SETTING NEW LIMITS TO THE PROTECTION OF DIGITAL MEDIA

By Petroula Vantsiouri*

Abstract

This paper analyses the impact of the anticircumvention provisions of the Information Society Directive and of the Digital Millennium Copyright Act on healthy competition and in particular it addresses the misapplication of such provisions for advancing the monopoly position of copyright holders in the markets for replacement or other compatible parts for their works. It argues that judicial interpretation of the EU and US anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy with fragmenting the market and that competition law is not capable of restoring this balance and, thus, it calls for an amendment of the existing legislation at an EU level as well as in the US.

1. Introduction

Of all the issues of copyright policy in the last twenty years, probably the most controversial has been the issue of technological protection measures (TPMs). TPMs constitute self-help mechanisms, which are designed to prevent acts of exploitation of intellectual property rights by way of controlling copying or access to works.[1] As was anticipated that ways would be found to circumvent these copy and access controls, the legal systems of many countries provide TPMs legal support by giving to the rightholders concerned specific protection when trying to enforce and manage their rights by technical means. These so-called anticircumvention norms do not create or enlarge exclusive rights as such, but they enhance the exploitation and enforcement of exclusive rights by making it illegal either to circumvent TPMs or to offer services that enable circumvention. [2]

At a global level the protection against circumvention of TPMs is recognized in the WIPO Copyright Treaty (hereinafter WCT) and in the WIPO Performances and Phonograms Treaty (hereinafter WPPT). The WCT and the WPPT, the so-called WIPO Internet Treaties, oblige the contracting parties to provide adequate legal

* PhD Candidate Cantab, LL.M. Harvard. This paper is a provisional draft and shall not be cited without the permission of the author. The author may be contacted at pv250@cam.ac.uk.

protection and effective legal remedies against the circumvention of effective technological measures that are used by authors, performers or producers of phonograms in connection with the exercise of their rights and that restrict acts, in respect of their works, which are not authorized by the right holders concerned or permitted by law.[3] The anticircumvention rules were implemented in the EU and the US in the European Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the harmonization of certain aspects of copyright and related rights in the information society (Information Society Directive) and in the Digital Millennium Copyright Act (DMCA) respectively. Article 6 of the Information Society Directive requires that Member States must provide adequate legal protection against circumvention of TPMs, whereas the Section 1201 of the DMCA prohibits the circumvention of effective access controls as well as the trafficking in circumvention tools of effective access and copy controls.

TPMs were hailed by the copyright industries as effective enforcement mechanisms that would protect their interests from the risks of piracy in the digital and networked environment and as means to enable them to take advantage of the new possibilities that the advent of technology provided them. Supporters of TPMs claimed that copyright works made available in digital formats would be especially vulnerable to unauthorized copying and redistribution and thus copyright holders would be discouraged to make their works digitally available to the general public.[4] On the other hand, critics of TPMs claimed that introduction of technological measures and their protection by anticircumvention laws would restrict access to works in the public domain and that they would not respect traditional copyright exceptions.[5]

The question of whether the legislature came to the right solution when enacting anticircumvention provisions remains one of the hottest ones on the agenda. However, anticircumvention regulation raises a variety of legal issues not only within the scope of copyright law but also in neighbouring domains, which have not attracted the same attention. One of these issues concerns the misapplication of anticircumvention laws to restrict healthy competition in aftermarket products markets. In particular, manufacturers and vendors of consumer primary products may seek to prevent competitors from selling replacement parts or other compatible parts (aftermarket products), by using some kind of TPMs in the primary products or the aftermarket products. The manufacturers then could try to use the anticircumvention

clauses to prevent competitors from distributing products, which circumvent the TPMs. More specifically, vendors and manufacturers of consumer primary products, who hold a dominant position in the primary product market, can use anticircumvention regulation in order to reinforce their dominant market position in the aftermarket by preventing interoperability of products on alternative systems.

The notorious *Lexmark International, Inc. v. Static Control Components, Inc* case, which involved a printer manufacturer trying to prevent others from remanufacturing printer cartridges, presents an excellent example that indicates how a company may seek to benefit from the protection granted by anticircumvention provisions for advancing its own monopoly position and for hindering competition in the aftermarket.[6] Lexmark's behaviour, though, was not unprecedented in the market for printers. Printer prices are increasingly subsidised by cartridge sales, as the combination of cheap printers and expensive cartridges enables vendors to target high-volume business users and price-sensitive home users with the same products.[7] However, the availability of reeled cartridges, and cartridges from third-party aftermarket vendors limit the level of cross-subsidy and thus TPMs have been employed in order to eliminate competition in the aftermarket. Similar business models have been applied in the adjacent markets for consoles for computer games and computer games, in the markets for mobile phones and service providers for mobile phones and recently in the markets for smartphones and applications for smartphones.[8]

In general, the practical issues as designated by US and European jurisprudence indicate that the anticircumvention provisions give birth to competition law issues that do not arise from the classic interaction between Intellectual Property and Competition. Intellectual Property rights create a temporary monopoly for their right holders, for which the legislator has set certain restraints so that the exercise of those rights does not obstruct healthy competition. According to supporters of TPMs the rationale behind the adoption of anticircumvention regulation is to enforce this monopoly and fulfil the goals of Intellectual Property legislation. However, anticircumvention legislation can result into creating further monopolies, which the legislator initially did not aim to protect and are not subject to the restraints imposed on Intellectual Property rights. Thus, the question that arises is how to balance the conflicting objectives of Intellectual Property and competition law and decide whether Intellectual Property protection should be enforced by extending monopolies to

further markets in expense of competition in these secondary markets or whether healthy competition should prevail over the interests and the incentives for the authors of creative works.

This paper analyses the impact of the anticircumvention provisions of the Information Society Directive and of the DMCA on healthy competition and in particular it addresses their misapplication for advancing the monopoly position of copyright holders. It argues that judicial interpretation of the EU and US anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy with fragmenting the market and that competition law is not capable of restoring this balance. Thus, it calls for an amendment of the existing legislation at an EU level as well as in the US. Parts 2 and 3 of this paper outline the substantive provisions of the Information Society Directive and the DMCA and examine how their application has led to anticompetitive conduct, being challenged in the courts. Part 4 analyses the inability of competition law to restore the anticompetitive effects generated by the misuse of the anticircumvention regulation. Finally Part 5 addresses the need for amendment of anticircumvention laws and attempts to propose how the doctrine should be amended in order for a better balance between protecting the legitimate rights of copyright uses and safeguarding competition in the market to be achieved. In particular it suggests, firstly, that the infringement of the anticircumvention norms should be explicitly conditioned to the infringement of a valid copyright and secondly, that there should be no differentiation in the treatment of tangible articles of commerce and cultural artifacts and courts should be instructed to apply all exceptions equally to both categories of works.

2. The substantive provisions on anticircumvention

2.1. The Information Society Directive

Article 6 of the Information Society Directive explicitly requires Member States to provide adequate legal protection against circumvention of effective technological measures[9] designed to prevent or restrict acts not authorized by the copyright holder, including the trafficking in devices, products or services which may be used to circumvent such technology.[10] As regards the implementation of the Information Society Directive by Member States, the Directive's open wording has led to

significant differences among implementing laws.[11] This has led to continuing controversies over the Directive itself and conflicts about the appropriate design of copyright law for the digital age. Unlike the DMCA, the Information Society Directive does not treat access and copy controls differently, as the definition of TPMs in the Directive indicates. [12] Furthermore, whether the act of circumvention actually infringes a copyright is not relevant for the purposes of the protection of the TPM.[13]

Article 6(4) of the Information Society Directive regulates permissible exceptions to strict TPM protection.[14] In other words, Article 6(4) regulates the occasions when the beneficiaries of certain copyright exceptions provided in Article 5 of the Directive are hindered from making use of these exceptions due to the TPMs. However, TPMs enjoy legal protection also when they hinder the beneficiaries of the exceptions of copyright from benefiting from them, as they are not exceptions to the liability of the circumvention of technological measures.[15] On the contrary, the Directive sets out a unique legislative mechanism, which imposes an ultimate responsibility on the right holders to accommodate certain exceptions. [16] In particular, the exceptions are reinforced voluntarily by measures taken by the right-holders and, if the right holders do not comply with this obligation, Members States must ensure that right holders provide beneficiaries of the exceptions with the appropriate means to benefit from them.[17]

While the Directive has a broad, but closed list for exceptions for fair dealing, the exceptions applicable to TPMs are limited. In particular, Article 6(4) sets out two categories of exceptions: the home copying exception, which is optional; and the public policy exceptions, which are mandated. The public policy exceptions are the photocopying exception, the archival copying exception, the broadcaster's exception, the non-commercial broadcast exception, the teaching and research exception, the disability exception and the government exception.

From the exceptions contained in the Directive, only the research exception could exempt from liability a competitor who circumvents a TPM in order to manufacture and/or distribute interoperable products with the product that incorporates the TPM. Relevantly, however, this exception is subject to a condition: it is available only to the extent "justified by a non-commercial purpose" and the circumvention's sole purpose must be that of scientific research. Thus, the 'research exception' cannot be relied on as defence by competitors who try to enter a market

closed by TPMs. Notably the exceptions in the Information Society Directive also do not include "reverse engineering". Such an exception exists in the Directive 91/250/ECC of 14 May 1991 on the legal protection of computer programs (Software Directive), which provides a limited safe harbour for those trying to achieve software interoperability.

It has been argued that Member States' ability to enact exceptions with regards to the protection of TPMs is limited to those enumerated in the list in articles 6(4) subparagraph (a), as there is no other reason for these exceptions to be specially picked out.[18] Such an approach, however, may disregard Recital 48 of the Information Society Directive, which requires that legal protection against technological measures should not hinder cryptographic research, although the Directive itself does not contain such an exception. In the end, and as the Recitals are not legally binding, it would be up to the ECJ to decide whether the Member States' implementing laws are in compliance with EU law, although such a controversy has not appeared in practice. In any case, the limited number of exceptions to the protection of TPMs that are provided in the Directive takes away from the Member States the flexibility to respond to changing technological situations and to respond to issues such as the anticompetitive use of the TPMs to raise barriers of entry to adjacent markets.

More importantly, the EU legislator nullified the exceptions to copyright in two ways: First, since general exceptions permitted by Article 6 do not automatically apply with respect to TPMs, copyright holders can impede TPMs in their works, so that the beneficiaries of the exceptions can not enjoin them. Secondly, even if one of the exceptions to Article 5 also applies with regard to TPMs, the beneficiaries can not make use of the exception contrary to the will of the copyright holder, unless they participate actively in judicial proceedings.

To elaborate further, the list of exceptions applicable with regard to copyright works protected by TPMs is limited, especially as seen by comparing it to the broad list of exceptions in Article 5 of the Information Society Directive.[19] Thus, the exceptions to copyright in Member States differ depending on whether a particular work is protected by TPMs or not. Accordingly, the exceptions which do not apply with respect to TPMs can be easily overridden by the copyright holders by simply impeding a TPM. To illustrate that, if a Member State has enacted an exception permitting reproduction of a work by the press without liability, as permitted under

Article 5(3)(c) of the Information Society Directive, it must punish the reproduction if it is obtained by circumventing a TPM.

Furthermore, the move away from the traditional norm where the exceptions are positive rights to use and the enactment instead of a unique legislative mechanism, which foresees an ultimate responsibility on the right holders to accommodate certain exceptions, places the burden of reassuring the application of those exceptions from the state to the beneficiaries of the exceptions. Practically, the beneficiaries of an exception will not be able to enjoy a copyright work if the copyright holder has not voluntarily agreed to do so and they will not be entitled to circumvent the TPMs either; instead they should engage into a timely and costly judicial proceeding against the particular right holder to be able to benefit from the exception. Of course, other copyright holders may still not permit the exception.

Summing up, there are three main problems with the anticircumvention provisions of the Information Society Directive. Firstly TPMs are protected also when they do not prevent copyright infringement; secondly, the number of exceptions applicable to TPMs is limited and in particular there is a lack of a reverse engineering exception; thirdly, the exceptions provided in Article 6 para 4 of the Information Society Directive are not exceptions to the liability of the circumvention of TPMs.

2.2. The DMCA substantive provisions on anticircumvention

The DMCA protects both access controls[20] and copy controls.[21] Both the act of circumvention[22] and trafficking in circumvention technologies are prohibited for the first; for the second, only trafficking in technologies that circumvent copy controls is banned. The DMCA created three new causes of action: Section 1201(a)(1)(A) prohibits the circumvention of TPMs that control access to copyright works; Section 1201(a)(2) prohibits -- under specific conditions -- making, offering to the public, or otherwise trafficking technology that circumvents TPMs that control access to the work; and, likewise, Section 1201(b)(1) prohibits – also under specific conditions -- making, offering to the public, or otherwise trafficking technology that circumvents TPMs that control specific uses of the work.[23]

Still, the statute exempts certain activities from one or all of the causes of action recognized in Section 1201. These exemptions are either expressed in the statute itself or have been recognized by the Library of Congress, pursuant to a

congressional mandate in Section 1201(a)(1)(c).[24] One of those exceptions is contained in Section 1201(f). This exception specifically allows reverse engineering of TPMs that protect computer programs in order to obtain interoperability.[25]

The interoperability exception allows the circumvention of TPMs that effectively control access to a particular portion of a computer program under the conditions that the circumventor has lawfully obtained the right to use a copy of that program and circumvention occurs for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently-created computer program. Additionally, the information obtained through reverse engineering should not be readily available to the person engaging in the circumvention and the identification and analysis should not constitute infringement.[26] The circumventor may make available the information that she obtained by the permitted circumvention, if she provides such information solely for the purpose of enabling interoperability to the extent that the actions do not constitute infringement.[27] The law provides an opportunity to distribute solutions to the interoperability problems to users with minimal technical knowledge, who would not have been able to circumvent the TPMs themselves; however it premises this safe harbor under the aforementioned narrow conditions.

The statute's main flaws include that it fails to protect against the circumvention of TPMs protecting copyright works other than computer programs and that it does not protect data interoperability.[28] In short, the interoperability exception does not deter companies from employing TPMs to restrict the development, distribution and use of interoperable technologies. Thus, despite of the inclusion of Section 1201(f) (1) and (3), the DMCA discourages the creation of unauthorized interoperable products; it prohibits their distribution and exposes the users of technologies that enable interoperability to liability.

Having examined the flaws of the EU and US anticircumvention provisions, it should be further examined whether those problems can be alleviated via the judicial route or whether there is a need for amendment of the anticircumvention norms. There are quite a few examples from the jurisprudence on the Information Society Directive and on the DMCA on that demonstrate how companies have tried to benefit from anticircumventionregulation in order to establish themselves in secondary markets. These cases also provide guidance on how one can expect the courts to handle future anticircumvention cases.

3. Relevant case law

3.1. Jurisprudence of European Courts

Neither the Court of First Instance nor the European Court of Justice ECJ have yet had the chance to interpret the substance of the provisions of the Information Society Directive regarding TPMs.[29] Thus, for the time being, one has to rely on the interpretations of the implemented provisions of the Directive by the national courts of the EU Member States. Even narrowed thus, the pool of interpretations is quite small – since many Member States delayed in implementing the Directive.[30]

Of particular interest is a dispute initiated by Kabushiki Kaisha Sony Computer Entertainment before the Tribunale di Bolzano, in Italy against Dalvit Oscar, a vendor of "neo 4" mod chips used to evade the protection measures of Sony's PlayStation (Defendant). The case demonstrates the efforts of the courts to interpret the Italian law implementing the Directive in a way that balances the goals of defeating piracy,[31] safeguarding healthy competition in the market and promoting consumer welfare.[32]

However, this is not the only interesting feature of the decision. Also of note is the fact that it involves efforts by a major computer game manufacturer, Sony, to control the market for its games.[33] Computer games manufacturers have been attempting to manipulate barriers to entry for many years. The business strategy that they follow is to subsidize sales of the actual consoles with sales of cartridges or, more recently, CDs containing the software. Sales of accessories, such as memory cards, are also controlled. [34] This was one of the many lawsuits that Sony initiated on globally invoking the anticircumvention legislation against unlicensed accessory vendors.[35]

The Defendant was selling the "neo 4" mod chips. These chips evaded the TPMs in the PlayStation2 console, so that the console could read pirated discs. This also meant that the console could read original Sony disks imported from countries with different region codes to the console; [36] disks containing games produced by other companies; back-up copies of original Sony discs; as well as disks containing programs other than games, so that the console could be used as a personal computer. The Defendant advertised the aforementioned mod chips in the site "hardstore.com".

The proceedings followed the seizure of modified consoles, mod chips, and related material, initiated by Sony, who later joined the penal proceedings as civil party (Party Civile). The seizure was based on Article 171ter (f) bis of the law on author's rights (Lda)[37], which implemented Article 6(2) of the Information Society Directive in Italian law.

Article 171ter (f) bis Lda provides that "it is an offence to make, import, distribute, sell, rent, transfer in any other way, advertise for sale or rental, possess for commercial purposes devices, products, or components or offer services *which have as their predominant purpose or commercial use to avoid effective technical protection measures or which are principally designed, produced, adapted, or put into effect for the purpose of making possible or facilitating the avoidance of such measures*" [emphasis added].

The Defendant responded that Article 171ter (f) bis Lda did not apply because the PlayStation2 Console was a "computer" and the games played were "computer programs"; thus, Article 171bis should apply instead. The nature of computer games as programs is crucial, because under Article 171bis, which implemented the Software Directive, liability can be established only if the sole function of the infringing device is to overcome the TPMs protecting the computer program. In contrast, under Article 171ter, which implemented the Information Society Directive and applies to TPMs protecting copyright works other than computer programs, a device infringes the law if its main purpose is to overcome TPMs.

Furthermore, the Defendant argued that, even if Article 171ter were to apply, the "predominant purpose or commercial use to avoid TPMs" requirement of the provision would not be satisfied, as the main function of the mod chip was to overcome monopolistic obstacles and to make better use of the console. Moreover, the Defendant claimed that according to the correct interpretation of Article 102quarter Lda, the protection of TPMs applies only if the function of the TPMs is to prevent copyright infringement and since Sony's TPMs did not serve this purpose, they should not enjoy legal protection.[38] Finally, it claimed that the contractual conditions limiting use contained within the packaging of the console were ineffective as all the terms of the contract must be known or knowable to the purchaser at the time of the formation of the contract for sale.

The proceedings followed the seizure of modified consoles, mod chips, and related material. An interlocutory decision was issued upholding the Defendant's

arguments; but, when the case was tried, the First Instance Court found in favour of Sony. This decision was appealed and reversed by the Court of Appeals. Finally, the case reached the Supreme Court of Italy.

The Sezione per il riesame, in its interlocutory decision of December 31, 2003 found in favour of the Defendant in an effort to protect competition in the market for video games and to advance consumer welfare and consumer choice.[39] The Court held that circumventing effective TPMs was not the main use of the mod chips, because the devices also had other legal uses. The Court also noted that the Defendant had not violated the Italian anticircumvention law, because its acts did not violate Sony's copyrights. Finally, the Court also held that there was no apparent reason why the purchaser of a console should be restricted as to its use through Sony's protection measures[40] and that the contractual terms that Sony imposed on its users were ineffective.

The First Instance Court found Article 171ter (f) bis applicable. It did so by holding that the console was not a "computer" and that the video games were not "programs". This was because they involve images, sounds and text. Since computer games should be appropriately regarded as copyright works, to which TPMs can be attached, the Court concluded that the defendant's behaviour should be assessed under Article 171ter.[41] Furthermore, the court held that protection of TPMs is offered independently of whether they protect author's rights, quoting directly from Art. 102.[42] Finally, the court held that the "predominant purpose to circumvent" requirement of Article 171ter (f)bis was satisfied. The Court accepted that Article 171ter envisages possible legitimate uses for devices, which also have the effect of overcoming TPMs and it rejected as illegitimate all the alternative uses suggested by the defendant.[43]

The Court of Appeals was more receptive to the defendant's arguments.[44] The Court held the PlayStation2 console to be a computer and the programs played on it to be computer programs. This meant that Article 171ter applied. That provision required proof that the only purpose of the mod chip was to overcome TPMs. That condition was not satisfied in this case because reading the back-up copy was permitted under Italian law. The Court further held that only the TPMs, which protected the author's rights were protected.

The Corte di Cassazione in the decision 3368/2007 of the Terza Sezione reversed the Court of Appeal's decision.[45] The Supreme Court held that Sony's video

games were not software programs, since the definition provided in Article 171 ter (d) better suited them. Thus, in order for the defendant to be found guilty, Sony only needed to prove the lower standard: that the mod chips' primary use was to overcome its TPMs.

Further, the Supreme Court overruled the Court of Appeal's finding that TPMs are protected only when they prevent copyright infringement and establish a right of access. The Supreme Court emphasized that article 102 of law 633/1941 had to be interpreted so as to protect the entirety of TPMs, including those in 171ter (F) which covered all TPMs designed to prevent acts that are not authorized by the copyright holder.

Courts in Italy have followed the Supreme Court decision. This is demonstrated by a recent decision of the Tribunale di Milano.[46] Following the same reasoning as the Supreme Court, the industrial and intellectual property division of the Tribunale ordered the seizure of mod chips, available from PCBox on the grounds that they violated the TPMs of Nintendo. The judge held that, since the primary function of the Mod chip is to read games that are copied, the chips should be confiscated.

Both the interlocutory decision as well as the decision of the Court of Appeals tried to provide an interpretation that would favour healthy competition in the market for video games and would advance consumer welfare and consumer choice. However, the Supreme Court held such an interpretation deviates from the spirit of the Information Society Directive. Although it may seem desirable that, in cases of extreme abuse of anticircumvention regulations by copyright holders, the European Courts should find in favour of healthy competition, the existing legal framework and judicial precedent create the wrong incentives. They do so by deterring competitors from engaging in practices that would enable them to enter into a market but risk liability under anticircumvention law.

3.2. Jurisprudence on the DMCA anticircumvention provisions

There is a common understanding among the critics of the DMCA that early litigation interpreting the statute expanded the definition of TPMs to such an extent that even modest innovations that could not qualify for patent protection would receive patent-like protection through anticircumvention laws.[47] However, it has been claimed that subsequent judicial interpretation has alleviated these dangers, and that the courts

have struck the right balance between innovator's interests and permitting public access and enhancing overall social welfare.[48] It will be demonstrated that, even after these new decisions, which seem to recognize some of the negative consequences of an overbroad application of the DMCA, the existing law can still discourage innovation and limit competition in the market.

Sony Computer Entertainment America, Inc. v. Gamemasters

One of the first cases to interpret the DMCA was *Sony Computer Entertainment America, Inc. v. Gamemasters*.[49] The video game manufacturer, Sony, sued Gamemasters for violating the DMCA. Gamemasters were selling a technology, called "Game Enhancer" that enabled players to modify Sony's Playstation. The court held that Game Enhancer violated the DMCA because its primary function was to circumvent a TPM, in particular the console's territory code mechanism. The court further held that the plaintiffs did not need to show copyright infringement.[50] Thus, although protection against piracy was not an issue in this case - which is the main objective that the DMCA is supposed to serve - the Court acknowledged that Sony had a right, broader than the rights conferred by copyright law, to control the uses of its work. The effect of that right was to permit Sony to restrict the development of new technologies.

Universal Studios v. Reimerdes

Universal Studios v. Reimerdes is another important case shaping the interpretation of the DMCA, as the District Court offered expansive readings of the DMCA's liability provisions and narrow interpretations of its various defences.[51] Motion picture studios brought action under the DMCA to enjoin an Internet web-site owner, Corley, from posting for downloading computer software that decrypted digitally encrypted movies on DVDs and from including hyperlinks to other web-sites that made decryption software available.[52]

The District Court held that DVD-copying programs violated the DMCA, despite the fact that they may have legitimate end uses and it enjoined their manufacture and sale.[53] Furthermore, it held that a technology can be found illegal independently under the Section 1201 of the DMCA, regardless of whether copyright infringement occurs.[54] As regards the interpretation of the interoperability exception, the District Court found Section 1201(f) inapplicable, as the provisions applies only to

the circumvention of TPMs that restrict the access to computer programs, not copyright works generally.[55] The Court further heightened the "sole" purpose for achieving interoperability requirement of the Section 1201(f)[56] and it, additionally, found the public distribution of exempted tools and information under Section 1201(f) unlawful. A s *Reimerdes* offered the sole judicial analysis of the interoperability exception until *Davidson*[57] was decided in 2004, the court's reasoning when rejecting the Section 1201(f) defence is of great interest.[58]

Rejecting the interoperability exemption on the basis that CSS[59] restricted access to movies stored on DVDs, is fully supported by the text of the provision that permits the circumvention of TPMs to "a person who has lawfully obtained the right to use a copy of a *computer program"* (*emphasis added*).[60] However, heightening the sole purpose requirement of Section 1201(f) and limiting the distribution of interoperability information and circumvention tools indicated scepticism from the court towards the statutory exception. To elaborate, the court held that the sole purpose requirement demands the plaintiff to show that interoperability is necessary to access or use a work, without baring the burden of actually proving the *purpose* of development of the circumventing device. [61] Second, the court ignored the language of Section 1201(f)(3) and held that the statute permitted dissemination of information obtained through reverse engineering, but *not the means of circumvention used to obtain such information*.[62] Finally, the court erred in imposing a blanket rule against the public distribution of exempted tools and information, despite the fact that DMCA contains no freestanding limit on the scope of distribution. More specifically, the court claimed that DMCA permits the sharing of interoperability information only by one who acquires that information. Such an interpretation, though, prevents publication of interoperability tools and information for a variety of purposes, including academic research.[63]

Although Section 1201(f) premises the safe harbour of the interoperability exception under really narrow requirements, the District Court's interpretation in *Reimerdes* raised the bar for the applicability of those requirements even higher. The combination of the narrow requirements of Section 1201(f) and their judicial interpretation in favour of copyright holders has nullified the importance of the statutory exception. The fact that no defendant has yet succeeded in a Section 1201(f) defence supports this argument. Thus, the interoperability exception failed to deter copyright holders from employing TPMs to restrict the development, distribution and

use of interoperable technologies; on the contrary the judicial interpretation of Section 1201(f) in *Reimerdes* emboldened plaintiffs to test the bounds of their control over interoperable products.[64] Lexmark's, Chamberlain's and Storage Technology's attempts to increase their market power by employing TPMs were the result of the early judicial reading of DMCA as demonstrated above.

Lexmark Int'l, Inc. v. Static Control Components

In *Lexmark Int'l, Inc. v. Static Control Components*, a major manufacturer of laser and inkjet printers who was also active in the market for cartridges for printers, attempted to enjoin its competitor, Static Control Components (SCC), from providing consumers with cartridges for the Lexmark printers by invoking the DMCA.[65] Lexmark sold prebate cartridges at a deep discount in exchange for an agreement that consumers would use the cartridge only once and it employed a TPM intended to prevent unauthorized cartridges from interoperating with its printers.[66] Defendant, SCC, had created the SMARTEK chip, which mimicked Lexmark's authentication sequence and could bypass Lexmark's TPM. Lexmark alleged that SCC was trafficking in a circumvention device,[67] and sought to enjoin it from selling cartridges with SMARTEK chip. The District Court granted Landmark's request for a preliminary injunction,[68] but the Sixth Circuit reversed. The court held that access to the Lexmark's copyright software wasn't controlled by the authentication sequence, but by the purchase of a Lexmark printer because the authentication sequence wasn't encrypted or otherwise protected against literal copying.[69] Since the authentication sequence did not meaningfully control access to the code, the DMCA did not apply.[70]

Although *Lexmark* narrowed the scope of the DMCA by conditioning its application upon the robust protection of the copyright work by TPMs[71], it could allow future plaintiffs to succeed under slightly different facts, if they ensure that their TPM is effective.[72] Likewise, both *Chamberlain Group, Inc., v. Skylink Techs* [73] and *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.* [74] narrowed the scope of the DMCA, this time by requiring a nexus between the access facilitated by the TPM and the protection of a legitimate copyright interest. However, the courts did not offer enough guidance as to the factual and legal predicates necessary for liability under the nexus requirement.[75]

Chamberlain Group, Inc., v. Skylink Techs

Chamberlain, a Garage door opener (GDO) manufacturer, sued Skylink, a manufacturer of universal remote transmitters for patent infringement and violation of DMCA. Chamberlain alleged that the rolling code used in its GDOs protected access to the copyright code that operated the GDOs and that Skylink transmitters permitted unauthorized access to the software that operated Chamberlain's GDOs, by imitating the rolling code. The United States District Court for the Northern District of Illinois entered summary judgement in favour of defendant on the DMCA claim, holding that consumers who purchased Chamberlain products were entitled to access the GDO software, and Chamberlain appealed.

The Federal Circuit agreed that Chamberlain customers possessed an "inherent legal right to use" the software embedded in the GDOs.[76] Furthermore, addressing an issue of first impression the court of appeals held that for DMCA to apply, a plaintiff must establish that the circumvention of that TPM bears some "reasonable relationship to the protection that the Copyright Act otherwise affords."[77] Since consumers were entitled to access the GDO software, Chamberlain was unable to prove the critical nexus between the access facilitated by Skylink's device and the protection of a legitimate copyright interest.[78] In the same line of thought the Federal Circuit held in *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.,* that "to the extend that rights under copyright law are not at risk, the DMCA does not create a new source of liability ".[79]

Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.

Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintenance code using a password protection scheme. As defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries, Storage Technologies sued invoking Section 1201(a) (1) of the DMCA. Although the district court issued preliminary injunction, the Federal Circuit mandated. The court found it unlikely that Plaintiff would be able to prove that the circumvention password "either infringes or facilitates infringing a right protected by the Copyright Act'.[80]

Despite the fact that both *Chamberlain* and *Storage* should be praised for resisting the expansive interpretation of the DMCA embodied in *Reimerdes*, the two

decisions didn't clarify the circumstances under which the nexus requirement with copyright infringement will exist. This uncertainty may affect the application of the nexus requirement in cases concerning "entertainment" or "informational" goods, when it is not equally obvious that the copyright holders are trying to promote a profitable business model rather than protect their rights. Thus, there is a higher risk that courts will disregard the fact that copyright holders misuse TPMs to hamper competition in markets of more "artistic" copyright works.

Davidson & Assocs. v. Internet Gateway

Davidson & Assocs. V. Internet Gateway [81], decided only one year after the *Lexmark* and *Chamberlain* decisions were issued, draws away from their line of thought and takes a step back towards *Reimerdes*.

Blizzard, the owner of copyrights in computer game software and online gaming service software, offered an online matchmaking service, Battle.net that allowed players to compete over the internet. Battle.net relied on a secret handshake with Blizzard games to validate unique CD keys. Defendants (bunted team) reverse engineered the protocols used by Blizzard games to communicate with Battle.net and developed alternative service software that interoperated with Blizzard games. However, since bnetd lacked access to Blizzard's database of CD keys, it was unable to ensure that all players used legitimate copies of Blizzard games. Blizzard sued the bnetd for breach of contract, circumvention of copyright protection system, and trafficking in circumvention technology. In response, Bnetd raised the interoperability exception as one of its defences, arguing that any circumvention of Blizzard's access controls occurred to enable reverse engineering meant to render the bnetd server software interoperable with Blizzard games and any tools it distributed that facilitated circumvention were intended to enable interoperability. [82]

The district court rejected bnetd's Section 1201(f) defence arguing that, first, bnetd lacked permission to circumvent[83], secondly, the sole purpose of bnetd's circumvention was to "avoid the anticircumvention restrictions of the game and to avoid the restricted access to Battle.net"[84] and third because bnetd server was not an independently created computer program, since it was intended as a functional alternative to the Battle.net service, one that was indistinguishable from Battle.net from the standpoint of the users. [85]

The district court's analysis was flawed, resulting into practically nullifying the interoperability exception, even for defendants that fall squarely within the protections for reverse engineering and interoperability. Firstly, under the court's holding that bnetd could benefit from the interoperability exception only if it had permission to circumvent, Section 1201(f) becomes redundant, and as if bnetd had permission an affirmative defence would be unnecessary. Besides, by holding that the sole purpose of the bnetd's circumvention was to avoid the anticircumvention restrictions, the court falls into a dangerous tautology; the circumventor's goal is always going to be to circumvent. Finally, the fact that bnetd server was intended as a functional alternative to the Battle.net service, that was indistinguishable from Battle.net, simply means that bnetd was successful in its attempt to enable interoperability, not that the bnetd server was not an independently created computer, as the court held.[86]

On appeal, the Eight Circuit, affirmed the district court's decision and held that bnetd's circumvention constituted infringement because unauthorized games of Blizzard games can be played on the server. The court erred in its holding, as the fact that some users connected to the bnetd server using unauthorized copies of Blizzard games does not prove that bnetd infringed Blizzard's rights under Section 106.

The day after Lexmark, Chamberlain, Storage and Davidson

Lexmark, *Chamberlain* and *Storage* were all motivated by common concerns; the impetus behind them was an effort to restore competition in the market and allow interoperability. The courts realized that the companies were not interested into protecting their code from unauthorized access or copying, but were rather trying to promote a profitable business model and take advantage of the anticircumvention regulation to increase their market share.[87]

The same concerns though could be true in cases of manufacturers and vendors of products from the entertainment industry. Courts, however, have failed to apply a similar approach that addresses the interests of competitors and consumers in cases involving the use of TPMs to protect "informational" or "entertaining" works. *Davidson* indicates that courts may issue their decisions focusing on an evaluation of the risk of piracy disregarding the potential of distorting competition and follow an expansive or restrained application of the DMCA's liability provisions accordingly. If this ascertainment is true, we should hold our reservations as to the extend that the

holding of the Lexmark, the Chamberlain and Storage holdings apply outside of the domain of tangible articles of commerce.

The approach that courts seem to follow, though, protects the interests of competitors and consumers in rather mundane commodities but fails to do the same for cultural artefacts.[88] The social harms generated by anticompetitive conduct in markets for informational and artistic goods are much higher. The traditional goal of Intellectual Property doctrine has been to provide incentives for the creation of as many and as diversified creative works as possible. Raising barriers to entry in markets of copyright works risks the quality and quantity of the produced works. Having a limited number of dominant firms controlling the production of creative works hinders the development of our culture and our civilization. Anticircumvention regulation steadily leads to concentration in the creative markets, a goal that directly opposes the "progress of sciences and useful arts".

4. The application of competition law and the misuse of anticircumvention legislation

Anticompetitive conduct issues are resolved as a rule by competition law in both sides of the Atlantic. As intellectual property rights, though, constitute limited monopolies, safeguards of healthy competition in the market are embedded within the intellectual property doctrine. Still, competition law authorities have intervened in the past in various occasions when intellectual property right holders have misused their monopoly power in expense of the market, especially in the EU.[89] As the misuse of anticircumvention legislation by the right holders harms competition in the adjacent markets at a cost to innovation and consumer welfare, it would be interesting to examine whether competition law could limit the control that TPMs yield over interoperable technologies. After all, competition law remedies and particularly the mandatory disclosure of technical information and the obligation to deal could facilitate interoperability.

In favour of relying on competition law to enable interoperability is the fact that courts and competition law authorities are less likely to be influenced by the lobbying efforts of the entertainment and software industry and thus may be more likely to strike the right balance between creative incentives and the creation of a robust public domain.[90] In addition, it has been argued that competition law allows

for forward-looking remedies that may guard against technological efforts to disrupt healthy competition in the market.[91] Of course, it should be noted that some scholars and courts have argued that courts are ill suited to assume the day to day control of the enforcement of the remedy.[92] However, the most significant practical disadvantage of relying on competition law to "correct" the implications of anticircumvention regulation is timing. In innovation markets, the ability for the authorities to interfere immediately and restore healthy competition is fundamental, because of the network effects that are created in the market. If consumer lock-in has already occurred, it is very hard to undo the consequences of an anticompetitive practice.[93] Amending anticircumvention legislation itself, and thus fixing the source of the problem, so that the Intellectual Property regime would afford developers and vendors of interoperable products immediate self-help is far preferable to providing them with competition law remedies some years subsequently.[94]

More importantly, because of the way that competition law doctrine and jurisprudence is formulated on both sides of the Atlantic, competition law appears unlikely to disturb the enforcement of the broad grants provided by anticircumvention regulation, for two basic reasons. First, both Section 2 of the Sherman Act and Article 102 TFEU impose a minimum threshold of market power in order to hold a conduct as anticompetitive. Secondly, competition law gives substantial deference to the lawful exercise of legitimately acquired intellectual property rights, especially in the United States.

The decision to exclude from the operation of the law competitors who do not have a dominant position and monopoly power in the relevant markets does not mean that the conduct of those competitors does not hinder competition. The condition of dominant position and monopoly power exists to ensure that competition law will not lead to over-deterrence of firms from engaging in the competitive process. Market power is solely an indication of the likelihood of anticompetitive effects.[95] The market power condition is important. Otherwise, all firms would risk violating competition law. Such a risk stifles desirable business activity because anti-competitive effect is not always easy to discern ex ante. For this reason competition law chooses to examine the conduct of firms only when they are most likely to engage in anticompetitive practices.[96] Therefore, to avoid over-deterrence, lawmakers are willing to permit *some* anticompetitive behaviors. However, as argued above, timing

is crucial in innovation markets. This means that when a competitor unlawfully gains a dominant position, it may be too late for the authorities to intervene.

Thus, competition law rules are too rigid to apply efficiently in cases of anticompetitive misuse of the anticircumvention provisions, pointing to the conclusion that these anticompetitive behaviours should be dealt with inside the field of anticircumvention law.

5. The need for amendment of the anticircumvention provisions

5.1. European Union

Since judicial interpretation of the European anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy on the one hand with fragmenting the market on the other and since competition law is not capable of restoring this balance an amendment of the existing legislation at an EU level seems indispensable.

Substantively, it is suggested that the Community legislator should limit the protection of TPMs to copy controls and add an explicit requirement that a circumventor of a TPM can infringe the anticircumvention regulation only if her act is a violation of a valid copyright or neighbouring right. Such a modulation would limit the effects of anticircumvention regulation to combating piracy and would not provide to copyright holders an additional right to control all the uses of their works in the digital environment by taking away this right from the public. This proposed amendment is congruent with the traditional theory of Intellectual Property law, according to which, copyright constitutes a limited exception to the right of the public to have access to creative works.

Furthermore, the requirement of the Software Directive that for a device to be held as violating the anticircumvention regulation sole purpose should be to circumvent an effective TPM should be extended to the Information Society Directive; alternatively the ECJ should interpret the “limited commercially significant purpose or use other than to circumvent” requirement in way that legalizes the circumvention of TPMs to achieve lawful purposes that enhance the uses of the copyright works and raise barriers to entry. Under such a legal regime competitors will be able to break the technical barriers to entry into new markets that first comers or dominant firms in adjacent markets raise.

Turning now to the exceptions to copyrights, the following major changes appear as essential. Firstly, all the exceptions to rights on copyright works that a Member States provides should automatically apply with respect to TPMs; secondly, the exceptions should constitute exceptions to the liability of circumvention of the TPMs.[97]

Of course if the violation of anticircumvention legislation becomes dependant upon a violation of copyright law by the circumventor, the latter modification would be redundant; to elaborate, despite the fact that access or copying the copyright work would be legally protected by the TPM, the beneficiary of an exception will be entitled to access or copy it and thus she will not be violating copyright law or neighbouring rights. Consequently, as the beneficiary will not be violating copyright law, she will not be violating the anticircumvention provisions either. If the anticircumvention legislation, though, does not have an auxiliary character to copyright law, and it provides a further right to the copyright holder to control the uses of copyright work, as it does today, it is crucial that the legislation at least ensures that the beneficiaries of exceptions to copyright are not forfeited by their rights.

Moreover, the exceptions in the Information Society Directive also do not include reverse engineering, [98] although such an exception exists in the Software Directive, which provides a limited safe harbour for those trying to achieve software interoperability.[99] From the Recitals of the Software directive and from its legislative history we can infer that the Community legislator wanted to encourage connecting all components of a computer system, including those of different manufacturers, so that they can work together.[100] The cooperation between manufacturers is a noble objective also in the fields of traditional copyright goods. Through cooperation of authors of artistic works the output of such works will increase creating a richer and fuller culture for European Citizens. The exclusive focus of this exception on computer programs must be abandoned in favour of an exception that applies in all classes of copyright works, recognizing the role that data plays in enabling system-level interoperability.[101]

Finally, it is crucial for European Union not to differentiate the treatment of tangible articles of commerce and to cultural artefacts. All the aforementioned substantive amendments, thus explicitly requiring “violation of a valid copyright or neighbouring right” for the affirmation of infringement of anticircumvention

regulation, introducing the "sole purpose to circumvent an effective TPM" requirement for the affirmation of infringement of anticircumvention regulation and introducing an "interoperability exception" should apply equally to consumer electronics products and informational and entertaining goods.

5.2. United States

After *Lexmark*, *Chamberlain* and *Storage Technologies* courts have tried to narrow the scope of the DMCA by demanding a nexus between a copyright violation and a DMCA infringement, and expanding the "effective restriction of access to copyright works" requirement for the protection of TPMs. However, courts may abandon this approach in the case of manufacturers of goods that fall under the traditional definition of copyright works.[102]

Thus, the legislator is the appropriate organ to balance the need for protection of copyright works on the one hand with the need to safeguard healthy competition in the "creative" markets. The scale should turn towards healthy competition, as innovation can be achieved only within a free market. Furthermore, a dispersed market of creative works advances diversification and variety in the arts and culture and promotes the development of civilization. Thus, the legislator should amend the DMCA to ensure that it does not lead to the creation of further monopolies, which the legislator initially did not aim to protect and that are not subject to the restraints imposed on Intellectual Property rights. After all, over-incentivizing authors of 'creative' works can have reverse effects than the ones expected, since when the level of protection is too high, creation and innovation are impeded rather than promoted.

In order to achieve the right balance between protecting competition in the secondary markets and promoting the interests of copyright holders the legislator should amend the DMCA in the following ways:

Firstly, a clause should be added that would ban the differential treatment of tangible articles of commerce and cultural artefacts and that shall instruct courts to apply all the provisions of the DMCA equally to both kinds of works.

Secondly, the legislator should explicitly condition the three causes of action of Section 1201 under the infringement of a valid copyright. The plaintiff should bare the burden of proving that her copyrights are infringed.

Thirdly, Section 1201(f) should be amended to explicitly create a safe harbour for circumventing TPMs protecting all kinds of copyright works and to protect data operability as well.

The most important consequence of the legislative intervention is that it will create a safety regarding the actions that a competitor is allowed to undertake, thus promoting competition and innovation. Furthermore, the altered legislative environment will discourage copyright holders from misusing TPMs in the detriment of their competitors and of consumer welfare. The power that the legislator has to form behaviors can not be compared with the effects of judicial intervention. This power makes an amendment of the law urgent as the disparity of decisions and the broad holdings have created an uncertainty that encourages anticompetitive conducts by copyright holders.

6. Concluding remarks

Academics have been warning for a long time that intellectual property laws are being rewritten in ways that neglect values embedded in neighbouring legal fields, such as contract, competition and free speech law. [103] Anticircumvention regulation constitutes an example of such move away from the traditional Intellectual Property law. It strengthens the rights of copyright holders at the expense of healthy competition and consumer welfare. As a result of anticircumvention regulation copyright owners enjoy three cumulative layers of protection: the legal protection of copyright law, the technical protection of their works achieved by TPMs and the legal protection against the circumvention of the TPMs.

Vendors and manufacturers of consumer primary products, who hold a dominant position in the primary product market, can use anticircumventionregulation in order to reinforce their dominant market position in the aftermarket by preventing interoperability of products on alternative systems. Unfortunately (The) judicial interpretation of the EU and US anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy on the one hand with fragmenting the market on the other and competition law is not capable of restoring this balance; Therefore, the existing legislation at an EU level as well as in the US needs to be amended. On the one hand, the infringement of the anticircumvention norms should be explicitly conditioned to the infringement of a valid copyright and on the other

there should be no differentiation in the treatment of tangible articles of commerce and cultural artifacts and courts should be instructed to apply all exceptions equally to both categories of works.

It is important to keep in mind that, just like any technology, TPMs are in themselves neutral; but, when used, are capable of both producing both “good” and “bad”. However anticircumvention regulation on both sides of the Atlantic allows, if it does not encourage, uses of TPMs that reduce consumer welfare and harm competition and thus it needs to be amended.

[1] For a detailed definition and description of TPMs see K.J. Koelman &N. Helberger, 'Protection of Technological Measures' in P. B. Hugenholtz (ed.) *Copyright and Electronic Commerce* (1998), p.168,172; A. Strowel &S. Dusollier, 'La protection legale des systemes techniques' in WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), WIPO doc WCT-WPPT/IMP/2, p.2.; J. DeWerra, 'The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other national laws (Japan, Australia)', Contribution to the ALAI 2001 Congress on Adjuncts and Alternatives to Copyright.

[2] M. Ficsor, *The Law of Copyright and the Internet, The 1996 WIPO Treaties, their Interpretation and Implementation,* (2002), p.544, S. Ricketson & J. Ginsburg, *International Copyright and Neighbouring Rights, The Berne Convention and Beyond,* (2006), p.965.

[3] See Article 11 WCT and 18 WPPT.

[4] Indicatively see C. Clark, 'The Answer to the Machine is in the Machine', in P. B. Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* (1996), p.139; A. Dixon &L. Self, 'Copyright Protection for the Information Superhighway' 11 *EIPR* 465(1994); J. C. Ginsburg, 'Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright Cyberspace', 95 *Columbia Law Review* 1466 (1995); B. Lehman, 'Intellectual Property and the National and Global Information Infrastructures' in P. B. Hugenholtz (ed.) *The Future of Copyright in a Digital Environment* (1996), 103

[5] Indicatively see Y. Benkler, 'Free As the Air To Common Use: First Amendment Constraints on the Enclosure of the Public Domain',74 *N.Y.U. Law Review* 354 (1999); J. E. Cohen, 'Copyright and the Jurisprudence of Self-Help', 13 *Berkeley Tech. L. J.* 1089 (1998); Ibid., 'A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace', 28 *Connecticut Law Review* 981 (1996); Ibid., 'Some Reflections on Copyright Management Systems and Laws Designed to Protect them', 12 *Berkeley Tech. L. J.* 161 (1997); S. Dusollier, 'Tipping the Scale in Favour of the Right Holders: The European anticircumvention Provisions', in E. Becker, W. Buhse, D. Günnewig, N. Rump (eds.) *Digital Rights Management. Technological, Economic, Legal and Political Aspects* (2003) 462; K.J. Koelman, 'A Hard Nut to Crack: the Protection of Technological Measures' 22(6) *EIPR* 272 (2000), at 275; J. Litman, *Digital Copyright* (2006); Ibid., 'Sharing and Stealing' 27 *Hastings Communications and Entertainment L. J.* 1 (2004); N. W. Netanel, 'Locating Copyright Within the First Amendment Skein', 54 *Stanford Law Review* 1 (2001); P. Samuelson, 'Intellectual Property and the Digital Economy: Why the anticircumventionRegulations Need to be Revised', 14 *Berkeley Tech. L. J.* 519 (1999); T. C. Vinje, 'A Brave New World of Technical Protection Systems: Will There Still be room for copyright', 18 *EIPR* 431 (1996); G. Westkamp, 'Transient Copying And Public Communications: The Creeping Evolution Of Use And Access Rights In European Copyright Law' 36 *George Washington International Law Review* 1057 (2004), at 1078.

[6] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 530 (6th Cir. 2004).

[7] Many printer cartridges come with chips that authenticate them to the printer, a practice that started in 1996 with the Xerox N24. In a typical system, if the printer senses a third-party cartridge, or a relled cartridge, it may silently downgrade from 1200 dpi to 300 dpi, or even refuse to work at all. An even more recent development is the use of expiry dates. Cartridges for the HP BusinessJet 2200C expire after being in the printer for 30 months, or 4.5 years after manufacture. See Ross Anderson, *Cryptography and Competition Policy – Issues with "Trusted Computing"*, 1, available at: http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf

[8] Among them, Apple's use of the "chain of Trust" in its popular iPhone device that prevents subscribers from installing applications from third parties is worth mentioning.

[9] The term effective is circularly defined as "an access control or protection process" which "achieves the protection objective", Article 6(3) of the Information Society Directive.

[10] Article 6(1) of the Information Society 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 is pursuing that objective.", whereas Article 6(2) of the Directive provides that "Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention 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."

[11] A linklist to international and national legislation on technological protection measures with focus on the relevant laws of EU member states has been made available at <http://cyber.law.harvard.edu/media/eucd> by the Berkman Center's Digital Media Project team. As regards the failure of the Information Society Directive to efficiently harmonize European law, which after all was the impetus behind the directive, especially in regard to the exceptions of TPMs legal protection see B. W. Elser, Technological Self-Help: Its Status under European Law and Implications for U.K. Law, BILETA, 17th BILETA Annual Conference, April 5th -6th, 2002, Free University of Amsterdam, p. 12 available at: http://www.bileta.ac.uk/02papers/esler.html in PETER PRESCOTT ET AL., THE MODERN LAW OF COPYRIGHT, Ch.

20 (3rd Ed. 2000), at 12.
[12] On the definition of TPMs in Article 6(3) of the Information Society Directive see above note 2
[13] Urs Gasser, Michael Girsberger, *Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States. A Genie Stuck in the Bottle?,* Berkman Publication No. 2004-10, available at: http://cyber.law.harvard.edu/publications,
[14] Article 6(4) and Articles 5(2)(a), 5(2)(c), 5(2)(d), 5(2)(e), 5(3)(a), 5(3)(b) and 5(3)(e) of the Information Society Directive. For a critical comment on Art. 6(4) see Dussolier, Exceptions and technological measures in the European Copyright Directive of 2001 – an empty promise, 34 I.I.C.62 et.seq (2003)
[15] Information Society Directive, Recitals 51-53.
[16] Nora Braun, *The Interface between the protection of the Technological Measures and the Exercise of Exceptions to Copyright and Related Rights: Comparing the Situation in the United States and the European Community*, 25 E.I.P.R. 11, 496, 499 (2003).
[17] Information Society Directive Article 6(4) and Recital 50. The enactment of exceptions to TPMs conditioned upon "the absence of voluntary measures taken by right holders" has been criticized as "making law making power contingent upon the acquiescence of corporate and private interests" and that "rightholders[…] may use Article 6(4) as a sword of Damocles over the heads of national legislatures, threatening them with challenges to their authority to govern the scope of copyright and its related rights. " B. W. Elser, supra note 11 at 12.
[18] Esler, *supra* note 11, at 12, arguing that "Without Article 6(4), it would be clear – pursuant to Article's 6(3) definition of "technological measures" – that any exceptions adopted would apply equally to TPM circumvention, i.e. circumvention in furtherance of an exception would not fall afoul of the law. By calling out eight specific exceptions which must be applied (at least "in the absence of voluntary measures taken by right holders, the clear implication is that other exceptions do not have to apply with respect to TPMs.)". However, we should note that Elser believes that "it would make more sense to apply all exceptions equally to TPMs" and suggests that the UK should do so.
[19] Cf Article 5 with Article 6(4).
[20] Access controls are TMPs intended to prevent unauthorized access to copyright works, or according to the wording of 17 U.S.C. 1201(a)(3)(B) "*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*".
[21] Copy controls are TPMs intended to prevent infringement of the exclusive right afforded by copyright, or according to the wording of 17 U.S.C. 1201(b)(2)(B) "*in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title"*
[22] Section 1201(a)(3)(A) defines anticircumvention as descrambling a scrambled work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing a technological measure, without the authority of the copyright owner.
[23] The DMCA provides both civil remedies and criminal sanctions for the violation of the aforementioned provisions. Violators will be sued in front of the federal court [17 U.S.C. Section 1203(a)] and the complaining party may elect to receive either the sum of the actual damages it suffered and the additional profits earned by the violator, or statutory damages [Id. para 1203(c)]. In addition to that, violators that are prosecuted criminally may face sanctions up to a USD 500,000 fine and five-year imprisonment for any para 1201 and the penalty will be doubled for a second violation [Id. para. 1203(c) and 1203(a)]
[24] The exemptions from anticircumvention provisions include conducting encryption research (17 U.S.C. Section 1201(g)), assessing product interoperability (Section 1201(f)) and testing computer security systems (Section 1201(j)). Exemptions under narrow circumstances are also provided for nonprofit libraries, archives and educational institutions "solely to make a good faith determination of whether to acquire a copy of that work" (Section 1201(d)).
[25] For the congressional recognition of the permissibility of reverse engineering and the value of interoperability, see S. Rep. 105-190, at 32 (1998).
[26] Section 1201(f)(1).
[27] Section 1201(f)(3).
[28] See *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, at 218 (S.D.N.Y. 2000); the Court rejected defendant's 1201(f) defence holding that the interoperability exception applies only to the circumvention of TPMs that restrict access to computer programs, not copyright works generally. For a discussion of the shortcomings of Section 1201(f) and why the statute needs to protect all interoperable technologies. Furthermore, the interoperability restriction fails to accommodate reverse engineering for other legitimate purposes. For example 1201(f) is not applicable in the cases of reverse engineers who extract uncopyrightable processes and principles to create non-interoperable products, or in the case of researchers who investigate the operation of TPMs. As regards the latter, although the encryption research and the security testing exceptions offer researchers some protection, the conditions set by Sections 1201(f) and (g) are very strict. For a discussion of the impact of Section 1201(g) on encryption research, see Joseph P. Liu, *The DMCA and the Regulation of Scientific Research,* 18 Berkeley Tech. L. J. 501 (2003). For a discussion of the benefits to the public that TPM research can offer outside of the encryption context see K. Mulligan & Aaron K. Perzanowski, *The Magnificence of a Disaster: Reconstructing the Sony*

BMG Rootkit Incident, 2 2 BERKELEY TECH. L. J. 1157 (2007) and Comment of J. Alex Halderman, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8 http://www.copyright.gov/1201/2008/comments /halderman-reid.pdf.

[29] However, a case is pending in front of the ECJ

[30] The European Court of Justice has issued decisions against Portugal (Case C-61/05), Spain (Case C-31/04), France (Case C-59/04), United Kingdom (Case C-88/04), Finland (Case C-56/04), Sweden (Case C-91/04) and Belgium (Case C-143/04) because they failed to adopt the laws, regulations and administrative provisions necessary to comply with the Information Society Directive.

[31] For example the Court of Fist Instance took into account emails sent to the defendant that showed that the principal purpose for which the mod chip was sought was to enable the playing of illegally copied games.

[32] The Sezione per il riesame, in its interlocutory decision of December 31, 2003 held that the main function of the mod chip was to overcome "monopolistic obstacles and to make a better use of the console". The Court of Appeals held that the use of the chip allowed the use of the console to its full potential.

[33] For the financial data regarding the video gaming industry see: ROBERT W. CRANDALL & J. GREGORY SIDAK, VIDEO GAMES: SERIOUS BUSINESS FOR AMERICA'S ECONOMY § 2, at 7 (2006), available at *:* http://papers.ssm.com/sol3/papers.cfm?_abstract_id=969728.For a discussion of gaming culture and social norms and their evolution as well as the methods that the gaming industry has employed to alter these norms see: Corinne L. Miller, *The Video Game Industry and Video Game Culture Dichotomy: Reconciling Gaming Culture Norms With the anticircumvention Measures of the DMCA*, 452 TEXAS INTELLECTUAL PROPERTY L. J. 16.

[34] Anderson, *supra* note 7.

[35] Sony has succeeded in preventing the playing of unauthorized video games by enforcing and protecting the measures it incorporates into the consoles in the United Kingdom. See Kabushiki Kaisha Sony Computer Entertainment v. Ball [2005] FRS 9. In the US, see Sony Computer Entertainment America Inc v. Gamemaster, 87 F.Supp. 2d 976 (ND Cal 1999). Sony failed in Australia: see Stevens v. Kabushiki Kaisha Sony Computer Entertainment [2005] HCA 58. For the US case, see below under Part IV section 2.

[36] The court also expressed dissatisfaction with Sony's practice of dividing the world into three regions and providing its games with codes depending on the region in which they were purchased. The result of the region-coding system was that games could only play in consoles purchased in the same region as the game. Sony changed this practice in November 2006, when it launched PlayStation 3.

[37] Legge 22 April 1941, n 633, amended by Decr. Leg. No 68, 9 April 2003 (Henceforth Lda).

[38] Article 102 quarter of the Lda expressly permits the holder's of author's rights and related rights to apply effective TPMs to their works.

[39] Decision of the Sezione per il riesame of the Tribunale di Bolzano, 31 December 2003, ECDR 18, 2006, online available at: http://www.ictlex.net/?p.

[40] In this regard, the court provided a "real world metaphor". It suggested that Fiat could not sell a car with the condition that it not be driven by foreigners or on country roads.

[41] Tribunale di Bolzano - Sentenza del 28 gennaio 2005 (Playstation modificate - 2), available at: http://www.interlex.it/testi/giurisprudenza/bz050128.htm.

[42] The court held that the TPMs employed by Sony should be protected under the act, "because they operated to prevent acts not authorized by the right holder"

[43] According to the court's ruling the use of imported games on consoles was considered illegitimate. This was because Article 17 prohibited importation from outside the European Union. However, this argument is ill-founded, because Art 17 prohibits only importation for the purposes of distribution, therefore not preventing individual imports. The argument that mod chips permitted the reading of back-up copies was also rejected, because the right to make back up copies applies only to software. According to Article 71sexies, the right to make a copy of other copyright works must respect any TPMs applied to the work. Evidence of emails sent to the accused showed that the principal purpose for which a mod chip was sought was to enable playing of illegally copied games.

[44]Tribunale di Bolzano - Sentenza del 20 dicembre 2005 (Playstation modificate - 3), available at: http://www.interlex.it/testi/giurisprudenza/bz051220.htm

[45] Cassazione, Sezione III Penale, Sentenza 25 maggio 2007 (dep. 3 settembre 2007), n. 33768 (35598/2006), available at http://www.civile.it/newS/visual.php?num=45307

[46] Tribunale Civile di Milano, Sezione proprietà industriale e intellettuale, Sentenza 5 Marzo 2009. An overview of the decision is available at http://www.dirittodautore.it/page.asp?mode=News&IDNews=4675&idcan=2.

[47] Dan L. Bruk. *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 570 (2005), arguing that "the anticircumvention provisions may therefore play the role that patents sometimes play in suppressing device interoperation".

[48] Steven P. Calandrillo and Ewa M. Davison, The Dangers of the Digital Millennium Copyright Act: Much Ado About Nothing?, WILLIAM & MARY LAW REVIEW, Vol. 50, 349, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262042.

[49] 87 F. Supp. 2d. 976 (N.D. Cal. 1999).

[50] See also Calandrillo & Davison, *supra* note 48, 18.

[51] *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Coley, 273 F.3d 429 (2d Cir.2001) affirming the constitutionality of the DMCA on challenge by defendant Corley form the district court. The court asserted that the DMCA "fundamentally altered the landscape" of copyright.

[52] The importance of Reimerdes is also illustrated by the fact that another maker of DVD copying software, similar to DeCss, filed a complaint for declaratory relief against movie studies in the Federal District Court of the Northern District of California, the court followed verbatim the court's opinion in Reimerdes. To elaborate, 321 sought a declaration that its products did not violate Section 1201 of the DMCA and also challenged the constitutional validity of the statute. The court held that 321's copying software was primarily designed to circumvent CSS-protected DVDs, a violation of the anticircumvention rule. See 321 Studios v. Metro Goldwyn Mayer Studios, Inc, 307 F. Supp. 2d 1085 (N.D.Cal. 2004).

Note, that in *321 Studios* the Federal District Court of the Northern District of California followed Southern District of New York opinion in Reimerdes and held

[53] *Id.* at 316-317. As regards the application of the Sony test for determining liability applied, the court held that "to the extend of any inconsistency between Sony and the new statute" Sony is overruled.

[54] *Id.* at 314; the court stated "At trial defendants repeated, as if were a mantra, the refrain that plaintiffs […] have no direct evidence of a specific occasion on which any person decrypted a copyrighted motion picture with DeCSS[…]. But this is unpersuasive."

[55] *Id.* at 218.

[56] *Id.*

[57] Davidson & Assocs. V. Internet Gateway, 334 F. Supp. 2d 1164 (E.M. Mo. 2004), aff'd' sub nom, 422 F. 3d 630 (8th Cir. 2005).

[58] Note that no defendant has yet succeeded on a Section 1201(f) defence. See Perzanowski, *supra* note 28, 22.

[59] Css, also known as "Content Scramble System" is a TPM encoded on DVDs by the Movie Industries to control access to the movies. DeCss was the software used to overcome Css. *Id*. at 308-309

[60] See the language of Section 1201(f)(1).

[61] The court rejected Defendants argument that the sole purpose of the DeCSS software used to overcome the TPMs was to enable interoperability with Linux-based DVD player software, arguing that as DeScc also enabled interoperability under Windows, where there was no compatibility concern. Reimerdes, 111F.Supp.2d. at 218.

[62] Section 1203(f)(3) verbatim provides "The information acquired through the acts permitted under paragraph (1), *and the means permitted under paragraph* (2), may be made available to others if […]" (emphasis added).

[63] See Perzanowski, *supra* note 28, at 22, footnote No. 92.

[64] Jerome H. Reichman, Graene Dinwoodie, Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L. J. 981, 1005-1006, 1024 (2007).

[65] Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 530 (6th Cir. 2004)

[66] Each time a printer was turned on, the printer and cartridge initiated a authentication sequence whereby each would calculate a code using an encryption algorithm. Static Control Components. *Id* at 350.

[67] *Id.* 530-531.

[68] Lexmark Int'l, Inc. v. Static Control Components, Inc., 233 F. Supp. 2d 943, 974(E.D. Ky. 2003)

[69] 381 F.3d. at 546-47.

[70] *Id.*

[71] See S. Callandrio & E. Davison, *supra*, 39-42.

[72] After all, if Lexmark had restricted access to its authentication sequence more fully, perhaps by encrypting the product code, its DMCA claim could have moved forward. See Perzanowski, *supra* note 28, 24. But See also Judge Merritt's concurrence, warning that future litigants could not escape the court's hostility to similar claims through minor variations on the Lexmark facts, 387 F.3d at 551-52 (Merritt, J., concurring).

[73] Chamberlain Group, Inc, v. Skylink Techs, 292 F. Supp. 2d 1040 (N.D. III.2003).

[74] Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc, 421 F.3d 1307, 1318 (Fed. Cir. 2005). Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintenance code using a password protection scheme. Defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries. Storage Technologies sued invoking Section 1201(a)(1) of the DMCA and although the district court issued a preliminary injunction, the Federal Circuit found otherwise.

[75] See also Perzanowski, *supra* note 28, 25.

[76] 381 F.3d at 1202.

[77] *Id.*
[78] *Id*. at 1203.
[79] Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc, 421 F.3d 1307, 1318 (Fed. Cir. 2005). Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintance code using a password protection scheme. Defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries. Storage Technologies sued invoking Section 1201(a)(1) of the DMCA and although the district court issued preliminary injunction, the Federal Circuit found it likely
[80] *Id*. at 318.
[81] *Davidson & Assocs. V. Internet Gateway,* 334 F. Supp. 2d 1164 (E.D. Mo. 2004), aff'd sub nom, 422 F.3d 630 (8th Cir. 2005). For an elaborate discussion of the Davidson case see: Paul J. Neufeld, *Circumventing the Competition: he Reverse Engineering Exemption in DMCA § 120,* 26 The Review Litigation, 525(2007); Perzanowski, *supra* note 28, 32.
[82] 334 F. Supp. 2d at 1183.
[83] *Id*. at 1185.
[84] *Id*. at 1186
[85] *Id.* at 1185.
[86] See also Perzanowski, *supra* note 28, 32.
[87] See also *ibid* stating: "Both courts worried that by adding fragments of copyrighted code to consumer goods, manufacturers could "gain the right to restrict consumers' rights to use [their] product in conjunction with competing products (Chamberlain, 381 F.3d at 1201). Such power, in turn, could "create monopolies of manufactured goods" (Lexmark, 387 F.3d at 1201) that relied on the DMCA to provide "broad exceptions from all []antitrust laws"(Chamberlain, 381 F.3d at 1201). "
[88] Nina Elkin-Koren*, Making Room for the Consumer under the DMCA*, 22 Berkeley Tech. L. J. 1119, (2007).
[89] See Joined cases C-241/91 P and C-242/91 P, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission (Magill), 1995 E.C.R. I-00743; Case T-65/98R, Van den Bergh Foods, 2003 E.C.R. II-4653; Case C-418/01, IMS Health v NDC Health, 2004 ECR I-5039, paragraph 49; T-201/04, Microsoft v Commission, 2007 E.C.R. II-3601, paragraphs 319, 330, 331, 332 and 33; See also Microsoft III, 253 F. 3d 34, 58(D.C. Circuit 2001).
[90] Herbert J. Hovenkamp, *Innovation and the Domain of Competition Policy*, 103 A. LA. L. Rev. 16 (2008).
[91] Perzanowski, *supra* note 28, 39.
[92] Phillip Areeda, Essential *Facilities: An Epihtet in Need of Limiting Principles*, 58 Antitrust L. J. 841, 853 (1989) arguing that an antitrust remedy shouldn't be available "when compulsory access requires courts to assume the day to day controls characteristic of a regulatory agency". Verizon Comms. V. Law Offices of Curtis V. Trinko, 540 US 398, 414 (2004).
[93] The Microsoft case seems to be a perfect example of that. Although Microsoft lost in court in both sides of the Atlantic, the remedies imposed could not restore competition in the market. Microsoft Corp., T-201/04, 249 (CFI Sept. 17, 2007) requiring Microsoft to disclose protocol specifications that enabled interoperability between Windows and work group server operating systems; United States v. Microsoft, 97 F. Supp. 2d 59, 67 (D.D.C. 2000) requiring disclosure of APIs, Communication Interfaces, and Technical Information used to enable interoperability; United States v. Microsoft, 231 F. Supp. 2d 144. 186-195, approving settlement agreement containing provisions for mandatory disclosure of interoperability information; United States v. Microsoft, 2006 U.S. D.D.C. Sept. 7, 2007, Modified Final Judgment.
[94] Phillip J. Weiser, *The Internet, Innovation, and Intellectual Property Policy*, 103 Colum. L. Rev. 534, 551-52 (2003) arguing that the speed of reverse engineering self-help renders it preferable to an antitrust conduct remedy.
[95] Adrian Majumbar, *Whither Dominance,* 4 E.C.L.R. 161, 162 (2006).
[96] Einer Elhauge & Damien Geraldin, Global Antitrust Law and Economics 256 (2007).
[97] Note that if a requirement that a circumventor of a TPM can infringe the anticircumvention regulation only if his/her act is a violation of a valid copyright or neighbouring right is enacted, such a provision
[98] See also Recital 50 of the Information Society Directive: "Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. […] Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs."
[99] Article 6 of the Software directive provides that 1. The authorization of the right holder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to to so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

[100] See Recitals of the Software Directive: "Whereas an objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together"

[101] See Perzanowski, *supra* note 28 arguing that "TPMs can not be neatly divided between those that restrict the use of entertainment content and those that control the use of computer programs. Frequently, the same TPM serves both functions", therefore the unavailability of an interoperability exception as regards entertainment content "ignores the role of data in enabling interoperable relationships, hampering the exceptions ability to fully accommodate interoperability" with further reference to URS GASSER & JOHN PALFREY, DRM-PROTECTED MUSIC INTEROPERABILITY AND EINNOVATION 21(2007), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-drm-music 0.pdf

[102] From the enactment of the DMCA many proposals have been articulated that would allow permissible uses of copyright works that are currently restricted under Section 1201. Dan Burk has argued that anticircumvention law requires its own doctrine of misuse (Dan L. Burk, *Anticircumvention Misuse, 50 UCLA L. REV. 1095 (2003)* 88). Timothy Armstrong has suggested that courts should more readily draw on fair use principles to create a body of judge-made fair circumvention law (Timothy K. Armstrong, Fair Circumvention, Brooklyn Law Review, Vol. 74, No. 1, pp. 1-50, 2008; U of Cincinnati Public Law Research Paper No. 08-08. Available at SSRN: http://ssrn.com/abstract=1095876). Aaron Perzanowski suggested to broaden the DMCA's existing interoperability exception to create an environment more hospitable to interoperable technologies (A. Perzanowski, *supra* 28.) Jerome Reichman, Graeme Dinwoodie and Pamela Samuelson have proposed a reverse notice and take down regime under which rights holders would be obligated to remove TPM restrictions after user-notification of a desire to make lawful uses of TPM-protected works (Jerome H. Reichman et al., supra note 64, 119). Each of this proposals have substantial merit and would address the many unintended consequences of the DMCA, but none of this proposals specifically address the importance to safeguard competition in the artistic markets.

[103] Indicatively see William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1659 (1988); Margaret Jane Radin, *A Comment on Infrormation Propertization and Its Legal Milieu*, 54 CLEV ST. L. REV. 23 (2006); Neil Weinstocl Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L. J. 283 (1996).