simply because others, many doubtless at defendants’ urging, are doing so as well.”<sup>79</sup> This would create incentives for defendants to: “ensure that others engage in the same unlawful conduct in order to set up the argument that an injunction against defendants would be futile because everyone else is doing the same thing.”<sup>80</sup> While acknowledging that equity should not act to grant a remedy where a controversy has become moot,<sup>81</sup> Judge Kaplan was apparently more troubled that a defendant could possibly destroy a valuable intellectual property right by posting circumvention measures on the Internet.<sup>82</sup>

In fact, more recent events suggest that this question itself may be moot. The movie studios, and other digital content industries, have continued relentlessly enforcing their rights under the DMCA as well as copyright law more generally in the digital age, regardless of the impact this might have on fair use. Two more recent cases on the DMCA, one involving criminal sanctions against a foreign corporation, arose in the wake of the *Reimerdes* litigation. Further, the music industry has continued to litigate against

---

<sup>76</sup> *Universal City Studios v Corley*, 273 F.3d 429, at headnote 5 (2nd Cir. 2001).

<sup>77</sup> *id.*

<sup>78</sup> *United City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 344 (S.D.N.Y. 2000).

<sup>79</sup> *id.*

<sup>80</sup> *id.*

<sup>81</sup> *id.*

<sup>82</sup> *id.*

online services that allow digital music filing sharing,<sup>83</sup> and has increasingly threatened individual file sharers with legal action.<sup>84</sup>

None of this is to say that digital content industries do not have every legal right to protect their copyright works in the online world. However, these developments do show that concerns about the ineffectuality of injunctions under laws like the DMCA are now moot. The digital content industries appear to be more than adequately able to use even the threat of litigation, based on some powerful judicial precedents, against those who would impinge on their actual or perceived rights. In spite of this, little legislative or judicial thought has been given to methods for more effectively protecting legitimate interests in digital copyright works that have not been expressly authorized by a copyright holder.

***b. United States v ElcomSoft Ltd***

The *Reimerdes* decision was followed by two federal court decisions involving similar factual situations. Each of the following cases came up with similar results to the *Reimerdes* courts. One of the cases involved the motion picture industry for a second time, and the other involved Adobe's digital eBook format. The eBook case was decided by the United States District Court for the Northern District of California, San Jose Division in 2002. It followed an unusual series of events involving the Adobe eBook formatting software, and the activities of a Russian Corporation, Elcom Ltd, and one of its employee computer programmers, Dmitri Sklyarov. Sklyarov and Elcom were the first software developers to be prosecuted under the criminal provisions of the DMCA.<sup>85</sup> This is a good example of the direct impact that domestic copyright anti-piracy laws can have in the international arena. Neither the initial defendant (Sklyarov), nor the ultimate defendant (Elcom), were present in the United States when the conduct in question occurred. However, the powerful DMCA sanctions were able to reach out to the Russian defendant and his employer, partly because of a chance visit by Sklyarov to the United States to attend an information technology conference.

The eBook format under consideration in this case was able to be used by online book publishers and distributors to limit the uses a purchaser could make of an eBook: for example, the format could be set for a purchaser to read the book on one computer, but not to copy it to another computer, or perhaps to read the book on a computer screen, but not to be able to print it out in hard copy. Elcom and Sklyarov developed software that could disable these restrictive features of Adobe's proprietary eBook format. Their

---

<sup>83</sup> See, for example *MGM Studios v Grokster*, 380 F.3d 1154 (2004), appealed to the United States Supreme Court.

<sup>84</sup> See Electronic Frontier Foundation, "File Sharing: It's Music to Our Ears", available at <http://www.eff.org/share/>, last viewed on 23 July 2004 (links to status of actions brought my music industry in the United States against consumers online)

<sup>85</sup> See discussion at Electronic Frontier Foundation, "US v. ElcomSoft & Sklyarov FAQ", available at: [http://www.eff.org/IP/DMCA/US\\_v\\_Elcomsoft/us\\_v\\_sklyarov\\_faq.html#ChargedWith](http://www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html#ChargedWith), last viewed on July 14, 2004.

software would enable activities not authorized by the original publisher/distributor of an eBook. The product developed by Elcom was called the Advanced eBook Processor (“AEBPR”).

The ability to use AEBPR to convert a restricted eBook file into a standard .pdf file capable of being copied and printed could enable purchasers of eBooks to engage in fair uses of legitimately purchased eBooks without infringing standard copyright law. It was assumed in the litigation that fair use allows a purchaser of an eBook to read an eBook on a different computer to the one it was originally downloaded on, to make a back-up copy of the eBook, or to print a hard copy of an eBook.<sup>86</sup> However, AEBPR could also allow a user to engage in a copyright infringement by making and distributing unlawful copies of an eBook.<sup>87</sup>

The course of events leading to the ultimate decision in *United States of America v Elcom Ltd*<sup>88</sup> commenced with the arrest of Sklyarov when he attended a computer science conference in Las Vegas in 2001. He was detained by American authorities between July 16 and December 13 of 2001. He was charged with five counts of violating American law, including four counts alleging circumvention offenses and aiding and abetting circumvention offenses, under the DMCA, along with a charge of conspiracy to traffic in a circumvention program. He faced up to 25 years in prison and a fine of up to \$2,250,000. His employer, Elcom, faced a penalty of \$2,500,000. He was eventually released from custody and allowed to return to Russia as part of an agreement that he would testify in the criminal case against his employer, and that criminal charges against him personally would ultimately be dropped.<sup>89</sup>

In the ensuing litigation, Elcom was found guilty with respect to all the charges against it. Similar arguments were raised by the defense as in the *Reimerdes* case, including arguments that the DMCA was constitutionally invalid under the First Amendment to the United States Constitution, and that the decryption technology in question (AEBPR) was able to be used by purchasers for fair use purposes which were protected by the First Amendment. These arguments were rejected for similar reasons to those upheld in *Reimerdes*. Elcom was ultimately acquitted by a jury on the basis that it did not mean to violate the law.<sup>90</sup> However, its AEBPR product was held to be illegal.

---

<sup>86</sup> See *United States v Elcom*, 203 F Supp 2d 1111, 1118-1119 (2002).

<sup>87</sup> *id.*, 1119.

<sup>88</sup> 203 F Supp 2d 1111 (2002).

<sup>89</sup> See Electronic Frontier Foundation, “US v. ElcomSoft & Sklyarov FAQ”, available at: [http://www.eff.org/IP/DMCA/US\\_v\\_Elcomsoft/us\\_v\\_sklyarov\\_faq.html#Status](http://www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html#Status), last viewed on July 14, 2004.

<sup>90</sup> Bowman, *ElcomSoft Verdict: Not Guilty*, available at: <http://news.com.com/2100-1023-978176.html>, last viewed on July 14, 2004. Interestingly, the defense in the *Elcom* case ran the argument that the DMCA was unconstitutional for being too vague in terms of what conduct was deemed to be illegal. This argument was also unsuccessful.

The court made some telling observations about the DMCA and fair use that go to the heart of the argument made here in favor of an administrative mechanism to facilitate fair uses of protected copyright works in the face of digital anti-piracy legislation. In particular, with respect to the argument that the DMCA adversely impacted on fair use rights, the court noted: “[W]ith regard to the argument that fair use rights are impaired [by the DMCA], the DMCA does not eliminate fair use or substantially impair the fair use rights of anyone. Congress has not banned or eliminated fair use and nothing in the DMCA prevents anyone from quoting from a work or comparing texts for the purpose of study or criticism. The fair user may find it more difficult to engage in certain fair uses with regard to electronic books, but nevertheless, fair use is still available.”<sup>91</sup>

The court here expressly accepts that digital technology does have an impact on fair use in that it may now be practically more difficult for a potential fair user to exercise her fair use right or privilege in the face of DRM measures applied to a work. Additionally, the court implicitly suggests that the DMCA is effectively neutral on this point. In other words, the DMCA neither hinders nor assists the fair user. However, this point is debatable. A law that bolsters the ability of a copyright holder to utilize restrictive DRM measures to disable access to, and particular uses of, a copyright work might arguably be described as a law that does adversely impact on fair use. Even if the DMCA does not ‘ban or eliminate’ fair use as the court suggests, it seems to have a significant impact here.

It could be argued that the *Reimerdes* and *Elcom* courts were incorrect not to read more significance into § 1201(c)(1) of the DMCA – the section that expressly preserves fair use in the face of the new anti-circumvention provisions. There have certainly been recent efforts to clarify this issue through new legislation that would guarantee the right of a user of a work to circumvent a DRM measure, or even to be involved in trafficking in a circumvention device, to make a fair use of a copyright work.<sup>92</sup> Both the Digital Choice and Freedom Bill<sup>93</sup> (‘DCFA’) and the Digital Media Consumers’ Rights Bill (‘DMCRA’),<sup>94</sup> if enacted by Congress, would allow circumvention and trafficking in a circumvention device where the resulting circumvention was excused by the fair use defense, among other things.<sup>95</sup>

---

<sup>91</sup> *United States v Elcom*, 203 F Supp 2d 1111, 1134-1135 (2002).

<sup>92</sup> See following discussion for similar initiatives under recent amendments to the Copyright, Designs and Patents Act (Eng.), 1988.

<sup>93</sup> Digital Choice and Freedom Act of 2003, H.R. 1066, 108<sup>th</sup> Cong. (2003).

<sup>94</sup> Digital Media Consumers’ Rights Act of 2003, H.R. 107, 108<sup>th</sup> Cong (2003).

<sup>95</sup> Digital Media Consumers’ Rights Act of 2003, H.R. 107, 108<sup>th</sup> Cong., § 5(b) (2003) (allowing circumvention of a technological protection measure if it does not result in a copyright infringement); Digital Choice and Freedom Act of 2003, H.R. 1066, 108<sup>th</sup> Cong., § 5 (2003) (allowing circumvention and/or trafficking in a circumvention device for purposes of making a non-infringing use of a copyright work in certain circumstances).

Like the suggestions made in this article for better supporting fair uses of digital copyright works through an administrative complaints procedure, the scheme of both the DCFA and the DMCRA in this respect appears to elevate fair use into a constitutionally guaranteed right, or to implicitly accept that fair use has always had that character. However, a significant problem with these legislative initiatives is that they do not impose any affirmative duties on copyright holders to facilitate access to, and use of, protected copyright works for fair use purposes. Again, they rely on the availability of circumvention devices for those who wish to make fair uses of copyright works. If litigation continues along the *Reimerdes* and *Elcom* path, such devices may well not be available to potentially legitimate users of copyright works.

It seems that the balance between the proprietary rights of digital content holders and those with competing interests in proprietary information is currently becoming eroded. Courts, in their efforts to uphold Congress' intention to prevent digital piracy, are increasingly opting to promote only the most difficult and old-fashioned methods of copying in order for an individual to make fair use of a work.<sup>96</sup> Additionally, courts have not found that there is any obligation on a right-holder to make any copyright work accessible in the first place in order for a fair use to be made of it. In other words, most of the judicial discourse to date in the United States has focused on *use*, rather than *access*, despite the fact that DRM measures prohibiting access and use are often merged in practice.<sup>97</sup> This may be a valid judicial approach given the current drafting of the DMCA. However, this being the case, it may be time for a new approach.<sup>98</sup> A number of different options might work here, and many have already been tried in the United States, including the triennial review of the operation of the DMCA by the Librarian of Congress. However, for reasons described below, a simple and inexpensive administrative complaints procedure tailored towards protecting individual fair use interests in copyright works, supported by appropriate legislation, may be a more useful solution.

### *c. 321 Studios v MGM Studios*

The case of *321 Studios v MGM Studios*<sup>99</sup> does not add a significant amount to the previous discussion of the fate of the fair use doctrine in the face of DRM technologies bolstered by the DMCA. However, it is a more recent case than the previous cases and

---

<sup>96</sup> For example, transcribing a passage of an eBook by hand, rather than making a digital copy, in the absence of access to digital decryption technology that would allow electronic 'cutting and pasting' for fair use purposes.

<sup>97</sup> R Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH LJ 619, 621 (2003).

<sup>98</sup> *id.*, at 657-665 (suggesting some possible legislative approaches to the current problems of merged access and control measures).

<sup>99</sup> 307 F Supp 2d 1085 (2004).

shows that the worrying trend of losing focus on fair use in the battle against digital copyright piracy is continuing along the same lines. This case, like *Reimerdes*, involved a defendant trafficking in DVD circumvention software with respect to the CSS code employed by the motion picture industry in marketing its DVDs. The defense raised similar arguments to those raised in *Reimerdes* and *Elcom* and was similarly unsuccessful. The Court unsurprisingly held that creating and marketing products that enable fair use of a digital copyright work will infringe the DMCA if they can be used to circumvent a DRM measure. The court noted that there is no clear authority that fair use is a constitutionally guaranteed right.<sup>100</sup> In any event, fair use is not a defense to a DMCA infringement claim.

The main factual point of distinction between this case and *Reimerdes* is that 321 Studios marketed and sold software products for copying DVDs with a particular emphasis on purchasers making fair uses of legitimately purchased DVDs with their software, including enabling back-up copies to be made. 321 Studios sought declaratory relief in part on the basis that their software had substantial non-infringing uses. However, this argument met the same fate as similar arguments in *Elcom* and *Reimerdes*. The court again took the view that the DMCA does not restrict fair use, and that prohibiting trafficking in circumvention technologies does not impinge on the ability to make fair use of a copyright work.

The court in *321 Studios* made some reference to the difficulty of increasingly ‘merged’ access and copy control measures, accepting that some DRM measures effectively control access and thus do technically restrict a potential fair user’s ability to access a copyright work in order to make a fair use of it.<sup>101</sup> However, the court noted that, on the facts in *321 Studios* at least, the purpose of the access control employed by the movie studio plaintiffs was to prevent *copying* even though it incidentally prevented *access*. Thus, it was validly protected by § 1201(b)(1) of the DMCA. Again, this is an example of how the technical merger of access and copy control measures leads to situations where applying the DMCA as currently drafted impinges in an undesirable way on fair use in copyright law.

Some of the most obvious points of concern about the DMCA and judicial determinations involving its anti-trafficking provisions relate to the balance between protection of proprietary interests in digital copyright works and other legitimate interests in digital copyright works. The fate of the fair use doctrine in these determinations is particularly noteworthy, including the fact that it has not generally been regarded as a legally guaranteed right by courts interpreting the DMCA. Additionally, confusions about the distinction between DRM measures on *access* and *use* of digital copyright works appear to be leaving some potential fair users out in the cold. Although there is technically no ban on fair use under the DMCA, as the *Elcom* and *321 Studios* courts take

---

<sup>100</sup> *id.*, 1101.

<sup>101</sup> See discussion in R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?* 16 BERKELEY TECHNOLOGY LAW JOURNAL 619 (2004).

pains to point out, there is no assistance provided for potential fair users who cannot *access* a work as a result of a DRM measure. There is certainly no provision in the DMCA as currently drafted that copyright holders must facilitate *access* to digitally encrypted works for people who wish to make fair uses of those works.

This is an area where the legal systems in the United States and other jurisdictions need to start being more proactive if an appropriate balance of interests is to be struck with respect to the access and use of digital copyright works. Some legislative initiatives have commenced in this direction, most notably the current triennial review of the DMCA by the Librarian of Congress, and the proposed DCFA and DMCRA measures described *supra*. Other countries are experimenting with different approaches to facilitating fair use of digitally encrypted works. The United Kingdom has recently adopted an interesting variation on the idea of an administrative complaints procedure to promote fair uses of such works – see *infra*.

How successful these initiatives ultimately become in practice remains to be seen. The new British regulations remain untested and may prove costly and unwieldy to implement.<sup>102</sup> Obviously, laws in the digital copyright area should be aimed at encouraging, rather than stifling, innovation. Laws that effectively prohibit all unauthorized access, and therefore use, of digital copyright works will miss the mark here because of their potential to damage society and innovation. However, it has been difficult to see what the alternatives could be, particularly with the digital content industries so focused on regulating *technologies* that could be used to injure their copyright interests. Thus, the answer may be to take the protection of fair use interests *away* from attempts to prevent digital copyright piracy, and to preserve fair use in other ways, rather than as legislative ‘carve-outs’ to the operation of anti-circumvention technology laws. An administrative approach such as that suggested in this article might provide a more sophisticated and nuanced solution to the DRM dilemma that meets the overall needs of the digital information society in terms of balancing competing interests in digital copyright works, while at the same time leaving undisturbed the existing digital copyright anti-piracy laws.

## 2. CRITIQUE OF THE TRIENNIAL ADMINISTRATIVE REVIEW MECHANISM

Before turning in more detail to some of the alternative approaches to protecting legitimate uses of copyright works in the face of DRM technology and anti-piracy legislation, it is worth briefly critiquing the triennial review procedure in the DMCA. As noted *supra*, the triennial review is intended to exempt certain classes of copyright works from the operation of the anti-circumvention provisions of the DMCA as they relate to individual *access to* a protected work.<sup>103</sup> In other words, the relevant provisions do not exempt any activities related to circumventing a *copy control* measure applied to a

---

<sup>102</sup> See *infra*.

<sup>103</sup> 17 U.S.C. § 1201(a)(1)(B)-(D).

copyright work, nor do they exempt trafficking in any anti-circumvention devices, whether those devices circumvent access or copy control measures, or both.

The triennial review, while useful in its own way, is not a sufficient measure to fully address the DRM dilemma identified in this article. The review does not effectively facilitate fair use of digitally encrypted copyright works in a manner appropriate to the needs of the digital information society. As with the above criticisms of the DCFA and the DMCRA draft legislation, there are no affirmative duties placed on copyright holders under the triennial review mechanism to facilitate fair use. Although certain individuals could argue, in light of a determination by the Librarian of Congress, that the DMCA's anti-circumvention provisions do not apply to their *accessing* a given work, such an individual is given no additional legal support to require that a copyright holder make access available. Assuming that the copyright holder is not prepared to make access available, the potential fair user may not personally have the technological sophistication to circumvent a relevant access-control measure herself. She may further not be able to gain the technological means to circumvent the access-control measure because the anti-trafficking provisions still apply in full force to effectively restrict the availability of devices that can circumvent both access-control and copy-control measures.

Further, the triennial review procedure does not deal with exemptions from *copy-control* technology. Thus, to the extent that an access-control measure is not merged with a copy-control measure applied to a particular work, the ability of an individual to gain access to the work by circumventing the access-control measure does not assist the individual in making a copy for fair use purposes. Such purposes may include creating a limited number of copies for classroom use or for distribution to members of a research team.

The triennial review mechanism is also not particularly timely in responding to concerns of potential fair users in the digital information society. Despite the exponentially fast pace of technological developments in digital content areas, the review is only conducted every three years, and the Librarian of Congress, at least to date, seems to be taking a fairly conservative stance on the number and type of exemptions ordered in any given review period.<sup>104</sup> In addition, the recommendations made are not specifically tailored to individual fair user's needs, but focus instead on classes of works that should be exempted from DMCA protection. By definition, this will tend to make the determinations much narrower than they might be if the Librarian of Congress was asked to focus on *uses* of protected works more generally, rather than on potential uses of *specific classes of works*.

If the administrative determinations are drafted in terms of classes of *works*, rather than classes of *uses* more generally regardless of the class of work involved, the

---

<sup>104</sup> Only four minor exemptions were made in the initial 2003 review of the operation of the anti-circumvention provisions, despite the fact that representations were made to the Registrar of Copyrights and the Librarian of Congress in relation to a number of other classes of works: see Library of Congress, *Copyright Office; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, available at <http://www.copyright.gov/fedreg/2003/68fr2011.html>, last viewed on April 13, 2005.

administrative decision-makers are much more likely to defer to copyright interests. This is because, faced with the choice of exempting an entire class of works from anti access protection, the Librarian of Congress is much more likely to protect the property rights holder by limiting orders to more obscure or obsolete works<sup>105</sup> so as not to discourage innovations in the copyright area. If a potentially expansive, new, or innovative class of works were targeted for exemption by public interest groups, this would likely be regarded by the Librarian of Congress as having extremely damaging consequences in a relevant copyright industry. Thus, the Librarian would be unlikely to ultimately make a determination exempting that class of works from the provisions of § 1201(a)(1)(A).

The administrative complaints procedure advocated in this article, on the other hand, focuses on protecting individual *uses* of copyright works regardless of the type of work. This has the potential to be better tailored to the specific needs of individuals in society. It is a more sophisticated and nuanced approach than the triennial review mechanism, even though it does place additional burdens on copyright holders that are not imposed under the current administrative mechanism. As noted *supra*, given the current tilting of the balance of copyright interests in favor of the rights-holders and away from those who would traditionally be able to access and use relevant works for fair use purposes, this may, in fact, be a desirable development. Further, the additional burdens placed on copyright holders are unlikely to be particularly onerous or unwieldy in practice given the actual nature of the obligations and the fact that copyright holders currently hold the technological know-how to make access of works available to certain people for particular stated purposes without going to any great efforts in terms of time and cost. This argument is taken up in more detail *infra*.

## II. RE-ALIGNING COMPETING INTERESTS IN DIGITAL COPYRIGHT WORKS: THE GLOBAL DIMENSION

### A. DRM LEGISLATION IN AUSTRALIA

#### 1. THE FRAMEWORK OF THE AUSTRALIAN LEGISLATION

The DRM dilemma is not peculiar to the United States. Although the federal Congress was the first legislature to enact DRM-supporting legislation in the guise of the DMCA, other countries soon followed suit. As each relevant country has enacted a new iteration of DRM-supporting legislation, more thought appears to have been given to the place of fair use in the digital copyright arena. The Australian and British legislation enacted in 2000 and 2003 respectively are good examples of this iterative development. The main problem with the approaches that have been developed so far is that none of them seems sufficiently nuanced to effectively deal with the DRM dilemma without imposing significant burdens on potential fair users. This is why a new approach is suggested here. If the United States were to adopt such an approach, it could be a world leader in redressing the balance of interests in digital copyright works. Further, it could

---

<sup>105</sup> This is arguably what happened in the initial 2003 review. *See id.*

prevent being relegated to following the lead of an approach developed in another country that may be looking at the issue more closely than is currently the case in the United States.<sup>106</sup>

Fairly soon after the enactment of the DMCA in the United States, the Australian federal parliament enacted the Copyright Amendment (Digital Agenda) Act. This legislation came into effect in September of 2000. Amongst other things, it inserted a new § 116A into the Australian copyright act of 1968. The new section is drafted somewhat differently to the DMCA, but is intended to achieve similar results. Section 116A(1) sets out the prohibited conduct in terms related to making, trading in, distributing, exhibiting, or importing a device that can circumvent a technological protection measure attached to a copyright work.<sup>107</sup> Section 116A(1)(c) includes a requirement that the defendant knew, or ought reasonably to have known, that the device in question would be used to circumvent, or facilitate the circumvention of a technological protection measure.

Exemptions from liability include: (a) activities lawfully done for the purposes of law enforcement or national security;<sup>108</sup> (b) supply of a circumvention device to a person for use for a 'permitted purpose';<sup>109</sup> and, (c) making or importing of a circumvention device solely for a permitted purpose.<sup>110</sup> 'Permitted purpose' is not defined in the legislation, although § 116A(3)(b)(v) contemplates that for the purposes of giving statutory notice to a supplier of a circumvention device the permitted purpose in question must be identified by reference to certain delineated sections of the copyright act.<sup>111</sup>

---

<sup>106</sup> This has certainly been a matter of concern in the United States with respect to *sui generis* database protection legislation. The United States did not act on this issue before the European Union Member States implemented the provisions of the E.U. Database Directive. This means that the United States now has to deal with the growing body of law on database protection in the European Union in formulating its own future proposals in the area because of the global reach of the issue. For a discussion of the relationship between the European Union approaches to database protection and some of the previous discussions in the United States, see Jacqueline Lipton, *Balancing Property Rights and Public Policies: Reconceptualizing Property in Databases*, 18 BERKELEY TECHNOLOGY LAW JOURNAL 773 (2003).

<sup>107</sup> 'Technological protection measure' is defined in § 10 as comprising an access control measure, a copy control measure or both.

<sup>108</sup> Copyright Act (Australia), 1968, § 116A(2).

<sup>109</sup> *id.*, § 116A(3).

<sup>110</sup> *id.*, § 116A(4).

<sup>111</sup> *id.*, §§ 47D, 47E, 47F, 48A, 49, 50, 51A, 183 and Part VB. None of these sections deals with traditional fair uses of a copyright work. Those uses are covered (as 'fair dealing' exemptions to copyright infringement) under sections 40 to 42 of the Copyright Act.

These sections do *not* include the general ‘fair dealing’<sup>112</sup> sections that are found in the copyright legislation.<sup>113</sup>

They do include sections that mirror some of the exemptions found in the DMCA: for example, reverse engineering computer software to create interoperable products,<sup>114</sup> to fix errors,<sup>115</sup> and for security testing purposes,<sup>116</sup> as well as certain uses of material for governmental purposes,<sup>117</sup> and certain uses by libraries and archives.<sup>118</sup> Thus, like the DMCA, there appears to be no general fair use exemption contemplated to the operation of the prohibitions on circumventing technological protection measures and/or trafficking in devices that facilitate such circumventions. However, there are some legitimate or ‘permitted’ purposes that, in some ways, resemble things that have been considered to be aligned with fair use doctrine in the past.<sup>119</sup>

The exemptions to § 116A liability are limited in their operation. The exemption for supplying a circumvention device to a person for a permitted purpose requires that the person to whom the circumvention device or service is supplied be a ‘qualified’ person.<sup>120</sup> Additionally, the person must give the supplier a signed declaration stating her name and address,<sup>121</sup> the basis on which she is a qualified person,<sup>122</sup> the name and address of the supplier of the circumvention device,<sup>123</sup> that the device in question is to be used only for a permitted purpose by a qualified person,<sup>124</sup> identifying the permitted purpose by reference to one of the relevant sections of the copyright act,<sup>125</sup> and, stating that the

---

<sup>112</sup> ‘Fair dealing’ is the Australian equivalent terminology to the American ‘fair use’ concept. The ‘fair dealing’ terminology is also employed in British copyright law.

<sup>113</sup> §§ 40-42 of the Copyright Act, 1968 (Aust.).

<sup>114</sup> § 47D.

<sup>115</sup> § 47E.

<sup>116</sup> § 47F.

<sup>117</sup> § 48A.

<sup>118</sup> §§ 50, 51.

<sup>119</sup> Such as reverse engineering of software – see note \_\_\_ *supra*.

<sup>120</sup> § 116A(3)(a). ‘Qualified person’ is defined in § 116A(8) with reference to statutory permissions to make interoperable products, to engage in security testing and / or to correct errors in a digital work, or who has authority to make a permitted use of a work from various listed government departments.

<sup>121</sup> § 116A(3)(b)(i).

<sup>122</sup> § 116A(3)(b)(ii).

<sup>123</sup> § 116A(3)(b)(iii).

<sup>124</sup> § 116A(3)(b)(iv).

<sup>125</sup> § 116A(3)(b)(v).

work in question is not readily available in a form that is not protected by a technological protection measure.<sup>126</sup>

These requirements may be difficult to fulfil in some circumstances. If, for example, a circumvention device is downloaded from a website, there may be no way to identify the supplier and her contact details for the purpose of sending the statutory notice. Of course, this may be what the legislature had in mind. The idea is presumably to encourage people who wish to circumvent a DRM measure for a permitted purpose only to obtain a circumvention device from a reputable supplier who can be easily identified and contacted in the case of a dispute about the device or circumvention activities conducted using the device.

Additionally, it may be difficult for a person to ascertain whether or not the work in question is readily available in a form that is not protected by a technological protection measure. There is no guidance in the legislation as to how much effort a person would be required to go to in order to ascertain that the work is not otherwise readily available: for example, would a 20 minute Internet search and a few phone calls suffice here? How does a defendant satisfy this test? What evidence needs to be adduced to show that the material was not otherwise readily available to the defendant? Overall, like the DMCA, additional burdens are imposed here on people seeking to make fair uses of a copyright work. Given the imbalance of resources between digital content owners and people likely to want to make legitimate uses of a digital work (researchers, educators etc), it would seem that perhaps a more appropriate balance would involve placing greater burdens on a copyright holder to facilitate the exercise of these kinds of interests.<sup>127</sup>

In relation to the exemption for making or importing a circumvention device solely for a permitted purpose, this may at first glance appear to be an improvement on the DMCA in that it allows making or importing of circumvention devices in certain circumstances. However, on a closer reading, it may operate as restrictively as the DMCA in practice. The DMCA prohibits trafficking in a circumvention device: (a) that is primarily designed to circumvent an access or copy control measure;<sup>128</sup> (b) that has only limited commercially significant use or purpose other than to circumvent an access or copy control measure;<sup>129</sup> or, (c) that is marketed specifically for the purpose of circumventing an access or copy control measure.<sup>130</sup>

---

<sup>126</sup> § 116A(3)(b)(vi).

<sup>127</sup> See, for example, approach taken under § 296ZE of the Copyright Designs and Patents Act, 1988 (Eng.) in the United Kingdom – *see infra*.

<sup>128</sup> 17 U.S.C. §§ 1201(a)(2)(A); 1201(b)(1)(A).

<sup>129</sup> 17 U.S.C. §§ 1201(a)(2)(B); 1201(b)(1)(B).

<sup>130</sup> 17 U.S.C. §§ 1201(a)(2)(C); 1201(b)(1)(C).

Section 116A(4) takes a contrasting approach, but probably achieves similar practical results in that it exempts from liability the making or importing of circumvention devices<sup>131</sup> for use *only* for a permitted purpose where the work in question is not readily available in a form not protected by a DRM measure,<sup>132</sup> or for the purpose of enabling a person to supply the circumvention device *only* for a permitted purpose.<sup>133</sup> It may be difficult in practice for a manufacturer or distributor of a circumvention device to establish that the device is *only* used for permitted purposes relating to works that are not readily available in forms unprotected by a DRM measure.

This again evidences the crux of the DRM dilemma when legislatures try to translate into statutory language a prohibition on circumvention technologies that may have the potential to be used for both legitimate and illegal purposes. As a result of this dilemma, the Australian provisions arguably achieve the same thing in practice as the relevant provisions of the DMCA in the United States. This is because, as noted in the *Elcom* and *321 Studios* cases, devices with substantial non-infringing uses are also likely to have the potential to be used for a variety of infringing uses. The realistic choice under DMCA-style legislation seems to be between a blanket ban on all such technology that would effectively restrict any legitimate uses of a relevant work, and a ‘free for all’ that makes such technology available but does little to stem the tide of digital copyright piracy.

Importantly, we see here further evidence of the fact that blanket prohibitions or blanket permissions to market decryption devices may not work very well to protect an appropriate balance of interests in the digital age. It may be that a more nuanced case-by-case approach needs to be taken to ensure that legitimate uses are facilitated, and infringing uses are discouraged or prohibited in practice, particularly with respect to DRM measures that effectively prevent unauthorized *access* to a protected work.

It may be that asking courts to make determinations about DRM *access* measures in the same way that they have traditionally made decisions about copying technologies as they have in the past - on a ‘blanket’ basis as to whether a particular technological innovation should be banned or not - is simply not realistic in this context. If technologies like CSS code, *Elcom*’s eBook decryption format, and *Studio 321*’s decryption code are freely available to everyone, this might indeed be the ruin of some digital content industries. If, on the other hand, these technologies are not available at all,

---

<sup>131</sup> ‘Circumvention device’ is defined in § 10 of the Australian copyright act in terms that reflect the DMCA’s conception of a circumvention device (“circumvention device” in the Australian legislation means: “a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of a technological protection measure”).

<sup>132</sup> § 116A(4)(a).

<sup>133</sup> § 116A(4)(b).

it may put an unfair burden on those who should have been able to utilize them to make fair use of a relevant work. This might, in turn, stifle innovation in society.<sup>134</sup>

It may be necessary, at least in the ‘access’ context, to replace the traditional ‘blanket’ approach that focuses on *circumvention technologies* with an approach that focuses instead on an individual user’s legitimate needs in relation to a protected work. Arguably, the Australian legislation is a good first step in this direction in terms of taking an individual user’s particular interests into account. However, it places unrealistic burdens on potentially unsophisticated users of copyright works. An approach that shifts some of the burden of facilitating access to the entity making a profit from the commercialization of the work may be preferable. This does not automatically deal comprehensively with the question of when, and how, to ban or regulate particular circumvention devices. However, it ensures that restrictions on marketing such devices do not encroach unnecessarily on the exercise of fair use rights in relation to digital copyright works.

## 2. JUDICIAL INTERPRETATIONS OF THE AUSTRALIAN LEGISLATION

The first judicial determination involving § 116A in Australia was in the case of *Kabushiki Kaisha Sony Computer Entertainment v Stevens*.<sup>135</sup> This was a relatively unremarkable case in many ways as it turned out to be a fairly straightforward application of the principles enshrined in § 116A. Interestingly, the Full Federal Court on appeal overturned the first instance decision of Judge Sackville in part, but the difference of opinion turned on the definition of ‘technological protection measure’, rather than on the broader operation of the anti-circumvention provisions.

The case involved Sony’s marketing of video game CDs for its PlayStation game system. These video game CDs were encrypted with ‘access codes’. The Sony PlayStation consoles read the access codes from the CDs and only allowed authorized Sony games with valid access codes to play. Unauthorized copies would not contain the access codes, so the PlayStations would not play them. The defendant sold ‘mod chips’ (also called ‘converter chips’) which could be installed in PlayStation consoles to overcome Sony’s access device. The defendant also installed these chips into PlayStation

---

<sup>134</sup> See, for example, Mark Lemley and R Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN L REV 1345 (2004) (suggesting a dispute resolution procedure to enable copyright owners to proceed against direct infringers and thus preserve technological innovations in file sharing technologies by reducing the likelihood of contributory infringement suits against those who develop and disseminate such technologies).

<sup>135</sup> [2002] FCA 906 (26 July 2002), available at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 14, 2004. This decision was overturned in part on appeal to the full federal court: see *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003), available at <http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/157.html>, last viewed on July 14, 2004.

consoles for his customers. Sony made several complaints against him,<sup>136</sup> including a claim that he had infringed § 116A of the copyright act by supplying devices to circumvent technological protection measures.

The difference of opinion between the trial judge – Judge Sackville – and the Appeal Court was that Judge Sackville at first instance took the view that the access code on the CD games could not be regarded as a ‘technological protection measure’ as contemplated in the legislation. He felt that the definition required something more than a device which generally discouraged copying of game CDs by rendering the copies unplayable: “There seems to be nothing in the legislative history to support the view that a technological measure is to receive legal protection from circumvention devices if the only way in which the measure prevents or inhibits the infringement of copyright is by discouraging infringements of copyright which predate the attempt to gain access to the work or to copy it.”<sup>137</sup>

In other words, the access control measures incorporated into CDs and PlayStation consoles by Sony were regarded by Judge Sackville as having an insufficient link to any possible copyright infringement to be regarded as the kind of encryption measure supported by the legislation as protecting the rights of a copyright holder. He rather regarded the access control measure as a mechanism whereby Sony could ensure that only authorized versions of their games were accepted by, and played in, their consoles. However, the access control measures did nothing to prevent an unauthorized copyist from accessing or copying the video game software on a CD – they merely prevented any unauthorized copy from playing in a Sony game console. There may have been a general deterrent effect on unauthorized copying in the sense that unauthorized copies were effectively useless because they could not be played in a Sony PlayStation console, but the access control measure itself did not specifically prevent access to the game software on the CDs, or copying of the software.

The Full Federal Court overturned Judge Sackville on this point. Judge Lindgren, in particular, took pains to go through the legislative history of the 2000 amendments to the copyright act in detail. He concluded that a device that inhibits copying of a work in the sense of deterring or discouraging copyright infringement by denying access to, and therefore prevention of use of, an unauthorized copy of a software program (computer game in this case) is within the scope of the definition of ‘technological protection measure’.<sup>138</sup>

---

<sup>136</sup> These claims included general copyright infringement with respect to unauthorized reproductions of video game software in hardware components of the system, as well as trade mark infringement with respect to Sony’s trade marks incorporated into video games.

<sup>137</sup> *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2002] FCA 906 (26 July 2002), available at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 14, 2004.

<sup>138</sup> *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003), para. 138 (Lindgren J judgment) available at <http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/157.html>, last viewed on July 14, 2004.

Although the results of this decision are ultimately unremarkable, given that the defendant did appear to be engaging in activities that could have adversely impacted on Sony's Australian video game market, we again see a potentially far-reaching approach to the protection of proprietary interests in digital copyright works. We also see the judiciary being relatively deferential to content industry interests, and ultimately preferring a broad interpretation of ideas like 'technological protection measure' than a narrow interpretation. Additionally, in terms of policy, the *Stevens* case in Australia might have a general chilling effect on a variety of activities in relation to digital copyright works.

For one thing, the decision seems to support attempts by digital content industries to utilize access control measures to regionally encode digital information products to avoid undesired parallel importing.<sup>139</sup> Although the 2000 amendments to the copyright act are aimed at the prevention of digital piracy, they could likely also be used as an impediment to those wishing to engage in otherwise potentially lawful parallel importing activities<sup>140</sup> where a case can be made that the defendant has interfered with a measure that *could* have an effect on copyright infringement.

This could happen, for example, in a situation where a defendant trades in a device that could circumvent an access control measure in a Sony PlayStation in order to enable copies of authorized Sony games, lawfully purchased by a consumer, but regionally encoded for another jurisdiction, to play in a locally purchased console.<sup>141</sup> The broad interpretation of 'technological protection measure' would likely prohibit the availability of the device even where it facilitated such presumably non-infringing uses of copyright material, provided that it could also be used to deter copyright infringement in the sense described by the Full Federal Court in *Stevens*.

---

<sup>139</sup> See, for example, Alison Morr, *Hong Kong's Copyright Ordinance: How The Ban On Parallel Imports Affects The U.S. Entertainment Industry And Hong Kong's Free Market*, 21 HASTINGS COMMUNICATIONS AND ENTERTAINMENT LAW JOURNAL 393 (1999). Information property holders increasingly utilize regional encoding on digital works to prevent unauthorized parallel importing (also known as a 'gray market' in the relevant product).

<sup>140</sup> Parallel importing activities that create 'gray markets' in products are not *per se* legal or illegal. Their legality will depend on relevant circumstances and the prevailing regulatory attitudes in a relevant jurisdiction to such activities.

<sup>141</sup> It is suggested in the first instance decision in *Sony v Stevens* that the issue of regional encoding was raised but not argued fully. At para. 108 of the decision, Sackville J noted that: "There is nothing in the evidence to suggest that the major purpose or objective of the protective device, from the applicants' perspective, was to ensure that the PlayStation consoles could only play PlayStation games lawfully acquired in Australia or Europe. It may be that if the topic had been explored, the evidence would have elucidated the applicants' global marketing strategies and the role of the device in implementing those strategies. But the topic was not explored." (Full text of the decision is available at: <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 23, 2004).

The Australian legislation in general, although drafted differently to the DMCA, takes a similar approach and potentially creates a similar imbalance of interests in proprietary digital copyrights. There is little to no real protection of fair use. The statutory exemptions provided to the new prohibitions are somewhat vague and, in any event, place significant burdens on those seeking to exercise legitimate interests in digital content. Overall, Australia seems to be moving in the same direction as the United States with respect to digital content management. Like the American position, the emphasis is on blanket bans on technological devices that could facilitate unauthorized access to, or use of, a protected work. This is understandable in light of the very real concerns of digital content industries to prevent digital piracy. However, it is not in itself a sufficiently nuanced approach to protect legitimate uses of a copyright work that may not have been specifically authorized by the copyright holder. A more sophisticated approach needs to be developed that can alleviate some of the content owners' concerns while supporting the rights of those who wish to exercise legitimate uses of a copyright work.

## B. DRM LEGISLATION IN THE UNITED KINGDOM

### 1. THE EUROPEAN UNION COPYRIGHT DIRECTIVE

The United Kingdom has been more guarded in its approach to the issue of digital copyright anti-piracy legislation than the United States and Australia, and is therefore an interesting model for the purposes of this discussion. The British Parliament has been more focused on protecting an appropriate balance of competing interests in digital information products than many other legislatures. To that end, it took a long time for it to consider the potential impact of legislation it might enact in implementing the DRM-supporting provisions of the European Union Copyright Directive<sup>142</sup> and, in fact, did not enact its legislation within the time period required under the Directive.<sup>143</sup> The final British legislative package came into force towards the end of 2003 and has not yet been judicially tested. In October of 2003, the Copyright and Related Rights Regulations 2003 (UK)<sup>144</sup> (the 'CRR Regulations') came into effect. These regulations give effect to provisions of the European Union Copyright Directive<sup>145</sup> that reflect the DRM requirements of the WIPO Copyright Treaty of 1996<sup>146</sup> and the WIPO Performances and Phonograms Treaty of 1996.<sup>147</sup>

---

<sup>142</sup> Directive 2001/29 on Copyright and related rights in the Information Society [2001] OJ L1767/10.

<sup>143</sup> The original deadline for transposing the requirements of the Copyright Directive into the law of individual European Union Member States was in 2002, but several Member States, such as the United Kingdom and Germany, did not implement the Directive in a timely manner, as it took them longer to sufficiently consider the implications of the legislation they needed to draft.

<sup>144</sup> S/I 2003 No 2498.

<sup>145</sup> Directive 2001/29 on Copyright and related rights in the Information Society [2001] OJ L1767/10.

<sup>146</sup> WIPO Copyright Treaty of 1996, Art. 11.

<sup>147</sup> WIPO Performances and Phonograms Treaty of 1996, Art. 18.

Article 6(1) of the Copyright Directive provides that: “Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she pursues that objective.” “Technological measures” are defined for these purposes in Art 6(3) as: “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised [sic] by the rightholder of any copyright or any right related to copyright as provided by law...”<sup>148</sup>

Article 6(2) of the Directive provides the ‘anti-trafficking’ provisions in relation to circumvention devices. It requires Member States to:

“provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

- (a) are promoted, advertised [sic] or marketed for the purpose of circumvention of, or
- (b) have only a limited commercially significant purpose or use other than to circumvent, or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

any effective technological measures.”

The provisions of Articles 6(1) and 6(2) are mandatory and must be implemented by all European Union Member States. These provisions are tempered by Article 6(4) which requires Member States to: “take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with [provisions set out in Article 5] the means of benefiting from that exception or limitation.” However, the Article 6(4) obligation only needs to be undertaken by national legislatures to the extent necessary for the beneficiary to benefit from the relevant exception or limitation, and where the beneficiary has ‘legal access’ to the protected work in question.<sup>149</sup>

The kinds of exceptions contemplated here are set out in Article 5 and include:  
(a) reproductions of a work for private use;<sup>150</sup> (b) use by public libraries, educational

---

<sup>148</sup> Art 6(3) of the Copyright Directive further defines an ‘effective’ technological measure as a DRM measure that ‘achieves the protection objective’. This definition is obviously somewhat circular. See discussion in Jacqueline Lipton, *Copyright in the Digital Age: A Comparative Survey*, 27 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL 333, 346-347 (2001).

<sup>149</sup> See Art 6(4) Copyright Directive.

<sup>150</sup> *id.*, Art 5(2)(b).

establishments or museums;<sup>151</sup> (c) use by social institutions such as hospitals and prisons that pursue non-commercial purposes;<sup>152</sup> (d) use for scientific research;<sup>153</sup> and, (e) use for public security.<sup>154</sup> However, the provisions of Article 5 are discretionary, rather than mandatory. The form of any such measures adopted at a national level is left to the discretion of each individual Member State. This has created the potential for disharmonized implementations of exceptions to the anti-circumvention regulations amongst European Union Member States. The specific implementation decisions hinge on the attitude each national legislature has taken towards balancing proprietary rights against competing interests in relevant information.<sup>155</sup> Outside these discretionary exemptions, the Copyright Directive does nothing to guarantee any form of fair use of a copyright work protected by a DRM measure.

Prior to the implementation of the CRR Regulations in the United Kingdom in 2003, some provision had been made in the Copyright, Designs and Patents Act of 1988 [hereinafter, the ‘CDPA’] for the protection of digital copyright works through anti-circumvention prohibitions. The pre-2003 legislation in the form of the original § 296(1) of the CDPA had made provision for licensed distributors to the public of a copyright work protected by a DRM measure to bring a copyright infringement action against a person who trafficked in a device or service enabling circumvention of a copy-protection measure. However, this provision did not protect copyright holders to the same extent as the requirements of the Copyright Directive. Thus, the new CRR Regulations incorporate a much more comprehensive anti-circumvention regime into the CDPA.

## 2. THE BRITISH COPYRIGHT AND RELATED RIGHTS REGULATIONS

### a. Software Copyrights: Anti-Device Provisions

The first thing to note about the current digital copyright legislation in the United Kingdom with respect to DRM measures is that it treats software copyrights differently from other kinds of digital copyright works. This is because the Copyright Directive excludes from its operation matters already covered by the Software Directive of 1991.<sup>156</sup>

---

<sup>151</sup> *id.*, Art 5(2)(c).

<sup>152</sup> *id.*, Art 5(2)(e).

<sup>153</sup> *id.*, Art 5(3)(a).

<sup>154</sup> *id.*, Art 5(3)(e), Copyright Directive. For a more detailed survey of potential exceptions to the anti-circumvention provisions of the Copyright Directive, see discussion in CORNISH, *supra* note \_\_\_\_, at 811-812.

<sup>155</sup> See discussion in Lipton, *supra* note \_\_\_\_, at 348 [*Copyright in the Digital Age*]

<sup>156</sup> Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC). See Copyright Directive, Arts 1 and 11, and Rec. 50.

Thus, the separate treatment of software copyrights in the CRR Regulations focuses on maintaining the requirements of the Software Directive. The additional provisions of the CRR Regulations that relate to works *other than software copyrights* are a new area for digital copyright law in the United Kingdom.<sup>157</sup>

With respect to computer software copyrights, the original § 296 of the CDPA was replaced with a new § 296 inserted under the CRR Regulations. The new provision focuses on computer programs encrypted by a ‘technical device’. It sets out the rights of holders of computer software copyrights, and those authorized by right-holders to issue relevant computer programs to the public. These rights are enforceable against those who *traffic* in a device or information capable of enabling or assisting the circumvention of a ‘technical device’<sup>158</sup> applied to a computer program. There is no prohibition on *circumvention per se* with respect to computer software copyrights. There is an ‘intent’ requirement for liability in sub-section 296(1)(b) to the effect that the defendant must know or have reason to believe that the circumvention measure in which she traffics will be used to make infringing copies of copyrighted software.

There are no specific exemptions to liability set out in relation to the prohibitions contained in § 296. However, it appears to be assumed, at least by some commentators, that this section should be read subject to a number of exemptions from basic copyright liability set out in earlier sections of the CDPA.<sup>159</sup> Nevertheless, it is not particularly clear from the face of the regulations whether any exemptions are contemplated to the operation of the new § 296 prohibitions. The prohibitions only relate to trafficking in circumvention measures, rather than in acts of circumvention *per se*. Thus, it is arguable that they should not impact on exemptions relating to copyright liability for engaging in activities in relation to *copying* a copyrighted computer program such as making a back-

---

<sup>157</sup> See UK Patent Office, “Consultation on UK Implementation of Directive 2001/29/EC on Copyright and Related Rights in the Information Society: Analysis of Responses and Government Conclusions”, para. 6.4, available at <http://www.patent.gov.uk/about/consultations/responses/copydirect/article6.htm>, last viewed on July 15, 2004 (“As enacted, s.296 of the CDPA already provided protection for TPMs, whether used on computer programs or other forms of works. The consultation paper proposed to retain s.296, as amended on implementation of Directive 91/250, but in relation to computer programs only, and not other works which are now subject to Article 6 of the present Directive. This remains the intention, but in the light of comments made by parties with particular interests in computer programs, the Government has concluded that it is desirable to make some further adjustments to s.296 in order to bring its wording into closer alignment with that of Article 7(1)(c) of Directive 91/250, which it is now the sole function of s.296 to implement. These changes do not, however, alter the basic approach in s.296, and the Government has concluded that it would not be appropriate to make more substantial changes, such as the introduction of criminal sanctions in s.296 as was called for by some interested parties, particularly since the Directive now being implemented does not revisit existing provisions on computer programs.”)

<sup>158</sup> For the purposes of this provision, ‘technical device’ is defined in sub-section 296(6) as: ‘any device intended to prevent or restrict acts that are not authorised [sic] by the copyright owner of that computer program and are restricted by copyright.’

<sup>159</sup> For example, see CORNISH, *supra* note \_\_\_\_, at 810 (noting that the CRR Regulations will likely dramatically expand liability for anti-circumvention *other than in the case of computer software copyrights*).

up copy,<sup>160</sup> decompiling the program to create an interoperable program,<sup>161</sup> or observing the operation of a program.<sup>162</sup>

As with the DMCA, there is no provision allowing people who want to make such legitimate uses of copyright software to obtain the means to do so if they are not otherwise technologically able to do so. If, for example, I own a copy of a copyrighted software program and I want to make a back-up copy of the program, but the program is digitally encrypted by a ‘technical device’ that prevents copying of the program, how can I engage in my lawful right to make a back-up copy? Assuming I do not have the technological skill to circumvent the technical device myself, and manufacturers of circumvention devices ultimately stop disseminating the devices publicly because of fears of liability under § 296, there may be no viable way for me to exercise my legitimate rights to make a back-up copy of the program.

This is obviously not the legislative intention behind § 296. For one thing, the definition of ‘technical device’ is limited to a device that is intended to prevent or restrict acts not authorized by the copyright owner that are also *restricted by copyright*. Making a personal back-up copy is arguably not restricted by copyright in the United Kingdom. This is because § 50A(1) of the CDPA expressly provides that it is *not* an infringement of copyright for a lawful user of a copy of a computer program to make a back-up copy of the program for lawful purposes. The problem is that many technical encryption devices are not sufficiently sophisticated to facilitate permitted uses while disallowing non-permitted uses. Again, we see the DRM dilemma at play here. It is impossible to regulate the devices only in terms of illegal uses to which they might be put without also encroaching on the ability to use such devices for legitimate purposes. Thus, we are left with a situation where the currently available legislative tools leave courts with an ‘all or nothing’ option on these issues. Either circumvention devices must be completely banned or they must be completely unrestricted. Both are undesirable outcomes, but there is little middle ground built into the current legislation to address the dilemma. Hopefully, an administrative mechanism of the kind suggested in this article would provide some such middle ground by effectively removing fair use concerns from the ambit of the ‘anti-piracy’ regulations.

There is certainly no current legislative requirement with respect to computer software copyrights in the United Kingdom that copyright holders are obliged to provide people with legitimate interests in their software with the means to access or copy the software to make legitimate uses of the software. Such uses might include making back-up copies<sup>163</sup> or creating interoperable programs.<sup>164</sup> There is some provision in § 296A of

---

<sup>160</sup> CDPA, § 50A.

<sup>161</sup> *id.*, § 50B.

<sup>162</sup> *id.*, §§ 50BA.

<sup>163</sup> *id.*, §50A(1).

<sup>164</sup> *id.*, §50B(2).

the CDPA to override *contractual restrictions* on permitted activities in relation to computer software. Statutorily permitted activities here include making back-up copies, decompiling software to create an interoperable program, and observing the functionality of software.<sup>165</sup> However, these provisions only make an agreement purporting to prohibit a permitted act void to the extent that it prohibits or restricts a permitted act. There is no affirmative duty imposed on the software copyright holder to facilitate technical *access* for a permitted purpose. Such duties may be increasingly necessary in the digital information age due to the technological sophistication of many information property holders, and the concurrent lack of sophistication of many who wish to exercise legitimate, if unauthorized, interests in proprietary information products.

***b. Works Other than Software: Anti-Circumvention and Anti-Device Provisions***

Unlike the computer software copyright provisions in § 296 of the CDPA, the new sections relating to works *other than software* provide prohibitions on both circumvention activities,<sup>166</sup> and trafficking in circumvention devices.<sup>167</sup> Section 296ZA provides a right of action against a person who circumvents an ‘effective technological measure’<sup>168</sup> applied to a copyright work other than a computer program. Section 296ZB provides criminal sanctions for trafficking in anti-circumvention devices, while § 296ZD provides a right of action by a copyright holder or its authorized agent against a person who traffics in a circumvention device.

The basic circumvention prohibition in § 296ZA applies to a person undertaking circumvention activities while knowing, or having reasonable grounds to know, that she is pursuing a circumvention objective.<sup>169</sup> It provides for a cause of action, akin to a copyright infringement suit, by a copyright holder and anyone authorized by the copyright holder to issue copies of the relevant work to the public.<sup>170</sup> Sub-section 296ZA(2) provides exemptions for persons engaging in research into cryptography unless, in so doing, a relevant person prejudicially affects the rights of the copyright

---

<sup>165</sup> *id.*, §§ 50A, 50B, 50BA, 296A.

<sup>166</sup> *id.*, § 296ZA.

<sup>167</sup> *id.*, § 296ZB.

<sup>168</sup> The component parts of an ‘effective technological measure’ for the purposes of these provisions are defined in § 296ZF. Section 296ZF(1) defines a ‘technological measure’ as: ‘any technology, device or component which is designed, in the normal course of its operation, to protect a copyright work other than a computer program.’ Section 296ZF(2) provides that a technological measure is ‘effective’ if the use of the work in question is controlled by an access control or copy control mechanism that achieves the intended protection. For the purposes of the § 296ZF(1) definition of ‘technological measure’, sub-section 296ZF(3)(a) further defines the concept of ‘protection of a work’ as: ‘the prevention or restriction of acts that are not authorised [sic] by the copyright owner ... and are restricted by copyright.’

<sup>169</sup> CDPA, § 296ZA(1)(b).

<sup>170</sup> *id.*, § 296ZA(3).

owner. There are no general fair use or other exemptions from liability set out in the section,<sup>171</sup> although there is a governmentally assisted remedy set out in § 296ZE for situations where the operation of a DRM measure prevents certain permitted acts in relation to a copyright work other than a computer program.

Sub-section 296ZE(2) provides that where the application of an effective technological measure prevents a person from carrying out a permitted act in relation to a copyright work other than a computer program, then that person, or a person being a representative of a class of persons prevented from carrying out the permitted act, may issue a complaint to the Secretary of State. ‘Permitted act’ is defined in this context as an act that may lawfully be done in relation to a copyright work by virtue of a series of provisions of the CDPA listed in Part 1 of Schedule 5A to the CDPA. These activities include fair dealing for research and private study along with various other basic exemptions to copyright infringement relating to activities permitted by librarians and archivists, for parliamentary and judicial proceedings, and statutory enquiries.<sup>172</sup> Notably absent from the list of permitted acts are fair dealing activities related to criticism, review and news reporting purposes.<sup>173</sup>

This procedure provides the Secretary of State with a discretion to give the owner of a copyright work or an exclusive licensee of the work such directions as appear to be requisite or expedient for the purposes of: (a) establishing whether any voluntary measure or agreement relevant to the copyright work subsists;<sup>174</sup> or (b) where there is no such measure or agreement in place, ensuring that the copyright owner or exclusive licensee makes available to the complainant the means of carrying out the permitted act to the extent necessary to benefit from the permitted act.<sup>175</sup> Sub-section 296ZE(5) provides that it will be a legal duty of any person given a direction by the Secretary of State under this procedure to give effect to that direction. This duty is owed to the original complainant or each member of a class of complainants, and breach of the duty is legally actionable by such persons.<sup>176</sup> However, the procedure is only available to persons who have *lawful access* to the protected copyright work.<sup>177</sup>

---

<sup>171</sup> UK Patent Office, “Regulatory Impact Assessment”, Annex IV, p xvii (noting that no fair use exemptions are contemplated in the UK legislation or in the EU Copyright Directive), available at <http://www.patent.gov.uk/copy/notices/2003/copyria.pdf>, last viewed on July 15, 2004.

<sup>172</sup> The complete list of permitted acts referred to in Part 1 of Schedule 5A includes the following sections of the CDPA: §§ 29, 32(2), 32(3), 35, 36, 38, 39, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 61, 68, 69, 70, 71, 74, and 75.

<sup>173</sup> CDPA, § 30.

<sup>174</sup> *id.* § 296ZE(3)(a).

<sup>175</sup> *id.*, § 296ZE(3)(b).

<sup>176</sup> *id.*, § 296ZE(6).

<sup>177</sup> *id.*, § 296ZE(10).

The advantage of this approach over the approaches in the United States and Australia is that it appears to take a more pro-active stance on *balancing* competing interests in valuable copyrights, rather than focusing on protecting the interests of copyright holders at the expense of other legitimate interests in a relevant work. An attempt is made not only to protect and preserve legitimate interests in digitally encrypted copyright works, but also to give those protections some teeth with the assistance of the very government that created and strengthened the original property rights. In particular, the British legislature has been prepared to impose affirmative legal duties on copyright holders and exclusive licensees of copyright works to give effect to an administrative direction made by the Secretary of State.

The main problem with the approach as currently drafted is that the duties of the Secretary of State are somewhat vague. The Secretary of State has discretion as to whether or not to act on any given complaint.<sup>178</sup> There is thus no guarantee of governmental assistance for a complainant seeking to make a permitted use of a relevant work. Further, even though the procedure imposes an affirmative legal duty on a copyright holder or exclusive licensee to facilitate permitted uses of a particular work, there may still be practical problems of enforcement if the beneficiaries of such duties do not have sufficient financial resources to enforce the duties in legal proceedings. It might have been more effective additionally to provide some governmental assistance in taking proceedings to enforce such duties. After all, governments are increasingly proving to be willing to bring criminal proceedings against those who are accused of infringing anti-circumvention and anti-device provisions.<sup>179</sup> It would seem only fair that the same governments should be equally willing to protect their individual citizens' countervailing rights in relation to the same information products.

Section 296ZB creates an additional criminal offense relating to trafficking in an anti-circumvention device. The prohibited activities include various permutations of manufacturing, importing, distributing, advertising, or possessing a circumvention device.<sup>180</sup> Most of the specific prohibitions relate to commercial activities. Thus, possession of a circumvention device is only prohibited in the context of business activities.<sup>181</sup> Presumably, possession for personal purposes would not be prohibited.

---

<sup>178</sup> Sub-section 296ZE(3) states that the Secretary of State *may* give directions to the owner of a copyright work or an exclusive licensee to facilitate the complainant's access to / use of a relevant work.

<sup>179</sup> For example, the United States government was very pro-active in the *Elcom* case in bringing criminal proceedings against the Russian programmer and his employer under the DMCA for infringing the legal rights of an American corporation. It also encouraged the Norwegian government to take criminal action against the student who created the DeCSS code ultimately at issue in the *Reimerdes* litigation at the behest of the motion picture industry. The British legislature has been prepared to institute criminal penalties for trafficking in circumvention devices: CDPA, § 296ZB and the Australian legislature certainly did not expressly dismiss the possibility of criminal sanctions for infringements of § 116A of the Australian copyright act.

<sup>180</sup> CDPA, § 296ZB(1).

<sup>181</sup> *id.*, § 296ZB(1)(c)(iv).

Importing a circumvention device for private and domestic purposes also appears to be exempted by the wording of the section which only contemplates a prohibition on importing such a device ‘otherwise than for ... private and domestic use’.<sup>182</sup>

Section 296ZB(3) carves out an exemption from liability for activities conducted by or on behalf of law enforcement or intelligence agencies in the interests of national security or for the prevention of crime, investigation of an offense, or conduct of a prosecution. Section 296ZB(5) also provides a defense if the defendant can establish that she neither knew, nor had any reasonable grounds for believing, that the device or service in question enabled or facilitated the circumvention of an effective technological measure. None of these provisions will give much comfort to the private individual wishing to utilize a circumvention device to make a legitimate use of a copyright work. They will only protect such individuals in particular circumstances from *criminal liability* for trafficking.

The criminal sanctions on trafficking in circumvention devices are supplemented by the availability of civil proceedings under § 296ZD. This provision follows the basic structure of the § 296ZA anti-circumvention prohibitions, creating a new cause of action for a copyright holder and for a person authorized by the copyright holder to distribute a relevant work to the public, against a person who has trafficked in a circumvention device or service. There are no exemptions from liability set out under this provision. Section 296ZD(1)(b) of the CDPA refers to trafficking in devices or services which: (a) are promoted, advertised or marketed for the purpose of circumventing a technological protection measure;<sup>183</sup> (b) have only a limited commercially significant purpose or use other than to circumvent a technological protection measure;<sup>184</sup> or, (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of a technological protection measure.<sup>185</sup>

This definition of a circumvention device or service is likely to raise similar problems of judicial interpretation as those currently arising under the DMCA in the United States and § 116A of the copyright act in Australia. It is very difficult to ascertain on the face of any given set of circumstances whether a particular device fits these criteria if it is also capable of substantial non-infringing purposes, such as to facilitate a fair use. In any event, most devices capable of substantial non-infringing uses will also be capable of substantial infringing uses and so will likely run afoul of this section, as has been the case in other jurisdictions that have adopted similar legislative provisions.

The legislative provisions described here from various countries evidence that the DRM dilemma has, in recent years, taken on a significant global dimension. Even with

---

<sup>182</sup> *id.*, § 296ZB(1)(b).

<sup>183</sup> *id.*, § 296ZD(1)(b)(i).

<sup>184</sup> *id.*, § 296ZE(1)(b)(ii).

<sup>185</sup> *id.*, § 296ZE(1)(b)(iii).

increasing thought given to protecting legitimate interests in copyright works from anti-circumvention legislation, the DRM dilemma persists. This is because, as long as the focus is on regulating circumvention *technologies*, the resulting legislation will be too blunt an instrument to discourage digital piracy while preserving legitimate uses of digital copyright works. The only way to resolve this dilemma is to take the legitimate use issues out of the equation and deal with them in some other way. Circumvention technologies should be able to be regulated globally to combat digital copyright piracy while new mechanisms are developed to promote legitimate uses of copyright works. The administrative procedure set out in the new § 296ZE of the CDPA in Britain may be a useful move in this direction. However, as noted above, there is still much room for improvement.

### III. DIGITAL ENCRYPTION AND THE PRESERVATION OF FAIR USE

#### A. CRAFTING A FAIR USE MECHANISM FOR DIGITAL COPYRIGHT ANTI-PIRACY LAW

So where are we now with the DRM dilemma? The currently emerging picture of DRM legislation and judicial interpretations of that legislation globally is worrying in terms of facilitating legitimate interests in digital copyright works. Such legitimate interests might include making back-up copies of software and decompiling software to create interoperable software products, as well as various scientific, technological and educational uses of copyright works, and even some level of private, non-transformative copying.<sup>186</sup> The laws in different jurisdictions vary on the extent to which these kinds of activities are permitted under general copyright law or as defenses to DMCA-type claims. This really leaves two problems unresolved: (a) identifying permissible uses of copyright works with any degree of certainty,<sup>187</sup> and, (b) facilitating access and use of protected copyright works for those permissible purposes. The following proposal seeks to address both issues.

The current imbalance of interests is understandable because the problems of protecting digital copyright works are complex due to the nature of technologies currently available to access, copy and disseminate digital works on a scope and scale never before possible. However, this imbalance does suggest that it is time to review the situation both domestically and globally with a view to developing a more nuanced approach to the regulation of digital copyright works that can promote legitimate interests in relation to those works while preventing digital copyright piracy.

---

<sup>186</sup> The issue of private, non-transformative copying has been particularly contentious in fair use jurisprudence in the United States. It has been unclear whether such uses should qualify as ‘fair use’ in American copyright law: see *Sony v Universal City Studios*, 464 U.S. 417 (1984). Some of these issues are currently being re-litigated in the *Grokster* file sharing litigation in the United States Supreme Court.

<sup>187</sup> Some may argue that ‘certainty’ here is neither desirable, nor possible. However, some greater data generation on social norms in relation to fair use in the digital age would certainly be a useful development for the further evolution of copyright principles and policies into the 21<sup>st</sup> century.

If, for example, copyright holders were required to facilitate access and use of protected works for users seeking to make limited legitimate uses of a work, the regulation of anti-circumvention technologies *per se* might not be so much of a threat to the balance of information dissemination and use in the digital age. This article suggests a simple administrative procedure to encourage copyright holders to facilitate such accesses and uses, while ensuring that copyright holders are still protected from digital piracy through the mechanisms currently in place to regulate the dissemination and use of anti-circumvention technologies. This approach would not necessarily deal with problems created by anti-trafficking laws in terms of stifling innovations in decryption technologies more generally. However, these issues would at least not be so immediately problematic to society if decryption mechanisms were required to be made available directly *by content holders* to those seeking to make *legitimate uses* of digital copyright works. One could perhaps assume under these circumstances that any external market for decryption technologies might well be focused on facilitating *impermissible* uses of copyright works. Such a market would thus be appropriately regulated by aggressive judicial enforcement of the DMCA and similar legislation in other countries.

The scheme suggested here for redressing the balance would require the development of an administrative mechanism utilizing an agency that could hear complaints brought directly by those seeking to make legitimate use of a copyright work. The agency would be empowered to make orders binding on a copyright holder to the effect that the copyright holder would be obliged to make access available to a relevant person for a limited stated purpose found to be legitimate by the agency. If the agency did not find the use to be legitimate, it would dismiss the claim. Any order made by the agency would be limited to the purposes stated in the order. If a successful claimant made any uses of a work outside those stated purposes, the copyright holder would retain its right to either raise a complaint with the administrative agency or bring a standard copyright infringement action in a court of competent jurisdiction.

The detailed operation of this procedure and some of the legal issues inherent in the suggestion are set out in more detail *infra*. They include questions involving: (a) how to determine whether a particular use is a fair use in this context; (b) ensuring continued access to courts in appropriate cases to review administrative orders made under this process; (c) how the procedure would impact on contractual restrictions on access or use to a protected digital copyright work; and, (d) the legal implications of elevating the idea of fair use into the legal basis for an administrative complaint against a copyright holder.

Prior to conducting that analysis, it is worth noting that in the related context of examining the impact of modern digital copyright law on technological innovation in the peer-to-peer file sharing context, Professors Lemley and Reese have recently suggested a different kind of administrative dispute resolution mechanism. To avoid confusion, it is important to briefly describe their suggestion, and to explain the difference between their ideas and the suggestions made in this paper. The similarities between the two ideas is that they each involve the use of administrative procedures to better streamline the balance of interests in digital copyright works. However, Professors Lemley and Reese

were dealing with different issues in a different context to the suggestions presented in this article. They were concerned with providing administrative remedies for copyright holders in respect of direct copyright infringements by individual file-sharers. This paper, on the other hand, deals with the flipside of that coin: protecting legitimate interests of individuals to access and use digitally encrypted copyright works for permissible purposes.

Professors Lemley and Reese suggested the development of a quick and inexpensive dispute resolution procedure that could refocus copyright holders' attention on direct copyright infringements, and away from secondary liability actions, largely in the peer-to-peer file sharing context.<sup>188</sup> Under their proposed mechanism, it would be easier and faster for digital copyright holders to bring complaints against direct copyright infringers, such as peer-to-peer file sharers, than is currently the case under existing copyright law. The existing copyright framework generally requires time consuming and cost-ineffective litigation where a copyright holder proceeds individually against direct infringers who may, in any event, be difficult to locate. Additionally, it may be difficult to generate sufficient evidence of copyright infringement against this class of infringers and, even if judgment was obtained against a large group of small scale infringers, the judicial remedies obtained would likely be inadequate to cover the damages actually suffered by digital content industries. This is why copyright holders have opted to sue alleged secondary infringers such as the Napster, Aimster, and Grokster file sharing services.<sup>189</sup>

Professors Lemley and Reese argued that if copyright holders were given a quick and inexpensive avenue to bring direct infringement proceedings against actual copyright infringers, they would be less inclined to proceed against secondary infringers, such as developers of peer-to-peer file sharing technologies. This could potentially remove the chilling effect on innovations in the area of file sharing technologies.<sup>190</sup> They suggested amending the American copyright legislation to allow a simple dispute resolution procedure for digital content holders to proceed directly against alleged copyright

---

<sup>188</sup> Mark Lemley and R Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN L R 1345 (2004); Mark Lemley and R Anthony Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, University of California-Berkeley, School of Law, Public Law and Legal Theory Research Paper Series (2004) (available for download from the Social Science Research Network at <http://ssrn.com/abstract=525682>).

<sup>189</sup> For a comprehensive discussion of the relevant litigation, see Alfred Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, forthcoming CASE WESTERN RESERVE UNIVERSITY LAW REVIEW, 2005.

<sup>190</sup> Mark Lemley and R Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN L R 1345 (2004); Mark Lemley and R Anthony Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, University of California-Berkeley, School of Law, Public Law and Legal Theory Research Paper Series (2004) (available for download from the Social Science Research Network at <http://ssrn.com/abstract=525682>).

infringers without needing to involve any peer-to-peer file sharing service an infringer may have utilized.<sup>191</sup>

The suggestion made in this article of an administrative procedure to hear ‘legitimate user’ complaints is a counter-point to the Lemley-Reese approach. Rather than advocating a mechanism to provide copyright holders with an easy, legislatively-enabled avenue to pursue direct copyright infringers, this article advocates an easy, legislatively-enabled avenue for persons seeking to make a fair use of a work to bring a complaint directly against a copyright holder. It imposes an obligation on the copyright holder to make the work accessible in appropriate cases. The work could be made accessible with additional contractual and technological restrictions preventing further copying and distribution by a successful complainant outside the scope of the legitimate use identified in the relevant proceedings. The underlying idea here is that a fair user’s interests in accessing and using a relevant work should be effectively protected by the government that has created the copyright protections and the additional DRM legislative supports for digital copyrights.

This approach may not have the same impact on preventing the chilling of technological innovation in the DRM area as Professor Lemley and Reese’s suggestion would likely have in the area of file sharing technology. This is because the administrative measure suggested here does nothing to preserve technological innovations in decryption technology *per se*. The presumption is that such innovations might, to some extent, be sacrificed if fair use could be preserved in other ways. Fair use would then foster a different kind of innovation in society as a result of the ability of more people to use copyright works to make scientific, technological, educational, artistic, and literary advances.

Another important point of comparison with the Lemley-Reese approach to minimizing secondary liability litigation is that the measures suggested in this article do not give anything additional to copyright holders, whereas the Lemley-Reese suggestions do give copyright holders an easy ability to sue direct infringers that they do not currently have. This potentially removes, or at least significantly tempers, their motivation to proceed against those who develop and distribute, say, digital file sharing technologies. The approach suggested here to DRM measures, in contrast, might be seen as taking something away from copyright holders without giving them anything back. In other words, it might be regarded as imposing additional duties on copyright holders to facilitate fair uses without giving them any commensurate benefits.

However, this is arguably not the right way to look at it. For one thing, if fair use has any real significance, it must be protected by the law. It has certainly been assumed at some level in most relevant jurisdictions that fair use has some significance as a legal

---

<sup>191</sup> To this end, they suggest the insertion of a new § 514 in Title 17 of the USC. Details of their proposed legislative mechanism are available in: Mark Lemley and R Anthony Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, University of California-Berkeley, School of Law, Public Law and Legal Theory Research Paper Series (2004) (available for download from the Social Science Research Network at <http://ssrn.com/abstract=525682>).

right.<sup>192</sup> Thus, the imposition of a requirement that a copyright holder employing DRM measures should facilitate access to a protected work for fair use purposes is not really ‘taking something away from’ the copyright holder. It is only requiring the copyright holder to facilitate a right in someone else that already exists. If it is not clear whether a relevant right exists in any given case, this is also something that may be clarified through use of the administrative procedure over time.<sup>193</sup> This approach may embody the kind of social bargain that should have been made when legislative measures such as the DMCA were enacted. In fact, it appears to be the bargain that Congress was trying to strike in the DMCA.<sup>194</sup> However, the actual drafting and subsequent judicial interpretations have not made that bargain sufficiently clear as exemplified by recent judicial determinations on the DMCA, involving fair use arguments.<sup>195</sup>

A final point of comparison to make between the administrative procedure advocated here and the Lemley-Reese administrative procedure is that the latter is postulated as an *alternative* to an already existing judicial right of action. Copyright holders currently have the option of bringing judicial proceedings against direct infringers (individual users) but, for the reasons suggested above, this approach may be more costly and unwieldy for copyright holders than an administrative proceeding. On the other hand, the administrative procedure suggested in this article to facilitate fair use is not an alternative to an already existing judicial action. Potential fair users cannot currently use their rights as a ‘sword’ to bring an action against copyright holders who deny them

---

<sup>192</sup> See, for example, MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW (3ed, 1999), 428 (citing *Rosement Enters Inc v Random House Inc*, 366 F 2d 303, 306 (2d Cir 1966), *cert denied*, 385 U.S. 1009 (1967) describing fair use as a ‘privilege’); WILLIAM CORNISH and DAVID LLEWELYN, INTELLECTUAL PROPERTY: PATENTS, COPYRIGHTS, TRADE MARKS AND ALLIED RIGHTS (5 ed, 2003) 808 (noting that British law has generally assumed that fair dealing exceptions to copyright infringement, the British equivalent to fair use, have generally been assumed to be constitutionally guaranteed rights of access and use, although there has historically been little actual debate about it).

<sup>193</sup> This is because over time the administrative procedure would generate more data relating to emerging social norms about fair use which would, in turn, help both copyright holders and potential fair users to know what kinds of uses are likely to be regarded as legally permissible.

<sup>194</sup> 17 U.S.C. § 1201(c)(1); 17 U.S.C. § 1201(a)(1)(B)-(D).

<sup>195</sup> See, for example, *United States v Elcom*, 203 F Supp 2d 1111, 1134-1135 (2002): “[W]ith regard to the argument that fair use rights are impaired [by the DMCA], the DMCA does not eliminate fair use or substantially impair the fair use rights of anyone. Congress has not banned or eliminated fair use and nothing in the DMCA prevents anyone from quoting from a work or comparing texts for the purpose of study or criticism. The fair user may find it more difficult to engage in certain fair uses with regard to electronic books, but nevertheless, fair use is still available.”; *Universal City Studios v Corley*, 273 F.3d 429, 458 (2d Cir. 2001) (“the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement.”). Further, as noted above, it is not currently clear that fair use is, in fact, a defense to a DMCA claim, at least in the United States: Dan Burk, *Anticircumvention Misuse*, 50 UCLA L REV 1095, 1137-1138 (2003) (DMCA makes no explicit provision for fair use with regard to the anticircumvention right itself, as distinct from the copyright in the underlying work); *Universal City Studios, Inc v Reimerdes*, 111 F Supp 2d 292, 322, 323-324 (S.D.N.Y. 2000); *aff’d* 273 F 3d 429 (2d Cir 2001) (fair use is not a defense to DMCA infringement); Pamela Samuelson, *Intellectual Property in the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Tech LJ 519, 539 n. 108 (1999).

access to, or use of, a relevant work. Fair use is only a ‘shield’ in the sense of a defense to a copyright infringement action. Thus, the procedure suggested here would require not only determinations of the kinds of fair uses that would be protected by the administrative procedure, but also revisions of relevant copyright legislation to allow fair uses to be utilized as a sword: in other words, as the basis of an action or complaint against a copyright holder.

One might argue that if the copyright legislation was amended in this way and fair use was legislatively elevated to the status of a legal sword, there would be no additional need for an administrative procedure to assist the complainant in asserting this right.<sup>196</sup> The complainant could simply go direct to a relevant court<sup>197</sup> to enforce her rights against the copyright holder. This would still be preferable to the current position because it would involve a third party – in this case a court – adjudicating an appropriate balance of rights and interests in a copyright work. This is obviously superior to the current position where a potential fair user only has the ability to request access directly from a copyright holder who will often have little to no incentive to grant that access without the intervention – or at least threat of intervention – of a third party such as a court or administrative agency.

The reason that an administrative procedure is advocated here rather than a judicial procedure is that an administrative procedure may be more easy to utilize by the classes of people likely to be asserting fair use rights in a DRM protected copyright work. Administrative approaches tend to be more flexible and less formal in their procedures than judicial processes and generally do not involve the expenses of a judicial hearing. All of these factors may prove more welcoming to the classes of people – individual users, educators, scientists etc – who may be interested in making fair uses of protected works. This may well be the reason that an administrative procedure was adopted in the 2003 revisions to the CDPA to facilitate permissible uses of a copyright work,<sup>198</sup> rather than the option of creating judicially enforceable rights to facilitate such uses of copyright works. Administrative procedures of the kind contemplated in this article are also generally faster and would allow for much more efficient generation of data about emerging social norms on fair use which could prove very useful in future delineations of the boundaries of the fair concept.<sup>199</sup>

## **B. DETERMINING PROTECTED USES**

---

<sup>196</sup> The author is indebted to Professor Thomas Nachbar for his thoughts on this issue.

<sup>197</sup> In the United States, this would presumably be a federal District Court.

<sup>198</sup> See new section 296ZE, CDPA.

<sup>199</sup> To some extent, some such data is currently collected in the United States under the triennial Librarian of Congress’ review of the anti-circumvention provisions: ss sections 1201(a)(1)(C)-(E) of Title 17 of the United States Code. However, what is suggested in this article is more comprehensive and perhaps more efficient in some ways.

A number of legislative and executive steps would be necessary to operationalize the kind of approach described here to better protect fair use with respect to a digitally encrypted copyright work. For one thing, the place of fair use within digital copyright anti-piracy law needs to be more clearly determined than is the case in much of the current legislation and literature. At the very least, fair use should be formally recognized as a defense to the circumvention of even an *access control measure* if the purpose of the access was to make a fair use of a protected work.<sup>200</sup> The elevation of fair use to a guaranteed right - or formal acknowledgment of fair use as such a right, depending on the perspective one takes of its current status - is necessary in the digital age. It is particularly important in an era of digital locks and fences that fair uses can be protected by the law to ensure an appropriate balance of information usage in the digital age. This means that fair use should be available to be utilized as a sword rather than merely a shield in the digital copyright context in order to ensure an appropriate societal balance of competing interests in digital copyright works. If copyright legislation could be amended to clarify the nature of fair use as a clear legal right and the basis for an independent cause of action, both administrative and judicial, this would be an important step in the right direction.

A procedure to better facilitate fair uses of digital copyright works could take a number of forms. The basic underlying principle should be that it should not impose unreasonable expense on the potential fair user – or the copyright holder for that matter - but that it should impose some affirmative duties on the copyright holder to facilitate the fair use. Where the balance of power with respect to DRM measures heavily favors copyright holders, it seems reasonable to impose some affirmative obligations on those right-holders to enable legitimate uses of copyright works to achieve an appropriate societal balance of interests here,<sup>201</sup> provided that these obligations do not impose unrealistic financial burdens on copyright holders.

Simply requiring a copyright holder to make some access and use available to identified individuals for limited stated purposes is not likely to be an undue burden. This could be achieved simply and cheaply by the copyright holder through digital means: for example, sending the relevant user a password to obtain limited access to a relevant work for the stated permissible purpose, or perhaps sending a hard copy of a relevant work (depending on the nature of the work) that could be photocopied by the

---

<sup>200</sup> This approach has been taken in two recent United States bills that have not been enacted into law. See Digital Media Consumers' Rights Act of 2003, H.R. 107, 108<sup>th</sup> Cong., § 5(b) (2003) (allowing circumvention of a technological protection measure if it does not result in a copyright infringement); Digital Choice and Freedom Act of 2003, H.R. 1066, 108<sup>th</sup> Cong., § 5 (2003) (allowing circumvention and/or trafficking in a circumvention device for purposes of making a non-infringing use of a copyright work in certain circumstances).

<sup>201</sup> For a more general discussion of balancing rights and obligations of owners of digital property interests, see Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLORIDA LAW REVIEW 135 (2004).

user, but not digitally disseminated.<sup>202</sup> The copyright holder could ensure protection against further unauthorized uses of a work by the fair user outside the scope of the relevant fair use by imposing additional contractual and technological measures which need not be dissimilar to those currently employed by copyright holders to restrict unauthorized access to, and use of, their works. This should not put an additional significant burden on copyright holders if they have already developed these measures as part of their standard business models. They may simply need to modify them to facilitate certain fair uses in given circumstances.

The next task in establishing a procedure to facilitate fair uses is to identify the broad classes of uses that need to be protected. This is, of necessity, a somewhat imprecise task, partly because the boundaries of the fair use defense in copyright law have never been particularly clear. The advantage of this imprecision is its flexibility of operation.<sup>203</sup> The administrative mechanism for enabling fair uses suggested in this article draws on this flexibility by ‘institutionalizing’ it. The idea is to give an administrative agency the power to develop fair use categories over time to keep pace with changing needs of society. Such a mechanism both keeps pace with social needs and generates data about developing social norms and expectations relating to fair use that can later be fed into judicial and legislative advances in digital copyright law.

Although some would argue that fair use either cannot or should not be ‘institutionalized’ in this way, it may be time to re-think the traditional position on the flexibility of the fair use doctrine. Perhaps a significant amount of uncertainty in relation to the scope and nature of fair use was acceptable prior to the digital age when there was not such a significant concern about copyright holders locking up copyright works through the use of DRM measures. However, now that digital technology has shifted the balance so profoundly in favor of those utilizing DRM measures to fence off all manner of digital information, it may be that more powerful competing interests need to be developed and effectively protected by the legal system. Creating a clearer taxonomy of ‘fair use’ type interests in copyright works that reflect emerging social norms about the balance of information usage in society may be a good way to start.

Even if a taxonomy of fair use interests could be created over time to reflect emerging social norms in this way, any administrative agency charged with implementing a scheme such as that described in this article would need some initial guidance on the nature and scope of fair use in order to make its early determinations on complaints brought before it. The agency might start by utilizing some of the uses that could have

---

<sup>202</sup> In such a scenario, a user granted access in this way could technically go to the trouble of scanning a relevant work into a computer and disseminating it digitally, but this would be a direct infringement of copyright if outside the scope of an access / use order made by the relevant administrative agency.

<sup>203</sup> *Iowa State Univ. Research Found, Inc. v American Broad. Cos.*, 621 F. 2d 57, 60 (2d Cir. 1980) (“the doctrine of fair use . . . permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which the law is designed to foster.”)

been facilitated by technologies banned in recent DMCA litigation in the United States<sup>204</sup> as an early guideline, as well as the kinds of things often regarded as fair or permissible uses under general copyright legislation. These uses might include things like: (a) making a back-up copy of a digital work (DVD, eBook, CD, .mp3 file) lawfully purchased; (b) making limited copies for educational/classroom use; (c) accessing a work or making a copy, or a limited number of copies, of a work for a research team; and, (d) accessing and using a work legally purchased but regionally encoded for another jurisdiction.<sup>205</sup>

These are familiar uses, some of which have already been protected as defenses against copyright infringement or anti-circumvention infringement, depending on the jurisdiction. To simply allow these uses to have more ‘teeth’ in the sense of permitting potential fair users to assert them in an administrative proceeding seeking to gain access or use does not seem to be an unfair change in the law even from the copyright holders’ perspective.<sup>206</sup> If these uses were already protectible as defenses to certain copyright infringement and related actions, they should be protectible in cases where copyright holders have utilized DRM measures to restrict access to, and use of, copyright works in a way that prejudices such uses.

It may be that more commercially-motivated interests, such as reverse engineering a digital encryption measure to create a work or device that is interoperable with a protected copyright work might also be included in the conception of fair use for these purposes. However, there are currently stand-alone legislative provisions that attempt to preserve these kinds of activities.<sup>207</sup> It might be easier in the first instance, and less threatening to copyright holders generally, to limit the administrative procedure to protecting non-commercial uses of digital copyright works, or at least uses that do not, or are not likely to, commercially compete with current or potential interests of a copyright holder.<sup>208</sup>

---

<sup>204</sup> See, for example, *Universal City Studios v Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff’d* *Universal City Studios v Corley*, 273 F.3d 429 (2nd Cir. 2001); *United States v Elcom*, 203 F Supp 2d 1111 (2002); *321 Studios v MGM Studios*, 307 F Supp 2d 1085 (2004).

<sup>205</sup> This is an issue that has recently arisen in Australian litigation in the *Sony v Stevens* case. See [2002] FCA 906 (26 July 2002), available at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 14, 2004. This decision was overturned in part on appeal to the full federal court: see *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003), available at <http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/157.html>, last viewed on July 14, 2004.

<sup>206</sup> Even the simple clarification that fair use could be used as a sword (ie cause of action) in a *judicial* proceeding, rather than as a mere defense to a copyright infringement action would be an improvement here, as noted above.

<sup>207</sup> CIPA, §50B(2); 17 U.S.C. § 1201(1)(f).

<sup>208</sup> Some teaching and research purposes, for example, might be classified as ‘commercial’ but may well not compete with copyright holders’ commercial interests and so should be protected under a new administrative mechanism. Working out whether a commercially interest might compete with a potential future commercial interest of the copyright holder will never be an easy task as current online file sharing

### C. THE ADMINISTRATIVE AGENCY AND ITS PROCEDURES

In terms of the administrative proceeding itself, copyright legislation might be amended to create a framework for an administrative mechanism to determine when, and on what basis, a particular fair use should be enabled.<sup>209</sup> As noted above, any legislative amendments should first clarify that fair use can be utilized as a legal sword: that is, as the basis for a complaint against a copyright holder for denial of appropriate access to a relevant work. The new administrative agency would make determinations on a case by case basis and would be empowered to make orders binding on a copyright holder to enable access and use for particular stated purposes, regardless of restrictive technological and contractual measures the copyright holder may otherwise have put in place with respect to the work.

The parties to the administrative proceeding should also have an appeal mechanism available through the administrative body itself: for example, an appeal to a more senior administrative officer or panel of officers. Ultimately, the parties could also bring an appeal before the courts. The ultimate appeal to the judicial system is another important reason why the status of fair use should be legislatively clarified prior to implementing any scheme to protect such uses against unfair technological or contractual denials of access to a copyright work. In this context, fair use should not simply be a defense to a complaint for copyright infringement – it should be a clear stand-alone legal right that can be enforced judicially as well as administratively.

The administrative mechanism would not oust the courts' jurisdiction, but would provide an inexpensive initial option for both resolving individual disputes, and ultimately generating some data on emerging social norms relating to the balance of interests in digital information products. In contrast with a purely judicial approach, the administrative approach advocated here would enable more people to have access to an inexpensive and effective determination of their rights in relation to a particular copyright work. Data generated by the new system about emerging social norms on fair use could usefully be fed back into the legal process to assist in future legislative and judicial determinations about balancing competing legitimate interests in digital copyright works.

The 2003 amendments to the CDPA in the United Kingdom might be a good starting point for the administrative scheme suggested in this article. However, the development of a simpler and less discretionary approach than that set out in the CDPA could be more useful. Some problems with the British approach might arise due to the fact that the Secretary of State under the CDPA has discretion whether or not to make any

---

cases in the United States demonstrate. However, the generation of some data about social norms on fair / legitimate uses of copyright works, taking these potential difficulties into account as much as possible, would still be a useful step forwards here.

<sup>209</sup> This discussion focuses on a domestic approach to this issue. However, the suggestions made here could ultimately be expanded to the international level, particular if an inexpensive online dispute resolution procedure were to be employed – see *infra*.

particular investigations or orders. The administrative system suggested here, on the other hand, is mandatory in nature: that is, the administrative agency must hear complaints brought before it, although it has no duty to make any particular order in a given case. It must weigh up the evidence and representations made to it.

The administrative agency contemplated here could be a stand-alone body or, in appropriate jurisdictions, could be a department established under the auspices of the Copyright Office.<sup>210</sup> The dispute resolution agency – or department - could collect fees to hear a complaint about failure of a copyright holder to provide sufficient access to make fair use of a relevant work. The fees may be sufficient to fund all or part of the administrative operation. This fee requirement may also limit the volume of frivolous complaints brought before the agency. Fees should be significantly lower than court costs, but their existence should operate as a deterrent to frivolous claims.

Thus, the new scheme would do two important things. It would establish fair use as a legally enforceable right against a copyright holder who is utilizing contractual or technological measures to restrict access to, and use of, a relevant work. It would also establish a mechanism to facilitate the exercise of a fair use right utilizing a low cost, administrative procedure established under the legislation. Thus, the legislation would create, or formalize, a particular conception of a fair use right that would enable administrative action against a copyright holder, but only in the limited area of seeking access to an encrypted work for particular, clearly delineated purposes. These purposes would be set out in any administrative order granting access to, and use of, a relevant work.

Both the complainant and the copyright holder would be entitled to make representations to the administrative agency with respect to the complaint. Thus, the copyright holder would have to be given notice that a complaint had been made. In fact, it may be a precursor to a complaint that the potential fair user has made a good faith effort to contact the copyright holder to seek access to a protected work for stated fair use purposes. Building such a requirement into the administrative procedure may ultimately reduce the number of complaints heard by the agency. If fair users were encouraged to make contact with copyright holders to seek fair use, and copyright holders were aware that failure to grant access for legitimate purposes might result in an unfavorable administrative order, private parties may over time become better at resolving these situations through private negotiations.

---

<sup>210</sup> Oversight by the Copyright Office would only be possible in jurisdictions with a Copyright Office, such as the United States. Many jurisdictions do not have a copyright registration system and do not have a Copyright Office. The dispute resolution procedure suggested by Lemley and Reese – *supra* - is focused on the American position and utilises a mechanism involving filing complaints with the Copyright Office and complaints being decided by an administrative law judge in that office: Mark Lemley and R Anthony Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, University of California-Berkeley, School of Law, Public Law and Legal Theory Research Paper Series (2004), suggested new 17 U.S.C. § 514(c) (available for download from the Social Science Research Network at <http://ssrn.com/abstract=525682>).

In fact, one of the indirect goals of the administrative procedure would be to assist in such private re-ordering of rights and interests. This would be achieved both by encouraging greater co-operation between right-holders and fair users in this way, and also by gradually establishing social norms with respect to fair use through complaints actually determined under the procedure. The identification and understanding of such norms would help private parties better determine their rights up front without needing to seek assistance from the administrative agency or the courts. It would help copyright holders to know when they should grant appropriate levels of access to particular individuals, and it would assist those individuals to understand if and when they had a valid claim to access and use a given work for a particular purpose. Although flexibility has been the norm in this area in the past, it may be that more certainty is now required in defining and operationalizing more precise categories of fair use interests, particularly in the face of the very real threat that copyright holders can unfairly monopolize all manner of digital information by utilizing restrictive DRM measures.

The administrative agency could borrow a number of procedures from existing informal dispute resolution mechanisms, notably the Uniform Domain Name Dispute Resolution Policy ('UDRP') adopted by the Internet Corporation for Assigned Names and Numbers ('ICANN') for dealing with domain name disputes in an effective and efficient, and ultimately global, manner. The UDRP has a simple and straightforward set of forms and procedures for lodging complaints, and responses to complaints. Most of the representations are done on paper or in electronic form.<sup>211</sup> Formal in-person hearings are hardly, if ever, required.<sup>212</sup> This enables simple, low cost determinations to be made. It also enables parties from geographically dispersed areas to have their complaints handled without the cost and expense of appearing before a particular court or body in any given jurisdiction. This kind of procedure might ultimately be adopted on an international level for digital copyright complaints, given the increasingly global reach of many digital copyright interests.

The agency would basically have two options in any given dispute. It could either make an order binding on the copyright holder to enable access for stated purposes, or it could refuse to make an order based on an inadequate showing of a legitimate purpose.<sup>213</sup> If it made an order to enable access, the order would set out the extent of access and use permitted, and the copyright holder would have a cause for appeal to the agency and

---

<sup>211</sup> Rules for Uniform Domain Name Dispute Resolution Policy, Rules 2(b), 3(b), 5(b). Full text of Rules available at: <http://www.icann.org/udrp/udrp-rules-24oct99.htm>, last viewed on January 24, 2005.

<sup>212</sup> Rules for Uniform Domain Name Dispute Resolution Policy, Rule 13 ("There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint."). Full text of Rules available at: <http://www.icann.org/udrp/udrp-rules-24oct99.htm>, last viewed on January 24, 2005.

<sup>213</sup> To some extent, this draws from the UDRP notion of the arbitrator(s) making a simple decision whether or not to order a domain name registrant to transfer a disputed domain name to a complainant. The analog here is a notion of arbitrator(s) making a decision whether or not to order a copyright holder to permit a particular use of a copyright work.

ultimately to a court if the complainant thereafter misused the work in terms of exceeding the scope of the order. The copyright holder could also impose additional contractual and DRM measures to ensure that a complainant did not utilize a given work outside the scope of a relevant order. If a copyright holder objected to the making, or scope, of any given order, it could also appeal either to a superior level of the administrative body or to a court. In terms of 'levels' of authority, the administrative procedure could allow for initial administrative determinations by a single administrator, with an appeal or reconsideration mechanism to a panel of administrators or to a more senior administrator.

Although this may sound like it changes the status quo from the current position and unfairly burdens copyright holders, it must be kept in mind that the current balance tends to unfairly burden potential fair users who generally have less financial ability and less legislative and judicial recourse to protect their interests to access and use relevant works. It is also currently unclear whether such individuals have any distinct legal rights to access and use copyright works in the first place. Further, it is likely that many of the complaints brought before the administrative agency would presumably be small scale in scope and unlikely to raise too many concerns for a copyright holder in terms of the costs of granting access and use. However, without the procedure in place, those copyright holders may have little to no incentive to grant *any* access to potential fair users. Thus the imposition of a third party alters the balance to what it should arguably have been in the first place and simply gives copyright holders a little added incentive to facilitate that balance without requiring anyone to incur exorbitant court costs in so doing.

All decisions of the administrative agency could be judicially reviewed if either or both parties were unsatisfied with the outcome. The potential risk with this is that powerful copyright holders might hijack the system by constantly appealing administrative determinations to the courts. However, this would still be less of a risk in terms of achieving an appropriate societal balance of interests in digital copyright works than the current system. At least with the new system, there might be something on the record – an administrative order – supporting the fair use rights in the first place. Thus, courts would have some evidence of an administrative agency being convinced of a particular legitimate purpose in a given case.

Secondly, constantly appealing administrative orders allowing access and use for legitimate purposes may generate negative publicity for powerful copyright holders. Finally, the costs of such litigation, as opposed to the costs of enabling limited access for legitimate purposes, may not be worth the trouble for copyright holders provided that they could ensure through technological, contractual, judicial and administrative means that fair users did not exceed the rights granted in any given administrative order. As noted above, it is likely that many of the complaints brought through the administrative proceeding would be small scale in scope and that it would not be particularly costly or difficult for copyright holders to implement relevant orders, nor should it significantly threaten the commercial markets for their works.

In any event, this system could be beneficial to copyright holders. If copyright holders and fair users could develop access and use strategies based on private

negotiations, facilitated by the administrative procedure, there may be less perceived need for legitimate users to seek out circumvention technologies in the first place. They could be more confident of obtaining the kinds of access and use required with respect to digital copyright works without seeking out the very technologies that are of the most concern to copyright holders in the modern world: those that might facilitate large scale digital piracy. Copyright holders, by enabling some access to fair users, could lessen the social pressures to develop and disseminate decryption technologies that might also be used for large scale digital piracy as well as small scale fair use activities.<sup>214</sup> It is unclear what kind of impact this might have on innovation in the ‘circumvention device’ area. However, it surely would not have a greater impact than the current set of laws that prohibit the marketing of such technologies on a significant scale, with little thought as to the needs of those who might utilize them for legitimate purposes.

In terms of an administrative decision denying access to a copyright work in any given case, the question would be open whether the complainant could then appeal her complaint to a court within a relevant jurisdiction. The suggestion has been made above that, whether an administrative or judicial approach is taken to facilitating fair use for the digital age, it is important that legal systems elevate fair use to the status of a legal ‘sword’: that is, a stand-alone right that can support administrative and judicial action. If the right was to be so elevated, both administrative and judicial recourse should be available to a person claiming fair use in the face of access having been denied or limited through technological or contractual means by a copyright holder. This article suggests that an administrative complaint should be the first avenue to assert the right, and then administrative or judicial appeal may follow in a given case.

Because the administrative agency would be limited to one of two options in the first instance – making an order or refusing to make an order enabling access for a particular purpose – the procedures could be kept relatively simple and inexpensive. This means, of course, that there are a number of difficult questions concerning copyright and fair use that the administrative agency would not consider. These questions include whether copyright was validly granted in the first place for the work in question.<sup>215</sup> This would be outside the scope of the administrative procedure. The administrative agency would have a narrow mandate simply to make orders to enable access and use in specific circumstances where the ability to make a legitimate use has been compromised by technological means, perhaps bolstered by contractual restrictions. The rationale for this is to redress the balance of interests that has become skewed since the digital content

---

<sup>214</sup> This might avoid situations such as that which arose in the *321 Studios* case – *supra* – involving the manufacture of a device capable of facilitating both infringing and non-infringing uses of a digital copyright work.

<sup>215</sup> This question is becoming increasingly problematic in the digital age with respect to software copyrights in particular. The recent appeal in the *Lexmark* litigation is a good example of courts revisiting issues relating to the initial copyrightability of certain classes of software code: *Lexmark v Static Control Components*, 387 F.3d 522, 537-544 (2004) (majority holding particular software code to be uncopyrightable for various reasons including merger of idea and expression, application of scenes a faire doctrine and because the code operated as a ‘lockout code’ on the facts in question).

industries started utilizing DRM measures to encrypt their works against unauthorized access and use, and since those strategies have been bolstered in effectiveness by legislation such as the DMCA.

When making determinations, the administrative agency could be guided by the factors currently considered by courts in making fair use determinations in cases of copyright infringement. These vary somewhat from jurisdiction to jurisdiction, although certain aspects of the fair use idea are usefully gathered together in § 107 of the American copyright legislation. These could serve as useful guidelines, and could be modified to suit the needs of the administrative proceedings. The administrative body could, for example, be guided by the following modified applications of the factors set out in § 107. It could, in any given case, consider factors such as: (1) the purpose and character of the use for which the complainant wants to access the work, including whether such use is of a commercial nature;<sup>216</sup> (2) the nature of the copyright work; (3) the amount and substantiality of the portion sought to be accessed and used in relation to the copyright work as a whole; and, (4) the effect of any permitted use upon the potential market for, or value of, the copyright work.

#### **IV. CONCLUSIONS**

Balancing the interests of digital copyright holders against the interests of those seeking to make a fair use of a protected work is an extremely difficult proposition. The same technologies that enable content holders to market ever more attractive products also enable digital pirates to make fast, efficient, near-perfect copies of relevant works. Sandwiched in the middle of this equation are those who want to make legitimate uses of copyright works, but who are now effectively prevented from doing so because of the copyright holders' increasing reliance on DRM measures whose effectiveness is bolstered by restrictive legislative schemes such as the DMCA.

The administrative procedure presented in this article, coupled with attempts to clarify the nature and scope of the fair use concept, may be a good middle-ground solution that could help to strike a better balance between copyright holders' interests and the interests of those seeking to make fair use of a digitally encrypted work. The advantages are that it is simple, quick, inexpensive and straightforward, and it creates an environment that promotes a culture of enabling fair use and developing social norms to clarify the boundaries of fair use over time.

It does leave certain questions open, including the impact of contractual restrictions on access to, or use of, a digital copyright work, as opposed to technological restrictions. It has been assumed in the above discussion that an administrative order to enable fair use in a given case would trump a contractual restriction on such a use.

---

<sup>216</sup> Section 107 of Title 17 of the United States Code actually contrasts 'commercial nature' with 'nonprofit educational purposes'. The 'educational purposes' criterion has been omitted here to give the test a more general application and allow more flexible development of emerging social norms on fair use in the digital age.

However, that may be an invalid assumption. It is possible that a law that establishes an administrative agency such as the one suggested here is not entitled to pre-empt contractual license restrictions on access to, or use of, a digital copyright work. The answer to this question may depend on the constitutional basis on which any such law is enacted in a given jurisdiction.

Another question left open is the problem of the use of DRM measures not to copy-protect a work, but rather to regionally encode it. The relevance of digital copyright law to DRM measures protecting regional encoding is currently unclear, although the *Sony v Stevens*<sup>217</sup> case in Australia suggests that copyright law will extend to protect such measures, at least under Australian law, if there is some indirect effect of discouraging copyright infringement. If this is the case, then is it reasonable for any administrative mechanism protecting fair use to be empowered to enable fair use even in the face of a regional encoding measure? In other words, should an administrative agency of the kind postulated here be entitled to order a copyright holder to enable fair use of a legally purchased, but regionally encoded, video game, movie DVD, music or software CD or DVD? Arguably, questions such as this are in fact ideally suited to the kind of administrative mechanism advocated here, particularly if it is capable of generating data points over time with respect to emerging social norms on such classes of uses of a protected work.

There is also the question of what impact the suggested administrative mechanism would have on markets for innovation in circumvention technology. It might be argued that situating disputes about fair use firmly between the copyright holder and the fair user, without the fair user needing to rely on third party circumvention devices, might lessen the demand for such devices overall, at least for legitimate purposes.<sup>218</sup> This may bolster the presumption that any such devices are mainly intended for illegal uses and it may, in fact, strengthen the position of copyright holders in combating the development and dissemination of such devices.

Whether or not this is a desirable outcome, it is important to understand that markets for anti-circumvention devices are not doing so well under the current legislative schemes in any event, at least if the recent cases are anything to go by.<sup>219</sup> This, coupled with the fact that copyright holders are increasingly bringing secondary liability suits against those who create digital *copying and distribution* technologies, such as peer-to-

---

<sup>217</sup> [2002] FCA 906 (26 July 2002), available at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/cases/cth/federal%5fct/2002/906.html?query=eddy+stevens>, last viewed on July 14, 2004. This decision was overturned in part on appeal to the full federal court: see *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2003] FCAFC 157 (30 July 2003), available at <http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/157.html>, last viewed on July 14, 2004.

<sup>218</sup> This assumes that the predominant use for such devices would be by digital pirates if fair users had more effective avenues to gain access to a work for legitimate use purposes.

<sup>219</sup> See, for example, *Universal City Studios v Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd* *Universal City Studios v Corley*, 273 F.3d 429 (2nd Cir. 2001); *United States v Elcom*, 203 F Supp 2d 1111 (2002); *321 Studios v MGM Studios*, 307 F Supp 2d 1085 (2004)

peer file sharing services raise some broader questions of digital copyright law that are beyond the scope of this article. Clearly the effective protection of digital copyright works has the potential to impact negatively on the production and dissemination of circumvention devices, and copying and distribution technologies.<sup>220</sup>

These are difficult questions that need to be resolved over time as digital information markets develop.<sup>221</sup> However, in the interim, it would be a shame if fair use was a casualty in the larger battle between innovation in copyright works and innovation in circumvention technologies. Removing the threat of unjust encroachments on fair use from the mix would allow future debates to focus more clearly on the battle of the technologies without incidentally implicating legitimate interests in copyright works in an attempt to discourage illegal activities. The DRM dilemma is not an insoluble problem. It simply requires a more nuanced approach, so that fair uses do not become unintended casualties in the battle of the technologies.

---

<sup>220</sup> Such as the online file-sharing software disputed in the *Napster* and *Grokster* litigation – see *supra*. For a more detailed discussion of the recent file sharing disputes, see also Mark Lemley and R Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN L R 1345, 1356-1366 (2004); Alfred Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, forthcoming CASE WESTERN RESERVE UNIVERSITY LAW REVIEW, 2005.

<sup>221</sup> Mark Lemley and R Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN L R 1345, 1356-1366 (2004); Mark Lemley and R Anthony Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, University of California-Berkeley, School of Law, Public Law and Legal Theory Research Paper Series (2004) (available for download from the Social Science Research Network at <http://ssrn.com/abstract=525682>); Alfred Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, forthcoming CASE WESTERN RESERVE UNIVERSITY LAW REVIEW, 2005.