

The Expanding Penumbra of the DMCA

St. John Courtenay III

April 2004

TABLE OF CONTENTS

I. Introduction	1
II. The Impact of <i>Lexmark International, Inc. v. Static Control Components</i>	2
III. <i>Chamberlain Group v. Skylink Technologies</i>	4
IV. Bundle of exclusive patent rights	7
V. The DMCA under <i>Lexmark</i> impedes the examination requirement of the U.S. Patent system	9
VI. The DMCA under <i>Lexmark</i> impedes the disclosure requirement of the U.S. Patent system	10
VII. Lack of harmony between the Patent term vs. the Copyright term	12
VIII. Fair Use under Copyright, but not under Patent law, and perhaps not under the DMCA.....	14
IX. Can the DMCA be used (i.e., misused) to extend the “limited time” accorded functional devices under patent law?	16
X. Remedies Under Patent Law Contrasted With Remedies Under The DMCA	18
XI. Criminal Prosecution under the DMCA stops competitors cold	19
XII. History of Criminal Remedies under Copyright Law	22
XIII. Lack of Harmony between Patent remedies and Copyright criminal remedies	25
XIV. Tackling the Enforcement Problem – a Proposed Solution	26
XV. The Expanding Penumbra of the DMCA	28
XVI. Conclusion	29

I. Introduction

The purpose of this paper is to provide an examination of recent trends in copyright law that have effectively expanded the penumbra of copyright law protection to arguably encroach upon subject matter that has traditionally been accorded protection under patent law. In particular, several recent cases have applied the Digital Millennium Copyright Act (DMCA) in a manner that has provided *de facto* patent-like protection to software-based devices that employ access control technologies to protect copyrightable aspects of the device, such as computer code. Given this apparent overlap in intellectual property coverage, this paper further examines and contrasts the respective roles of copyright law and patent law. The lack of harmony between copyright law and patent law is also explored with respect to term of coverage, scope of coverage, and available remedies.

To qualify for copyright protection, a work must be original and fixed in a tangible medium of expression, such as paper, computer diskette, video tape, photographic film, canvas, and the like. Under copyright law, “original” means that the work was independently created by the author and that it possesses at least some minimal degree of creativity. Copyright protection is intended to cover the expression of an idea, and not the underlying idea itself.

To qualify for patent protection, an invention must also be original. The patent applicant is required to sign an oath that he believes himself to be the “original and first inventor of the process, machine, manufacture, or composition of matter, or improvement thereof, for which he solicits a patent.”¹ In addition, to be patented, an invention must not be anticipated nor obvious to one of ordinary skill in the art in light of the prior art. The broad categories of subject matter

¹ 35 U.S.C. §115.

that may be patented are limited to a “new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.”²

Under the Digital Millennium Copyright Act, encryption source code and associated encryption protection mechanisms can be used to completely bypass the U.S. patent system and realize a *de facto* “DMCA Patent” for any invention that contains a software component. Alternately, an inventor can obtain patent protection and simultaneous patent-like protection under the DMCA for any invention that includes a software component.

The computer code contained within any software-based invention is subject to copyright protection, assuming it is original and fixed in a tangible means of expression, such as computer disk, or a computer memory chip. The DMCA imposes restrictions under Title 17 U.S.C. §§1201(a)(1)(A), 1201(a)(2), and 1201(b)(1) that bar the circumvention of technological measures that control access of a protected work, trafficking in access tools, and trafficking in copying tools, respectively.

II. The Impact of *Lexmark International, Inc. v. Static Control Components*

The seminal case regarding the use of patent-like protections under the DMCA is *Lexmark International, Inc. v. Static Control Components*.³ In *Lexmark*, the U.S. District Court for the Eastern Division of Kentucky granted Lexmark’s motion for a preliminary injunction to stop Static Control Components (SCC) from making laser toner cartridges that were compatible with Lexmark’s printers. SCC manufactured a “SMARTEK” microchip that allegedly infringed Lexmark’s copyright in its “Toner Loading Programs.” With respect to the copyright

² 35 U.S.C. §101.

³ *Lexmark International Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Kentucky 2003).

infringement claim, the court found that SCC “identically copied the entire protectable expression of each Toner Loading Program.”⁴

Lexmark asserted two additional counts of circumvention against SCC, charging that SCC circumvented technological measures “that control access to Lexmark’s Toner Loading Programs and its Printer Engine Program,” in violation of the DMCA.⁵ The District court found that the authentication sequence used by authentic Lexmark toner cartridges constituted a “ ‘technological measure’ that ‘controls access’ to a copyrighted work.”⁶ The court noted that the DMCA does not define “access.” The court accorded the statutory term “access” its ordinary and customary meaning by applying the Webster’s dictionary definition, i.e., “access” means the “ability to enter, to obtain, or to make use of.”⁷

In *Lexmark*, the court found that SCC’s SMARTEK microchips circumvented the technological measures that control access to Lexmark’s copyrighted toner loading program and also to Lexmark’s copyrighted printer engine program.⁸ The court also found that SCC’s manufacture, distribution, and sale of its SMARTEK microchips fell within the plain language of §1201(b)(1)(A) of the DMCA that bars trafficking in devices that circumvent measures to protect the rights of a copyright owner and also trafficking in devices that circumvent measures to effectively control access to a protected work under §1201(a)(2)(A).⁹

The plain language statutory construction by the *Lexmark* court clearly applies the reach of the DMCA well beyond the protection of more typical copyrighted works such as books, CDs, and DVD movie disks. The effective impact of the *Lexmark* case is to expand the protections

⁴ *Id.* at 965.

⁵ *Id.* at 947.

⁶ *Id.* at 967.

⁷ *Id.*

⁸ *Id.* at 968.

⁹ *Id.* at 969.

under the DMCA to software-based devices. This expansion of protectable subject matter clearly encroaches into the realm of patent law where patents on computer software are now commonplace. While the *Lexmark* case deals with embedded software, it is also true that general purpose computers are software-based devices, and if such computers contained copyrighted software or other copyrighted material that is protected by a technological measure that effectively controls access to the software or the computer itself, then the DMCA would apply in a manner similar to the court's finding in *Lexmark*.

The preliminary injunction granted by the *Lexmark* court prevented SCC from manufacturing, distributing, and selling, or marketing the SMARTEK chips.¹⁰ This injunctive remedy fashioned by the *Lexmark* court is functionally equivalent to the application of the exclusive rights codified under Title 35 of the patent statutes to “make and use, sell, and offer to sell the claimed invention during the patent term.”¹¹

Since it is trivial for a software programmer to include encryption code or other code to restrict access in any software-based invention, e.g., a *Lexmark* printer cartridge, the DMCA's broad bar against circumvention of technological measures that control access of a protected work can clearly be used to realize patent-like protection for a wide variety of software-based devices.

III. *Chamberlain Group v. Skylink Technologies*

A second seminal case along the same line of *Lexmark* is *Chamberlain Group v. Skylink Technologies* where the District Court for the Northern District of Illinois granted Skylink's

¹⁰ *Id.* at 947.

¹¹ 35 U.S.C. § 271.

motion for partial summary judgment on Nov. 13, 2003.¹² The court found that Chamberlain failed to show that it “demonstrated its intention to prohibit customers from using any competing products,” the issue turning on whether Chamberlain’s customers had authority from the copyright owner (Chamberlain) to circumvent its “rolling code” security feature.¹³

Chamberlain is a company that manufactures and sells garage door openers that utilize a “rolling code” access control technology that prevents a practice known as “code grabbing.” Code grabbing is where an unauthorized party captures and records the garage door transmitter signals to obtain illegal access to a homeowner’s garage. The “rolling code” access control technology is marketed by Chamberlain as its top “Security+” line that customers are willing to pay a premium for.¹⁴

Skylink is a company that markets universal remote control devices that operate many brands of garage doors. Skylink’s remote control Model 39 can be used to open a Chamberlain “Security+” garage door opener, but only if the user first stores the Model 39 signal into the Chamberlain garage door opener.¹⁵ Chamberlain argued that it never authorized its customers to circumvent the “rolling code” access control security measure because the scope of its product manual and product warranty did not cover the use of “unauthorized parts or accessories.” Chamberlain argued that it did not know that circumvention of its “Security+” line was possible before introduction of the Model 39 by Skylink.¹⁶

¹² Chamberlain Group v. Skylink Technologies, 292 F. Supp. 2d 1023 (N.D. Ill 2003).

¹³ *Id.* at 1045.

¹⁴ *Id.* at 1042.

¹⁵ *Id.*

¹⁶ *Id.*

Under the DMCA, circumventing a technological measure is only circumvention if it is done without the authority of the copyright owner.¹⁷ Skylink counterargued that “Chamberlain cannot demonstrate that Skylink’s Model 39 transmitter provides unauthorized access.”¹⁸ The *Chamberlain* court found that under §1201(a)(3)(A) of the DMCA “it is clearly the plaintiff’s burden to demonstrate that the defendant circumvented a technological measure ... and that this requires a showing that the defendant acted ‘without authority of the copyright owner.’ ”¹⁹

In a detailed analysis of whether Chamberlain expressly prohibited circumvention in its product manual, product warranty, and product web page, the court found that “Chamberlain did not advise its customers that no other universal transmitter would work on its Security+ line, let alone prohibit them from using such products ... In addition, a homeowner has a legitimate expectation that he or she will be able to access the garage even if the original transmitter is misplaced or malfunctions.”²⁰ The District court found that Chamberlain did not expressly deny authority to its customers to use competing products, and therefore Chamberlain failed to show that the defendant acted “without the authority of the copyright owner” as required under §1201(a)(3)(A).²¹

Although the outcome in *Chamberlain* is opposite the injunctive relief applied by the *Lexmark* court, it appears certain that Chamberlain’s claims under the DMCA would have prevailed (under the court’s construction of the statute) if only it had given its customers clear constructive notice against circumvention, such as by including use restrictions on the product or product packaging. It is arguable whether this is a consumer rights labeling issue, such as

¹⁷ 17 U.S.C. §1201(a)(3)(A).

¹⁸ *Chamberlain*, 292 F. Supp. 2d at 1043.

¹⁹ *Id.* at 1044.

²⁰ *Id.* at 1045.

²¹ *Id.* at 1044.

labeling copy-protected CDs, or a copyright issue. Chamberlain admitted “the packaging for its Security+ GDO does not include ‘any restrictions on the customer’s ability to buy a replacement transmitter or additional transmitter.’”²² The lack of such notice combined with the reasonable expectations of consumers that they can replace the Chamberlain GDO with “a competing, universal product without violating federal law” was apparently construed by the court as an implied grant of authority. If Chamberlain had provided clear notice against circumvention, the use of such notice would have likely allowed Chamberlain to realize patent-like protections under the DMCA for its garage door products, and obtain injunctive relief, as was the remedy in *Lexmark*.

Significantly, the DMCA is silent with respect to any requirement that the copyright owner give constructive notice against circumvention. A similar issue arose in *Universal Studios v. Corley*, where the Appellants argued “that an individual who buys a DVD has the ‘authority of the copyright owner’ to view the DVD,” and therefore is exempted from the DMCA pursuant to §1201(a)(3)(A) when the buyer circumvents an encryption technology in order to view the DVD on a different platform (such as Linux).”²³ The court found that this argument misread §1201(a)(3)(A), which, according to the court, “exempts from liability those who would ‘decrypt’ an encrypted DVD with the authority of the copyright owner, not those who would ‘view’ a DVD with the authority of the copyright owner.”²⁴ From *Corley*, it appears that affirmative authority from the copyright owner is the only defense against circumvention. However, *Corely* is silent on the issue of whether the copyright owner must give constructive notice against circumvention as a prerequisite for enforcement under the DMCA, as implied by the *Chamberlain* decision, *supra*.

²² *Id.*

²³ *Universal Studios, Inc., v. Corely*, 273 F.3d 429, 444 (2nd Cir. 2001).

²⁴ *Id.*

IV. Bundle of exclusive patent rights

Similar to the bar against circumvention “without authority of the copyright owner” under the DMCA,²⁵ the claimed subject matter of a U.S. patent can not be infringed without express authority from the patent owner (e.g., a license). A U.S. Patent is a grant of intellectual property rights by the U.S. government that accords an exclusive right for a limited time to one or more inventors. U.S. patents are granted only to individual inventors. Like copyrights, the legal bundle of rights associated with a patent grant can be assigned to another person or other legal entity such as a business or corporation.²⁶ Employees who develop patentable ideas that arise within the scope of their employment are typically required to assign any resultant patent grant to the employer as a condition of employment.

A grant of a U.S. patent provides a specific bundle of rights to the inventors (or assignee(s) of record) that include the exclusive rights to make and use, sell, and offer to sell the claimed invention during the patent term.²⁷ In addition, subsequent to Congressional ratification in Dec. 1994 of the General Agreement on Tariffs and Trade (GATT), Congress amended U.S. patent law to be in harmony with patent law in other countries under the Trade-Related Aspects of Intellectual Property Rights agreement (TRIPS). Patentees were further granted the exclusive right to prevent others from importing their claimed invention into the United States.²⁸

Significantly, the bar under the patent statutes against others making, using, offering to sell, selling, and importing the claimed invention is quite similar to the anti-trafficking language under the DMCA, where “No person shall manufacture, import, offer to the public, provide, or

²⁵ 17 U.S.C. §1201(a)(3)(A).

²⁶ 37 U.S.C. § 261.

²⁷ 35 U.S.C. § 271.

²⁸ *Id.*

otherwise traffic in any technology, product, service, device, component, or part thereof, that – ... is primarily designed for the purpose of circumventing protection ...”²⁹ While the scope of coverage under the patent statutes is limited to the claimed subject matter of the invention, and the scope of coverage under the DMCA is limited to trafficking in a circumvention technology, the result is effectively the same in situations where functional devices are accorded protection under the DMCA, as in the case of *Lexmark, supra*. Although trafficking was not charged under *Lexmark*, the court found that “SCC intentionally copied Lexmark’s Toner Loading Programs and purposely developed and sold [i.e. offered to the public] a product that circumvents the access control measure that protects Lexmark’s copyrighted marks.”³⁰

V. The DMCA under *Lexmark* impedes the examination requirement of the U.S. Patent system

A U.S. Patent is obtained only after a search and examination process conducted by a patent examiner skilled in the art. Patents are only granted if a comprehensive search of the prior art shows that the claimed subject matter is novel and non obvious to one of ordinary skill in the art at the time the invention was made.

In contrast, the patent-like protection accorded under the DMCA by the *Lexmark* court requires no examination of subject matter for patentability. In fact, the copyrighted subject matter of a software-based device protected under the DMCA need not be disclosed at all, since it is usually copyrighted computer code that is obscured by encryption or an alternate access control technology.

²⁹ 17 U.S.C. §1201(b)(1).

³⁰ *Lexmark*, 253 F. Supp. 2d at 973.

To protect a software-based device under the DMCA, one need not hire a patent attorney, and one can avoid the patent examination process entirely. Protection begins immediately when the software code is fixed in a tangible means of expression. Without the circumvention barred by the DMCA, it is impossible for a third party to determine whether the copyrighted expression is original because the computer code is generally not accessible.

VI. The DMCA under *Lexmark* impedes the disclosure requirement of the U.S. Patent system

Significantly, the patent-like protection accorded under the DMCA in *Lexmark* impedes one of the central goals of patent law – i.e., full disclosure of how to make and use the invention, and the requirement to set forth a best mode. To be considered by the Patent Office, each patent application must provide full disclosure of the claimed invention, as set forth under 35 U.S.C. § 112, 1st paragraph, shown below:

35 U.S.C. §112(1)

“The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.”

Unlike the absence of any disclosure requirement under the DMCA, the patent application process involves significant disclosure requirements. Under 35 U.S.C. § 122 (b)(1)(A), each patent application is published after the expiration of a period of 18 months from the earliest filing date for which a benefit is sought. The same statute provides for publication before the end of the 18-month period if an explicit early publication request is received from the patent applicant. If an applicant certifies that the U.S. patent application will not also be filed in

a foreign country, or under a “multilateral international agreement, that requires publication of applications 18 months after filing,” then the U.S. application will not be published at 18 months after filing.³¹ In addition, a patent applicant has a duty to disclose all information material to patentability, including prior art cited in search reports of a foreign patent office in a counterpart application.³²

Significantly, there are no analogous disclosure requirements when a party seeks patent-like protections for a software-based device covered under the anti-circumvention provisions of the DMCA. In fact, because of encryption or other access control technologies, the inventive subject matter protectable in a *de facto* manner under the DMCA is never disclosed and is therefore not searchable in the course of an examination search for prior art by the U.S. Patent & Trademark Office.

While it is true that a patent applicant need not disclose the actual source code of a patentable computer program, the applicant still must provide sufficient support in the specification to enable one skilled in the art to make and use the claimed invention by relying solely upon the patent disclosure.³³ While one skilled in the art may rely upon the reverse engineering exception under §1201(f) of the DMCA to enable interoperability of an independently created computer program with other programs, interoperability is not the same as providing an enabling disclosure that teaches one skilled in the art how to make and use the claimed invention. Therefore, the reverse engineering exception under the DMCA does not maintain the status quo because it permits interoperability only, and it does not require an enabling disclosure of the protected subject matter. Such fully enabling information cannot likely

³¹ 35 U.S.C. § 122 (b)(2)(B)(i).

³² 37 C.F.R. §1.56.

³³ 35 U.S.C. §112, 1st paragraph.

be obtained by one skilled in the art without engaging in the circumvention that is proscribed by the DMCA.

VII. Lack of harmony between the Patent term vs. the Copyright term

The TRIPS Agreement mandated that the term for patent applications filed after June 7, 1995 would run 20 years from the filing date. While patent protection extends for merely 20 years from the date the patent application is filed under the U.S. patent system, patent-like protection for devices controlled under the DMCA runs until the expiration of the copyright associated with the computer code or other copyrightable feature of the invention.

Congress legislated a patent term that is shorter than the copyright term for a good reason. Given the rapid advances in technology, it arguably does not promote the progress of the useful arts to let a patent owner lock up a patent grant monopoly for the extended length of time granted to copyright holders. Such an extended monopoly could tie up essential technologies for many decades. The use of the DMCA to provide patent-like protection for the duration of the copyright term defeats the rationale for having a shorter patent term.

In fact, the patent term can be even shorter than the 20-year patent term that runs from the date of filing. Unlike copyrights, whether registered or unregistered, a patent grant requires payment of maintenance fees to the Patent Office at intervals of 3, 7, and 11 years after the date the patent was granted.³⁴ The claimed subject matter of the patent lapses into the public domain if the patent owner fails to pay the required maintenance fees when due. Perhaps such a policy should be considered by Congress with respect to registered copyrights for the purpose of encouraging the entry of commercially unmarketable copyrighted material into the public domain. As with the case of registered copyrights, a patent grant carries with it a presumption of

³⁴ 37 C.F.R. §1.362(d).

validity.³⁵ Unlike the case of registered copyrights, a patent grant does not entitle one to statutory attorney's fees. In patent cases reasonable attorney fees will only be awarded to the prevailing party in exceptional cases.³⁶

After passage of the Sony Bono Copyright Term Extension Act of 1998, the term for a copyright was extended to last for the life of the author, plus 70 years.³⁷ If the software development was contracted as "a work made for hire," the copyright term can last as long as 95 years from the year of first publication or 120 years from the year of the work's creation, whichever expires first.³⁸

Under the DMCA, the bar against circumvention only attaches to a technological measure that controls access to a work protected under Title 17, i.e., a work protected by copyright, such as computer code.³⁹ Because copyright expires after a limited time it follows that the DMCA anticircumvention provisions have no legal effect upon expiration of the copyright term. However, copyrightable content is frequently mixed with public domain content, and access to both types of content is typically controlled by a single technological access control system. While "unauthorized extraction of unprotectable content from a copyrighted work has consistently been held not to violate copyright ... extraction of such unprotectable content from a technologically controlled copy would violate the anticircumvention right."⁴⁰

³⁵ 35 U.S.C. §282.

³⁶ 35 U.S.C. §285.

³⁷ 17 U.S.C. § 302(a).

³⁸ 17 U.S.C. § 302(c).

³⁹ 17 U.S.C. §1201(a)(1)(A).

⁴⁰ See Burk, Dan L., *Anti-Circumvention Misuse*, University of Minnesota, 2002, page 18.

VIII. Fair Use under Copyright, but not under Patent law, and perhaps not under the DMCA

There is no explicit fair use exemption under §1201(c)(1) that permits one to engage in circumvention of a technological access control measure.⁴¹ It has been argued that the omission of fair use was deliberate because Congress provided for certain exemptions to the DMCA under §1201(a) that are reviewed and updated by the Librarian of Congress every three years.⁴² However, in *U.S. v. Elcom*, the California District Court explicitly found that the DMCA does not eliminate nor prohibit fair use:

First, the DMCA does not eliminate fair use. Although certain fair uses may become more difficult, no fair use has been prohibited. Lawful possessors of copyrighted works may continue to engage in each and every fair use authorized by law. It may, however, have become more difficult for such uses to occur with regard to technologically protected digital works, but the fair uses themselves have not been eliminated or prohibited.⁴³

In *Corley*, *supra*, the 2nd Circuit Court of Appeals adopted a similar position on fair use:

We know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original ... The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of constitutional limitation of fair use.⁴⁴

It seems intuitive that if one cannot access an encrypted work because of the §1201(a)(1) bar on circumvention of access protection measures, then fair use has been restricted. The counter argument is that once lawful access is obtained, one should then be able to make fair use

⁴¹ *Reimerdes v. Universal Studios*, 111 F.Supp.2d 294, 308 (S.D.N.Y. 2000).

⁴² Ginsberg, Jane C., *How Copyright Got a Bad Name for Itself* 26 COLUM.-VLA J.L. & Arts 61, 70 (2002).

⁴³ *U.S. v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1131 (N.D. Cal. 2002).

⁴⁴ *Corely*, 273 F.3d at 459.

of legally accessed copyrighted material. If a work (or portion of a work) is truly in the public domain, then that work should be freely available from more than one source, at least in theory, and the fair use exceptions are clearly only applicable to copyrighted subject matter.

Some have argued that the anti-circumvention provisions of the DMCA appear in conflict with the §107 fair use exceptions in the case where a single technological access control measure controls both the copyrighted and public domain portions of the work. As observed by Dan Burk, “Because the right of access is defined in terms of the technological system, rather than the terms of the content, both copyrightable and uncopyrightable materials will be covered by the anti-circumvention right.”⁴⁵

The §1201(a)(1) bar on circumvention of access control measures for any purpose, including fair use, appears in conflict with the 9th Circuit holding in *Sega v. Accolade* regarding another type of circumvention – the disassembly of copyrighted object code, arguably a type of reverse engineering:

Although the question is fairly debatable, we conclude based on the policies underlying the Copyright Act that disassembly of copyrighted object code is, as a matter of law, a fair use of the copyrighted work if such disassembly provides the only means of access to those elements of the code that are not protected by copyright and the copier has a legitimate reason for seeking such access.⁴⁶

However, the legislative history indicates that Congress provided the reverse engineering exemption under sections 1201(f)(2) and (3) to preserve the *Sega* holding and allow software programmers “to continue engaging in certain activities for the purpose of achieving interoperability between computer programs.”⁴⁷

⁴⁵ Burk, *supra* note 40, at 18.

⁴⁶ *Sega v. Accolade*, 977 F.2d 1510, 1518 (9th Cir. 1992).

⁴⁷ House Manager’s Report at 14, 65 FR 64556, 64558 n.4 (October 27, 2000).

In contrast to the 9th Circuit holding in *Sega*, the *Lexmark* court interpreted the reverse engineering exemption under sections 1201(f)(2) and (3), as not being “broad exceptions that can be employed to excuse any behavior that makes some device ‘interoperable’ with some other device,” the court essentially finding that copying is not equivalent to reverse engineering.⁴⁸ In contrast, under patent law, there has never been a fair use exception to patent infringement, although the doctrines of contributory infringement and patent misuse are well established.⁴⁹

IX. Can the DMCA be used (i.e., misused) to extend the “limited time” accorded functional devices under patent law?

The intellectual property clause (also referred to as the “copyright clause”) provides the authority for copyright law under Title 17 and patent law under Title 35 of the United States Code.⁵⁰ Clearly, DMCA protections such as the bar against circumvention extend well beyond any authority that can reasonably be derived under the copyright clause of the constitution. As in the case of trademark law, the authority for the DMCA appears to be based upon the power of Congress to regulate commerce under the Commerce Clause, as Judge Whyte observed in *Elcom*.⁵¹

Simultaneous protection under patent law and the DMCA appears to conflict with the exclusive right for a “limited time” *quid pro quo* set forth in the Constitution under the Intellectual Property Clause by effectively allowing a patent holder to use patent-like protection accorded under the DMCA (as applied in *Lexmark*) to extend the term of protection beyond the expiration of the patent term to a new term controlled under copyright law. In fact, a virtual perpetual term of protection can be obtained by merely rewriting the source code in a manner

⁴⁸ *Lexmark*, 253 F. Supp. 2d at 970.

⁴⁹ Burk, *supra* note 40, at 49.

⁵⁰ U.S. Const., Art. I, Sect. 8, Cl. 8.

⁵¹ *Elcom*, 203 F. Supp. 2d at 1138.

that creates a new or derivative work for purposes of copyright, but does not materially change the functionality of the resultant executable computer code. This application of dual terms of protection to the same underlying intellectual property is arguably a misuse of the DMCA.

By using DMCA in the manner described above, an inventor may obtain an “exclusive right” for a virtually unlimited time by merely including an encryption feature as an aspect of their invention and rewriting and recompiling the source code periodically without changing the functionality of the executable code. Such modifications are trivial exercises for experienced programmers. Why bother with the time and expense of the U.S. patent system when you can obtain powerful intellectual property protection in virtual perpetuity? What better way to avoid the time and expense of patent infringement litigation? This loophole in existing law allows clever inventors to protect their invention with powerful civil and criminal remedies unavailable under U.S. patent law.

The counter argument essentially is an argument for a registration system for U.S. patents as opposed to an examination system. Many inventors have long complained that by the time their patent application is examined and a patent is granted (generally 3 or more years after filing), their technology may be obsolete in a rapidly changing marketplace. By realizing *de facto* patent-like protection for software-based devices under the DMCA, immediate protection is provided at low cost without engaging the patent system. Such arguable misuse of the DMCA is similar to a patent registration system. The main reason we don't have a patent registration system in the U.S. is because such a system would be subject to abuse and would likely overload the courts with patent infringement litigation.

X. Remedies Under Patent Law Contrastd With Remedies Under The DMCA

While a patent grants the patentee exclusive rights to make and use, sell, and offer to sell the claimed invention during the patent term,⁵² the remedies available under the U.S. patent system are limited to civil remedies. The right to civil remedies for patent infringement is set forth under U.S. law at 35 U.S.C. § 281 that requires “A patentee shall have remedy by civil action for infringement of his patent.”

The civil remedies available under patent law are tame compared to the remedies available under copyright law and the DMCA. With respect to patent infringement, U.S.C. § 283 provides injunctive relief “to prevent the violation of any right secured by patent.” Economic compensatory damages for patent infringement are set forth under 35 U.S.C. § 284 that are “in no event less that a reasonable royalty for the use made of the invention by the infringer, together with interest and costs as fixed by the court.”

Treble damages are available under 35 U.S.C. § 284 at the discretion of the court. Treble damages are usually found in the case of willful infringement or where it has been proven that the defendant knowingly enforced an invalid patent. In exceptional cases, the court may award reasonable attorney fees to the prevailing party.⁵³ A statute of limitations requires that all patent infringement complaints or counterclaims must be filed within six years of the alleged infringement.⁵⁴

⁵² 35 U.S.C. § 271.

⁵³ 35 U.S.C. § 285.

⁵⁴ 35 U.S.C. § 286.

In contrast, under the DMCA, a wide range of civil remedies⁵⁵ and criminal remedies⁵⁶ are available to prevent circumvention of technological measures that control access to a protected work,⁵⁷ or trafficking in a technological measure designed for the purpose of circumventing,⁵⁸ effectively precluding the equivalent of infringement.

Under 17 U.S.C. § 1204, it is a criminal offense to violate §1201 or §1202 for purposes of commercial advantage or private commercial gain. The statutory penalties under §1204 range from up to a \$500,000 fine or up to five years imprisonment for a first offense, and up to a \$1,000,000 fine or up to 10 years imprisonment for subsequent offenses. These powerful remedies for circumvention (i.e., functionally equivalent to “infringement”) make the U.S. patent system look thoroughly impotent by comparison.

XI. Criminal Prosecution under the DMCA stops competitors cold

Several high-profile cases have found computer scientists in conflict with the DMCA. With respect to criminal prosecution under the DMCA, *U.S. v. Elcom Ltd.* is the seminal case.⁵⁹ On July 16, 2001, Russian computer scientist Dimitry Sklyarov, Ph.D, was arrested after he presented his research at the DEF CON Nine computer security conference held in Las Vegas, Nevada. While working for his Russian employer, Elcomsoft, Sklyarov created software called “Advanced Ebook Processor (AEBPR) that enables owners of legitimately purchased Adobe eBooks to bypass the copy protection features of the eBook format and convert eBooks into the

⁵⁵ 17 U.S.C. § 1203.

⁵⁶ 17 U.S.C. § 1204.

⁵⁷ 17 U.S.C. §1201(a).

⁵⁸ 17 U.S.C. §1201(b).

⁵⁹ *Elcom*, 203 F. Supp. 2d at 1111.

widely used Adobe Portable Document Format.⁶⁰ It is noted that while §1201(b)(1) prohibits the trafficking in devices that circumvent copy protection measures, there is no statutory bar under the DMCA that proscribes circumvention of copy protection measures, per se, e.g., by individual hacking. Sklyarov was arrested for distributing software that circumvents the Adobe Digital Rights Management code and was charged with four counts of trafficking under the DMCA under 17 U.S.C. § 1201(b)(1)(A) & (b)(1)(C), one count of aiding and abetting circumvention, and one count of conspiracy under 18 U.S.C. § 371, 18 U.S.C. § 2, and 17 U.S.C. § 1201(b)(1)(A) to traffic in a circumvention program.⁶¹ The U.S. District Court in California denied Sklyarov's motion to dismiss his indictment.

In his defense, Sklyarov's lawyers argued that §1201(b) of the DMCA was unconstitutionally vague under the due process clause of the Fifth Amendment, that the same section violated the first amendment rights of third parties to engage in fair use, and that §1201(b) was too vague regarding what speech was proscribed, and that Congress exceeded its constitutional power in enacting the DMCA.⁶² After spending several months in jail, Sklyarov was allowed to return to Russia after consenting on Dec. 13, 2001 to a "Pretrial Diversion Agreement" with the Dept. of Justice.⁶³

The Dept. of Justice proceeded in bringing criminal charges under the DMCA against Sklyarov's employer, Elcomsoft. Elcomsoft was eventually acquitted of all charges in what

⁶⁰ See Robinson, Laura J., *Anticircumvention Under the Digital Millennium Copyright Act*, Journal of the Patent and Trademark Office Society, Dec. 2003, Vol. 85, No. 12, page 961.

⁶¹ See *United States v. Elcom Ltd. et al.*, Indictment, United States District Court Northern District of California, San Jose Division, filed Aug. 28, 2001, pages 1-6.

⁶² *Elcom*, 203 F. Supp. 2d at 1122.

⁶³ See *PRETRIAL DIVERSION AGREEMENT* No. CR 01-20138 RMW, United States District Court, Northern District of California, San Jose Division, Dec. 13, 2001, pages 1-7.

arguably was a case of jury nullification. CNET news.com reported the public comments the jury made after the trial was over:

Jury foreman Dennis Strader said the jurors agreed ElcomSoft's product was illegal but acquitted the company because they believed the company didn't mean to violate the law.

"We didn't understand why a million-dollar company would put on their Web page an illegal thing that would (ruin) their whole business if they were caught," he said in an interview after the verdict. Strader added that the panel found the DMCA itself confusing, making it easy for jurors to believe that executives from Russia might not fully understand it.⁶⁴

Because corporate officers and directors can conceivably be held accountable under criminal copyright sanctions, the mere threat or possibility of criminal sanctions has the effect of stopping competitors cold. The mere threat of criminal sanctions reduces competition in the marketplace, resulting in higher prices, and arguably has a chilling effect on innovation when the DMCA is used to realize *de facto* patent-like protections as applied under *Lexmark*.

As of April 2004, there have been two criminal convictions under the DMCA. There was a first criminal conviction when the U.S. Attorney's Office for the District of Nebraska obtained a guilty plea from defendant Rick Oliver regarding his alleged modification of a chip that circumvented a software security measure on Sony *Playstation* games.⁶⁵ Defendant Oliver was sentenced on May 24, 2002 to seven months incarceration and ordered to pay Sony restitution of

⁶⁴ See Bowman, Lisa M., *ElcomSoft verdict: Not guilty*, CNET news.com, <http://news.com.com/2100-1023-978176.htm> December 17, 2002, pages 1-2.

⁶⁵ See (no author given) *Criminal Copyright Charges Involving More than 4,500 bootlegged tapes*, <http://www.cybercrime.gov/mynafPlea.htm>

\$40,000 for selling modified *Playstations* that allowed the unauthorized use of non-Sony games.⁶⁶

The second conviction on March 28, 2002 involved defendant Mohsin Mynaf of Vacaville, California, who “pled guilty to six counts of criminal copyright infringement; six counts of trafficking in counterfeit labels; and one count of circumventing a technological measure that protects a copyrighted work.”⁶⁷ Mynaf was allegedly operating a counterfeit movie videocassette reproduction lab that bypassed the Macrovision copyright guard.⁶⁸

XII. History of Criminal Remedies under Copyright Law

The first criminal penalties for copyright infringement were enacted by Congress in 1897.⁶⁹ These first criminal copyright sanctions made it a misdemeanor for “unlawful performance or presentation, done willfully and for profit, of a copyrighted dramatic or musical composition,” and provided for imprisonment for up to one full year.⁷⁰

The *Copyright Act of 1909* provided that “misdemeanor penalties of up to one year in jail or a fine between \$100 and \$1,000, or both, be imposed upon ‘any person who willfully and for profit’ infringed a protected copyright,” although the provision was seldom used.⁷¹ The act was amended again by Congress in 1974 to increase the penalties for record piracy such that one who “willfully and for profit infringed a copyright in sound recordings would be subject to a fine of up to \$25,000 or imprisonment for one year or both.”⁷² The *Copyright Act of 1976*⁷³ relaxed

⁶⁶ NIPLECC REPORT, The National Intellectual Property Law Enforcement Coordination Council 2001-2002, page 9.

⁶⁷ See *Criminal Copyright Charges Involving More than 4,500 bootlegged tapes*, *supra*, note 65.

⁶⁸ See NIPLECC REPORT, *supra*, note 66 at 9.

⁶⁹ See Act of Jan. 6, 1897, 29 Stat. 481.

⁷⁰ *Dowling v. United States*, 473 U.S. 207, 222 N14 (1985).

⁷¹ *Id.* at 221.

⁷² *Id.* at 222.

⁷³ See Pub. L. No. 94-553, 90, Stat. 2541, Oct. 19, 1976.

the scienter requirement by requiring “only that the infringement be undertaken willfully and for purposes of commercial advantage or private financial gain, rather than for profit.”⁷⁴

In 1982 Congress increased the sanctions for criminal infringement by passing the *Piracy and Counterfeiting Amendments Act of 1982*.⁷⁵ The *Copyright Felony Act* was enacted in October of 1992 to address the growing problem of piracy of computer software by amending 18 U.S.C. § 2319 to broaden the coverage to protect all copyrighted works and “lowering the numerical and monetary thresholds for felony sanctions” without changing the scienter requirement.⁷⁶ Before passage of the 1992 *Copyright Felony Act*, only unauthorized copying of “sound recordings, motion pictures, or audiovisual works” constituted a felony under federal law.⁷⁷

In December 1997 the *No Electronic Theft Act* (“NET Act”) was enacted. The *NET Act* removed the financial gain requirement and made illegal reproduction or distribution of copyrighted materials a federal crime where the “government need only prove either that the infringer acted for financial gain, or that [the infringer] reproduced or distributed one or more copies of copyrighted works with a total retail value of \$1000.”⁷⁸

The passage of the DMCA on Oct. 28, 1998 expanded criminal penalties even further to their present form under §1204 where willful violations or violations for purposes of commercial advantage or private gain of §1201 or §1202 are punishable with severe criminal sanctions. The statute of limitations under the DMCA is limited to five years after the cause of action arose with a maximum fine of \$1,000,000 and not more than 10 years imprisonment for subsequent

⁷⁴ See Barr et al., *Intellectual Property Crimes* 40 Am. Crim. L. Rev. 771, at 789, citing H.R. REP. NO. 104-556, at 6 (1996), reprinted in 1996 U.S.C.C.A.N. 1074, 1075.

⁷⁵ See Act of May 24, 1982, Pub. L. No. 97-180, 96 Stat. 91 (codified at 18 U.S.C. § 2319 (1994)).

⁷⁶ Barr, *supra*, note 72, at 790.

⁷⁷ *Id.*

⁷⁸ *Id.*

offenses.⁷⁹ Significantly, the legislative history indicates that Congress strengthened criminal sanctions over the years because it believed that the “existing misdemeanor penalties for copyright infringement were simply inadequate to deter the enormously lucrative activities of large-scale bootleggers and pirates.”⁸⁰

Presently, with respect to copyright violations (not under the DMCA) willful copyright infringement is a criminal offense under 17 U.S.C. § 506 if the infringement is made “for purpose of commercial advantage or private financial gain” or for the “reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000.”⁸¹ A criminal statute of limitations is set forth under §507(a) that is limited to five years after the alleged copyright infringement occurred.

Criminal sanctions for copyright violation are also found under Title 18 U.S.C. §2319, the criminal section the United States code. The maximum penalty set forth under §2319(b)(2) is for 10 years imprisonment for second or subsequent violations for reproduction or distribution of works with a retail value of more than \$2,500 during any 180 day period. Furthermore, under the “Definitions” section 1961 of the *Racketeer Influenced and Corrupt Organizations Act* (RICO), racketeering charges may be applied to Title 17, section 2319 criminal copyright infringement.⁸² A RICO claim for copyright infringement requires that the infringing acts “continue over a period of time and relate to each other in a common plan created by the

⁷⁹ 17 U.S.C. §§ 1204(c) & 1204(a)(2).

⁸⁰ *Id.* at 224.

⁸¹ 17 U.S.C. § 506.

⁸² *See Racketeer Influenced and Corrupt Organizations Act (RICO)*, Title 18 U.S.C. §§ 1961-1968.

violators with the intent to defraud.”⁸³ A “pattern of activity” under RICO merely requires two acts of racketeering activity within a ten-year period.⁸⁴

XIII. Lack of Harmony between Patent remedies and Copyright criminal remedies

The disparity between patent law and copyright law with respect to criminal remedies is striking, especially since copyright law (Title 17) and patent law (Title 35) both derive their authority under the Intellectual Property Clause, often called the Copyright Clause of the U.S. Constitution.⁸⁵ How can one justify the vast difference in the remedies provided by Congress, given that patent infringement cases often involve high-value intellectual property running into the tens of millions of dollars in compensatory economic damages?

In a recent patent infringement victory by Eolas Technologies, Inc. against Microsoft Corp., Eolas won a \$521 million dollar judgment for infringement of its U.S. Patent number 5,838,906.⁸⁶ Eolas is seeking further injunctive relief and Microsoft is appealing the verdict, which was reached in less than two days of deliberation by the jury. Clearly the “enormously lucrative activities of large-scale bootleggers and pirates” that motivated Congress to strengthen criminal copyright sanctions never even remotely approached the aforementioned half-billion dollar verdict for patent infringement.⁸⁷

How can such a lack of harmony (with respect to criminal remedies) between copyright law, the DMCA, and patent law be justified? Although copyright law and patent law clearly differ in scope of protection, it seems unclear why is it justifiable to jail an individual for willfully violating the DMCA under §§1201 or 1202 and then merely apply civil sanctions

⁸³ Barr, *supra*, note 72, at 771.

⁸⁴ 18 U.S.C. § 1961(5).

⁸⁵ U.S. Const. Art. I, §8, cl. 8.

⁸⁶ Eolas Technologies, Inc. v. Microsoft Corp., 274 F.Supp.2d 972 (N.D.Ill. 2003).

⁸⁷ *Dowling*, 473 U.S. at 224.

against a willful patent infringer? It would appear that the increasingly large patent infringement verdicts, (often in the ranges of tens or even hundreds of millions of dollars), would motivate Congress to apply criminal sanctions to patent infringement as well.

Alternately, it would seem that if civil remedies are sufficient under patent law, that they should likewise be sufficient under copyright law and the DMCA. Perhaps Congress is deterred by the probable culpability of corporate officers and directors under a criminal patent statutory provision. In contrast, it appears that violators of criminal statutes under traditional copyright law are more likely to be individuals, although that is not necessarily the case when criminal sanctions are applied under the DMCA, as described in *U.S. v. Elcom, supra*. Supreme Court Justice Blackmun reflected upon the lack of criminal sanctions for patent infringement in *Dowling*, stating in dicta: “Despite its undoubted power to do so, ... Congress has not provided criminal penalties for distribution of goods infringing valid patents.”⁸⁸

XIV. Tackling the Enforcement Problem – a Proposed Solution

The main problem with recent legislative proposals to increase criminal sanctions for copyright infringement is the lack of effective enforcement provisions. Recently proposed bills provide increased criminal penalties, but tend to fall short when it comes to providing actual funds and personnel for copyright law enforcement. For example, the recently proposed *Piracy Deterrence and Education Act of 2004* recognizes “Many computer users simply believe that they will not be caught or prosecuted for their conduct.”⁸⁹ However, the same proposed bill explicitly states: “Nothing in this section shall be construed to expand the investigative or enforcement powers of the Federal Bureau of Investigation” [and] “The program created

⁸⁸ *Dowling*, 473 U.S. at 227.

⁸⁹ *The Piracy Deterrence and Education Act of 2004*, H.R. _____, 108th Cong., §2(4), (2004).

under subsection (a)(1) shall not use funds or resources of the Department of Justice allocated for criminal investigation or prosecution.”⁹⁰

What is needed is a comprehensive solution to enforce intellectual property rights. Because the Department of Justice and the F.B.I. are already short of critical resources to combat significant national threats such as international terrorism and drug cartels, a new approach is warranted.

What is needed is a dedicated executive branch federal agency to enforce all intellectual property rights. The new Federal Bureau of Intellectual Property (FBIP) would combine the registration and examination functions of the Copyright Office and the Patent & Trademark Office with a contingent of administrative law judges and a new intellectual property enforcement division. The new FBIP would have the goal of reducing the time and dollar cost of enforcing intellectual property rights across the broad spectrum of copyrights, patents, and trademarks.

As an executive branch agency dedicated to the protection and enforcement of intellectual property rights, the proposed FBIP would supersede the present role of the *National Intellectual Property Law Enforcement Coordination Council* (NIPLECC). NIPLECC was created on Sept. 29, 1999 when President Clinton signed into law the *Treasury/Postal Appropriations Bill*.⁹¹ Pursuant to 15 U.S.C. §1128(b), the mission of NIPLECC is to coordinate federal agency activities relating to “domestic and international intellectual property rights enforcement.”

According to a recent article in *Forbes* magazine, “In the 16 years from 1988 through 2002, the average [number of copyright infringement cases] was 2,252 [cases] per year, less than

⁹⁰ *Id.* at §§3(a)(2)(b), 3(a)(2) (c).

⁹¹ Public Law No. 106-58, section 633.

1% of all cases in the U.S. federal courts.”⁹² Such a docket could be better managed by a dedicated system of specialized administrative law judges (ALJs) geographically dispersed throughout the country. The proposed FBIP would ideally be self funding by applying an administrative surcharge against all infringing parties who lost their case before the ALJ tribunal.

The proposed FBIP would have a fully funded enforcement division that would monitor the Internet and commerce in general for all forms of copyright, patent, and trademark infringement. The FBIP would investigate complaints of infringement by intellectual property owners and would have the right to bring actions on behalf of intellectual property owners whose works are allegedly being infringed, including claims of violations under the DMCA.

XV. The expanding penumbra of the DMCA

To date, numerous constitutional challenges to the DMCA have failed and the penumbra of the DMCA appears to be expanding, even beyond the realm of obtaining patent-like protections. Recently, in *Pearl Investments v. Standard I/O*, the U.S. District Court for the District of Maine found that a Virtual Private Network (VPN) “squarely fits the definition of a ‘technological protection measure put in place by the copyright owner to control access to a copyrighted work.’ ”⁹³ Pearl Investments operated a computerized automated trading system configured on a VPN. Pearl alleged that a programmer employed by Standard I/O, Inc. (who developed the trading system under contract with Pearl) violated the DMCA “by circumventing the protections of Pearl’s encrypted, password protected virtual private network (‘VPN’) to gain access to Pearl’s copyrighted software.”⁹⁴

⁹² Manes, Stephen, *Let’s Have Less of Lessig*, Forbes, April 2, 2004 at http://www.forbes.com/2004/04/02/cz_sm_0402manes_print.html.

⁹³ *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp 326, 350 (D. Me., 2003).

⁹⁴ *Id.* at 349.

The rogue programmer was operating his own private automated trading system on a second server connected via router using a “tunnel” to Pearl’s own private network.⁹⁵ The programmer actually had other access to Pearl’s copyrighted software as “he had written the software in question himself and maintained a backup file of it for Pearl.”⁹⁶ Significantly, the *Pearl* court found “the fact that Chunn [the programmer] had alternative means of access to the works is irrelevant to whether the VPN effectively controls access to them.”⁹⁷

If other courts decide to follow the precedent of *Pearl Investments*, then the anti-circumvention protections under the DMCA can and will be used for purposes of protecting any type of Virtual Private Network, including private peer-to-peer (P2P) file sharing networks with access control features, Voice over IP telephone calls, and the like. If this trend continues, it appears likely that the penumbra of the DMCA will encroach upon other relevant existing federal statutes in the areas of computer networks and telecommunications, such as *The Computer Fraud and Abuse Act of 1986*,⁹⁸ the *Wiretap Act*,⁹⁹ and the *Electronic Communications Privacy Act of 1986*,¹⁰⁰ and the *Patriot Act*.¹⁰¹ In summary, the scope of the DMCA appears to be expanding well beyond the original legislative intent of Congress that was focused mainly on protecting digital versions of documents, songs and movies.

XVI. Conclusion

The use of the DMCA to realize *de facto* patent-like protection for devices that have associated access control features, as applied by the *Lexmark* court, is arguably a misuse of the

⁹⁵ *Id.*

⁹⁶ *Id.* at 350.

⁹⁷ *Id.*

⁹⁸ 18 U.S.C. § 1030.

⁹⁹ 18 U.S.C. § 2511(1)(a) - statute only covers messages intercepted during transmission, not those intercepted in storage.

¹⁰⁰ 18 U.S.C. § 1367.

¹⁰¹ H.R. 3162, Sec. 202 - Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

DMCA. Congress clearly intended the DMCA to provide strong protection for traditional copyrightable subject matter published in new digital formats, such as electronic documents, songs, and movies. However, Congress did not likely envision nor intend the DMCA to be applied as a new *de facto* exclusive right that encroaches upon the well established policies and statutes of the U.S. patent system.

Congress did not likely intend for the DMCA to be misused to apply patent-like *de facto* protections to functional devices, as was the clearly the result in *Lexmark*. Congress did not likely intend for the DMCA to be applied to securing computer and telecommunication networks, as was the clear result in *Pearl Investments*.

With respect to remedies, the lack of harmony between patent law and copyright law is striking, especially in the area of criminal sanctions under copyright law and the DMCA. It is self evident that additional criminal sanctions under copyright law are likely to be ineffective unless actual enforcement provisions are enacted into law and funded, such as the proposal to create a new Federal Bureau of Intellectual Property, *supra*.

Given the enormous sums routinely awarded in patent infringement suits, it appears increasingly difficult to justify criminal remedies under copyright law and the DMCA and not under patent law. In the interest of justice, Congress should either eliminate criminal sanctions under copyright law and the DMCA, or Congress should consider instituting criminal sanctions for patent infringement. If the latter policy is eventually adopted, the next patented product you purchase could come with an F.B.I. warning, just like the present warnings found on DVDs and CDs.