DIGITAL RIGHTS MANAGEMENT

Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)

JON O. NEWMAN, *Circuit Judge*.

When the Framers of the *First Amendment* prohibited Congress from making any law "abridging the freedom of speech," they were not thinking about computers, computer programs, or the Internet. But neither were they thinking about radio, television, or movies. Just as the inventions at the beginning and middle of the 20th century presented new *First Amendment* issues, so does the cyber revolution at the end of that century. This appeal raises significant *First Amendment* issues concerning one aspect of computer technology—encryption to protect materials in digital form from unauthorized access. The appeal challenges the constitutionality of the Digital Millennium Copyright Act ("DMCA") and the validity of an injunction entered to enforce the DMCA.

Defendant-Appellant Eric C. Corley and his company, 2600 Enterprises, Inc., (collectively "Corley," "the Defendants," or "the Appellants") appeal from the amended final judgment of the United States District Court for the Southern District of New York (Lewis A. Kaplan, District Judge), entered August 23, 2000, enjoining them from various actions concerning a decryption program known as "DeCSS." The injunction primarily bars the Appellants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS is posted. We affirm.

Introduction

Understanding the pending appeal and the issues it raises requires some familiarity with technical aspects of computers and computer software, especially software called "digital versatile disks" or "DVDs," which are optical media storage devices currently designed to contain movies. Those lacking such familiarity will be greatly aided by reading Judge Kaplan's extremely lucid opinion, beginning with his helpful section "The Vocabulary of this Case".

This appeal concerns the anti-trafficking provisions of the DMCA, which Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would *circumvent* these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201 (a)(1)), but also anyone who would traffic in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201 (a)(2), (b)(1)).

Corley publishes a print magazine and maintains an affiliated web site geared towards "hackers," a digital-era term often applied to those interested in techniques for circumventing protections of computers and computer data from unauthorized access. The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves, including copyright infringers who want to acquire copyrighted material (for personal use or resale) without paying for it.

In November 1999, Corley posted a copy of the decryption computer program "DeCSS" on his web site, http://www.2600.com ("2600.com"). DeCSS is designed to circumvent "CSS," the encryption technology that motion picture studios place on DVDs to prevent the unauthorized viewing and copying

of motion pictures. Corley also posted on his web site links to other web sites where DeCSS could be found.

Plaintiffs-Appellees are eight motion picture studios that brought an action in the Southern District of New York seeking injunctive relief against Corley under the DMCA. Following a full non-jury trial, the District Court entered a permanent injunction barring Corley from posting DeCSS on his web site or from knowingly linking via a hyperlink to any other web site containing DeCSS. The District Court rejected Corley's constitutional attacks on the statute and the injunction.

Corley renews his constitutional challenges on appeal. Specifically, he argues primarily that: (1) the DMCA oversteps limits in the Copyright Clause on the duration of copyright protection; (2) the DMCA as applied to his dissemination of DeCSS violates the *First Amendment* because computer code is "speech" entitled to full *First Amendment* protection and the DMCA fails to survive the exacting scrutiny accorded statutes that regulate "speech"; and (3) the DMCA violates the *First Amendment* and the Copyright Clause by unduly obstructing the "fair use" of copyrighted materials. Corley also argues that the statute is susceptible to, and should therefore be given, a narrow interpretation that avoids alleged constitutional objections.

Background

For decades, motion picture studios have made movies available for viewing at home in what is called "analog" format. Movies in this format are placed on videotapes, which can be played on a video cassette recorder ("VCR"). In the early 1990s, the studios began to consider the possibility of distributing movies in digital form as well. Movies in digital form are placed on disks, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, *i.e.*, one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. This case arises out of the movie industry's efforts to respond to this risk by invoking the anti-trafficking provisions of the DMCA.

I. CSS

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing

agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997, and DVDs quickly gained in popularity, becoming a significant source of studio revenue. In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

II. DeCSS

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any other computer file. DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. The distinction between source code and object code is relevant to this case, so a brief explanation is warranted. A computer responds to electrical charges, the presence or absence of which is represented by strings of 1's and 0's. Strictly speaking, "object code" consists of those 1's and 0's. While some people can read and program in object code, "it would be inconvenient, inefficient and, for most people, probably impossible to do so." Computer languages have been written to facilitate program writing and reading. A program in such a computer language—BASIC, C, and Java are examples—is said to be written in "source code." Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. This task is usually performed by a program called a compiler. Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans. Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code.

In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, *2600: The Hacker Quarterly*, which Corley has been publishing since 1984. As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users—such as threats to online privacy—the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to

circumvent the security systems. Representative articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, . . . you have to show your evidence . . . and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence . . . we have" that there is in fact technology that circumvents CSS. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a story about a picture and not printing the picture." Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to many of these sites. These efforts met with only partial success; a number of sites refused to remove DeCSS. In January 2000, the studios filed this lawsuit.

III. The DMCA

The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." Even before the treaty, Congress had been devoting attention to the problems faced by copyright enforcement in the digital age. Hearings on the topic have spanned several years. This legislative effort resulted in the DMCA.

The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. This provision prohibits a person from "circumventing a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." The Librarian of Congress is required to promulgate regulations every three years exempting from this subsection individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses."

The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work . . . or otherwise to . . . bypass . . . a technological measure, without the authority of the copyright owner."

Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure *that effectively controls access* to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who

traffic in technology that can circumvent "protection afforded by a technological measure *that effectively protects a right of a copyright owner* under" Title 17. In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to *prevent access* to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to *permit access* to a work but *prevent copying* of the work or some other act that infringes a copyright. Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

The DMCA contains exceptions for schools and libraries that want to use circumvention technologies to determine whether to purchase a copyrighted product, individuals using circumvention technology "for the sole purpose" of trying to achieve "interoperability" of computer programs through reverse-engineering, encryption research aimed at identifying flaws in encryption technology, if the research is conducted to advance the state of knowledge in the field, and several other exceptions not relevant here.

The DMCA creates civil remedies and criminal sanctions. It specifically authorizes a court to "grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation."

. . . .

Discussion

. . . .

II. Constitutional Challenge Based on the Copyright Clause

In a footnote to their brief, the Appellants appear to contend that the DMCA, as construed by the District Court, exceeds the constitutional authority of Congress to grant authors copyrights for a "limited time," because it "empowers copyright owners to effectively secure perpetual protection by mixing public domain works with copyrighted materials, then locking both up with technological protection measures." This argument is elaborated in the *amici curiae* brief filed by Prof. Julie E. Cohen on behalf of herself and 45 other intellectual property law professors. For two reasons, the argument provides no basis for disturbing the judgment of the District Court.

First, we have repeatedly ruled that arguments presented to us only in a footnote are not entitled to appellate consideration. Although an *amicus* brief can be helpful in elaborating issues properly presented by the parties, it is normally not a method for injecting new issues into an appeal, at least in cases where the parties are competently represented by counsel.

Second, to whatever extent the argument might have merit at some future time in a case with a properly developed record, the argument is entirely premature and speculative at this time on this record. There is not even a claim, much less evidence, that any Plaintiff has sought to prevent copying of public domain works, or that the injunction prevents the Defendants from copying such works. As Judge Kaplan noted, the possibility that encryption would preclude access to public domain works "does not yet appear to be a problem, although it may emerge as one in the future."

III. Constitutional Challenges Based on the *First Amendment*

A. Applicable Principles

Last year, in one of our Court's first forays into *First Amendment* law in the digital age, we took an "evolutionary" approach to the task of tailoring familiar constitutional rules to novel technological

circumstances, favoring "narrow" holdings that would permit the law to mature on a "case-by-case" basis. In that spirit, we proceed, with appropriate caution, to consider the Appellants' *First Amendment* challenges by analyzing a series of preliminary issues the resolution of which provides a basis for adjudicating the specific objections to the DMCA and its application to DeCSS. These issues, which we consider only to the extent necessary to resolve the pending appeal, are whether computer code is speech, whether computer programs are speech, the scope of *First Amendment* protection for computer code, and the scope of *First Amendment* protection for decryption code. Based on our analysis of these issues, we then consider the Appellants' challenge to the injunction's provisions concerning posting and linking.

1. Code as Speech

Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the *First Amendment*. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for *First Amendment* purposes, it is not because it is written in an obscure language.

2. Computer Programs as Speech

Of course, computer code is not likely to be the language in which a work of literature is written. Instead, it is primarily the language for programs executable by a computer. These programs are essentially instructions to a computer. In general, programs may give instructions either to perform a task or series of tasks when initiated by a single (or double) click of a mouse or, once a program is operational ("launched"), to manipulate data that the user enters into the computer. Whether computer code that gives a computer instructions is "speech" within the meaning of the *First Amendment* requires consideration of the scope of the Constitution's protection of speech.

The *First Amendment* provides that "Congress shall make no law . . . abridging the freedom of speech . . . ." "Speech" is an elusive term, and judges and scholars have debated its bounds for two centuries. Some would confine *First Amendment* protection to political speech. Others would extend it further to artistic expression.

Whatever might be the merits of these and other approaches, the law has not been so limited. Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded *First Amendment* protection.

Thus, for example, courts have subjected to *First Amendment* scrutiny restrictions on the dissemination of technical scientific information, and scientific research, and attempts to regulate the publication of instructions.

Computer programs are not exempted from the category of *First Amendment* speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance on an electric guitar. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer. But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it

is the conveying of information that renders instructions "speech" for purposes of the *First Amendment*. The information conveyed by most "instructions" is how to perform a task.

Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being. A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes. Limiting *First Amendment* protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).

Vartuli is not to the contrary. The defendants in *Vartuli* marketed a software program called "Recurrence," which would tell computer users when to buy or sell currency futures contracts if their computers were fed currency market rates. The Commodity Futures Trading Commission charged the defendants with violating federal law for, among other things, failing to register as commodity trading advisors for their distribution of the Recurrence software. The defendants maintained that Recurrence's cues to users to buy or sell were protected speech, and that the registration requirement as applied to Recurrence was a constitutionally suspect prior restraint. We rejected the defendants' constitutional claim, holding that Recurrence "in the form it was sold and marketed by the defendants" did not generate speech protected by the *First Amendment*.

Essential to our ruling in *Vartuli* was the *manner* in which the defendants marketed the software and intended that it be used: the defendants told users of the software to follow the software's cues "with no second-guessing," and intended that users follow Recurrence's commands "mechanically" and "without the intercession of the mind or the will of the recipient". We held that the values served by the *First Amendment* were not advanced by these instructions, even though the instructions were expressed in words. We acknowledged that some users would, despite the defendants' marketing, refuse to follow Recurrence's cues mechanically but instead would use the commands as a source of information and advice, and that, as to these users, Recurrence's cues might very "well have been 'speech.'" Nevertheless, we concluded that the Government could require registration for Recurrence's intended use because such use was devoid of any constitutionally protected speech.

Vartuli considered two ways in which a programmer might be said to communicate through code: to the user of the program (not necessarily protected) and to the computer (never protected). However, this does not mean that *Vartuli* denied *First Amendment* protection to all computer programs. Since *Vartuli* limited its constitutional scrutiny to the code "as marketed," *i.e.*, as an automatic trading system, it did not have occasion to consider a third manner in which a programmer might communicate through code: to another programmer.

For all of these reasons, we join the other courts that have concluded that computer code, and computer programs constructed from code, can merit *First Amendment* protection, although the scope of such protection remains to be determined.

3. The Scope of *First Amendment* Protection for Computer Code

Having concluded that computer code conveying information is "speech" within the meaning of the *First Amendment*, we next consider, to a limited extent, the scope of the protection that code enjoys. As the District Court recognized, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available. A content-neutral restriction is permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored, which "in this context requires

. . . that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'"

"Government regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech." The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others." The Supreme Court's approach to determining content-neutrality appears to be applicable whether what is regulated is expression, conduct, or any "activity" that can be said to combine speech and non-speech elements.

To determine whether regulation of computer code is content-neutral, the initial inquiry must be whether the regulated activity is "sufficiently imbued with elements of communication to fall within the scope of the First . . . Amendment[]." Computer code, as we have noted, often conveys information comprehensible to human beings, even as it also directs a computer to perform various functions. Once a speech component is identified, the inquiry then proceeds to whether the regulation is "justified without reference to the content of regulated speech."

The Appellants vigorously reject the idea that computer code can be regulated according to any different standard than that applicable to pure speech, *i.e.*, speech that lacks a nonspeech component. Although recognizing that code is a series of instructions to a computer, they argue that code is no different, for *First Amendment* purposes, than blueprints that instruct an engineer or recipes that instruct a cook. We disagree. Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a *First Amendment* analysis that treats code as combining nonspeech and speech elements, *i.e.*, functional and expressive elements.

We recognize, as did Judge Kaplan, that the functional capability of computer code cannot yield a result until a human being decides to insert the disk containing the code into a computer and causes it to perform its function (or programs a computer to cause the code to perform its function). Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe. Judge Kaplan, in a passage that merits extensive quotation, cogently explained why this is especially so with respect to decryption code:

> The focus on functionality in order to determine the level of scrutiny is not an inevitable consequence of the speech-conduct distinction. Conduct has immediate effects on the environment. Computer code, on the other hand, no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really "a proxy for effects or harm" and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.
>
> The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.
>
> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used. And that is not all.

> There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source.
>
> In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.
>
> . . .
>
> These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Causation in the law ultimately involves practical policy judgments. Here, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

The functionality of computer code properly affects the scope of its *First Amendment* protection.

4. The Scope of *First Amendment* Protection for Decryption Code

In considering the scope of *First Amendment* protection for a decryption program like DeCSS, we must recognize that the essential purpose of encryption code is to prevent unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function, CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.

DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products. DeCSS enables anyone to gain access to a DVD movie without using a DVD player.

The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD. However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales. The advent of the Internet creates the potential for instantaneous worldwide distribution of the copied material.

At first glance, one might think that Congress has as much authority to regulate the distribution of computer code to decrypt DVD movies as it has to regulate distribution of skeleton keys, combinations to

safes, or devices to neutralize store product security devices. However, despite the evident legitimacy of protection against unauthorized access to DVD movies, just like any other property, regulation of decryption code like DeCSS is challenged in this case because DeCSS differs from a skeleton key in one important respect: it not only is capable of performing the function of unlocking the encrypted DVD movie, it also is a form of communication, albeit written in a language not understood by the general public. As a communication, the DeCSS code has a claim to being "speech," and as "speech," it has a claim to being protected by the *First Amendment*. But just as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized—indeed, unlawful—access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its *First Amendment* protection.

With all of the foregoing considerations in mind, we next consider the Appellants' *First Amendment* challenge to the DMCA as applied in the specific prohibitions that have been imposed by the District Court's injunction.

B. First Amendment Challenge

The District Court's injunction applies the DMCA to the Defendants by imposing two types of prohibition, both grounded on the anti-trafficking provisions of the DMCA. The first prohibits posting DeCSS or any other technology for circumventing CSS on any Internet web site. The second prohibits knowingly linking any Internet web site to any other web site containing DeCSS. The validity of the posting and linking prohibitions must be considered separately.

1. Posting

The initial issue is whether the posting prohibition is content-neutral, since, as we have explained, this classification determines the applicable constitutional standard. The Appellants contend that the anti-trafficking provisions of the DMCA and their application by means of the posting prohibition of the injunction are content-based. They argue that the provisions "specifically target . . . scientific expression based on the particular topic addressed by that expression—namely, techniques for circumventing CSS." We disagree. The Appellants' argument fails to recognize that the target of the posting provisions of the injunction—DeCSS—has both a nonspeech and a speech component, and that the DMCA, as applied to the Appellants, and the posting prohibition of the injunction target only the nonspeech component. Neither the DMCA nor the posting prohibition is concerned with whatever capacity DeCSS might have for conveying information to a human being, and that capacity, as previously explained, is what arguably creates a speech component of the decryption code. The DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional capability is not speech within the meaning of the *First Amendment*. The Government seeks to "justify," both the application of the DMCA and the posting prohibition to the Appellants solely on the basis of the functional capability of DeCSS to instruct a computer to decrypt CSS, *i.e.*, "without reference to the content of the regulated speech". This type of regulation is therefore content-neutral, just as would be a restriction on trafficking in skeleton keys identified because of their capacity to unlock jail cells, even though some of the keys happened to bear a slogan or other legend that qualified as a speech component.

As a content-neutral regulation with an incidental effect on a speech component, the regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest. The Government's interest in preventing unauthorized access to encrypted copyrighted material is unquestionably substantial, and the regulation of DeCSS by the posting prohibition plainly serves that interest. Moreover, that interest is unrelated to the suppression of free expression. The injunction regulates the posting of DeCSS, regardless of whether DeCSS code contains any information comprehensible by human beings that would qualify as speech. Whether the incidental

regulation on speech burdens substantially more speech than is necessary to further the interest in preventing unauthorized access to copyrighted materials requires some elaboration.

Posting DeCSS on the Appellants' web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet, and such person can then instantly transmit DeCSS to anyone else with Internet access. Although the prohibition on posting prevents the Appellants from conveying to others the speech component of DeCSS, the Appellants have not suggested, much less shown, any technique for barring them from making this instantaneous worldwide distribution of a decryption code that makes a lesser restriction on the code's speech component. It is true that the Government has alternative means of prohibiting unauthorized access to copyrighted materials. For example, it can create criminal and civil liability for those who gain unauthorized access, and thus it can be argued that the restriction on posting DeCSS is not absolutely necessary to preventing unauthorized access to copyrighted materials. But a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective. It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests." The prohibition on the Defendants' posting of DeCSS satisfies that standard.

2. Linking

In considering linking, we need to clarify the sense in which the injunction prohibits such activity. Although the injunction defines several terms, it does not define "linking." Nevertheless, it is evident from the District Court's opinion that it is concerned with "hyperlinks". A hyperlink is a cross-reference (in a distinctive font or color) appearing on one web page that, when activated by the point-and-click of a mouse, brings onto the computer screen another web page. The hyperlink can appear on a screen (window) as text, such as the Internet address ("URL") of the web page being called up or a word or phrase that identifies the web page to be called up, for example, "DeCSS web site." Or the hyperlink can appear as an image, for example, an icon depicting a person sitting at a computer watching a DVD movie and text stating "click here to access DeCSS and see DVD movies for free!" The code for the web page containing the hyperlink includes a computer instruction that associates the link with the URL of the web page to be accessed, such that clicking on the hyperlink instructs the computer to enter the URL of the desired web page and thereby access that page. With a hyperlink on a web page, the linked web site is just one click away.

In applying the DMCA to linking (via hyperlinks), Judge Kaplan recognized, as he had with DeCSS code, that a hyperlink has both a speech and a nonspeech component. It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user's computer screen (or, as Judge Kaplan put it, to "take one almost instantaneously to the desired destination."). As he had ruled with respect to DeCSS code, he ruled that application of the DMCA to the Defendants' linking to web sites containing DeCSS is content-neutral because it is justified without regard to the speech component of the hyperlink. The linking prohibition applies whether or not the hyperlink contains any information, comprehensible to a human being, as to the Internet address of the web page being accessed. The linking prohibition is justified solely by the functional capability of the hyperlink.

Applying the *O'Brien*/*Ward*/*Turner Broadcasting* requirements for content-neutral regulation, Judge Kaplan then ruled that the DMCA, as applied to the Defendants' linking, served substantial governmental interests and was unrelated to the suppression of free expression. We agree. He then carefully considered the "closer call," as to whether a linking prohibition would satisfy the narrow tailoring requirement. In an especially carefully considered portion of his opinion, he observed that strict liability for linking to web sites containing DeCSS would risk two impairments of free expression. Web site operators would be inhibited from displaying links to various web pages for fear that a linked page might contain DeCSS, and a prohibition on linking to a web site containing DeCSS would curtail access to whatever other information was contained at the accessed site.

To avoid applying the DMCA in a manner that would "burden substantially more speech than is necessary to further the government's legitimate interests," Judge Kaplan adapted the standards of *New York Times Co. v. Sullivan* to fashion a limited prohibition against linking to web sites containing DeCSS. He required clear and convincing evidence

> that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.

He then found that the evidence satisfied his three-part test by his required standard of proof.

In response to our post-argument request for the parties' views on various issues, including specifically Judge Kaplan's test for a linking prohibition, the Appellants replied that his test was deficient for not requiring proof of intent to cause, or aid or abet, harm, and that the only valid test for a linking prohibition would be one that could validly apply to the publication in a print medium of an address for obtaining prohibited material. The Appellees and the Government accepted Judge Kaplan's criteria for purposes of asserting the validity of the injunction as applied to the Appellants, with the Government expressing reservations as to the standard of clear and convincing evidence.

Mindful of the cautious approach to *First Amendment* claims involving computer technology expressed in *Name.Space*, we see no need on this appeal to determine whether a test as rigorous as Judge Kaplan's is required to respond to *First Amendment* objections to the linking provision of the injunction that he issued. It suffices to reject the Appellants' contention that an intent to cause harm is required and that linking can be enjoined only under circumstances applicable to a print medium. As they have throughout their arguments, the Appellants ignore the reality of the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Under the circumstances amply shown by the record, the injunction's linking prohibition validly regulates the Appellants' opportunity instantly to enable anyone anywhere to gain unauthorized access to copyrighted movies on DVDs.

At oral argument, we asked the Government whether its undoubted power to punish the distribution of obscene materials would permit an injunction prohibiting a newspaper from printing addresses of bookstore locations carrying such materials. In a properly cautious response, the Government stated that the answer would depend on the circumstances of the publication. The Appellants' supplemental papers enthusiastically embraced the arguable analogy between printing bookstore addresses and displaying on a web page links to web sites at which DeCSS may be accessed. They confidently asserted that publication of bookstore locations carrying obscene material cannot be enjoined consistent with the *First Amendment*, and that a prohibition against linking to web sites containing DeCSS is similarly invalid.

Like many analogies posited to illuminate legal issues, the bookstore analogy is helpful primarily in identifying characteristics that *distinguish* it from the context of the pending dispute. If a bookstore proprietor is knowingly selling obscene materials, the evil of distributing such materials can be prevented by injunctive relief against the unlawful distribution (and similar distribution by others can be deterred by punishment of the distributor). And if others publish the location of the bookstore, preventive relief against a distributor can be effective before any significant distribution of the prohibited materials has occurred. The digital world, however, creates a very different problem. If obscene materials are posted on one web site and other sites post hyperlinks to the first site, the materials are available for instantaneous worldwide distribution before any preventive measures can be effectively taken.

This reality obliges courts considering *First Amendment* claims in the context of the pending case to choose between two unattractive alternatives: either tolerate some impairment of communication in order to permit Congress to prohibit decryption that may lawfully be prevented, or tolerate some decryption in order to avoid some impairment of communication. Although the parties dispute the extent of impairment of communication if the injunction is upheld and the extent of decryption if it is vacated, and differ on the availability and effectiveness of techniques for minimizing both consequences, the

fundamental choice between impairing some communication and tolerating decryption cannot be entirely avoided.

In facing this choice, we are mindful that it is not for us to resolve the issues of public policy implicated by the choice we have identified. Those issues are for Congress. Our task is to determine whether the legislative solution adopted by Congress, as applied to the Appellants by the District Court's injunction, is consistent with the limitations of the *First Amendment*, and we are satisfied that it is.

IV. Constitutional Challenge Based on Claimed Restriction of Fair Use

Asserting that fair use "is rooted in and required by both the Copyright Clause and the *First Amendment*," the Appellants contend that the DMCA, as applied by the District Court, unconstitutionally "*eliminates* fair use" of copyrighted materials. We reject this extravagant claim.

Preliminarily, we note that the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might arguably be enlisted for such a requirement. In *Stewart v. Abend*, the Court merely noted that fair use "'permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster'". In *Campbell v. Acuff-Rose Music, Inc.*, the Court observed, "From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, 'to promote the Progress of Science and useful Arts . . . .'"

We need not explore the extent to which fair use might have constitutional protection, grounded on either the *First Amendment* or the Copyright Clause, because whatever validity a constitutional claim might have as to an application of the DMCA that impairs fair use of copyrighted materials, such matters are far beyond the scope of this lawsuit for several reasons. In the first place, the Appellants do not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits them from making such fair use. They are barred from trafficking in a decryption code that enables unauthorized access to copyrighted materials.

Second, as the District Court properly noted, to whatever extent the anti-trafficking provisions of the DMCA might prevent others from copying portions of DVD movies in order to make fair use of them, "the evidence as to the impact of the anti-trafficking provisions of the DMCA on prospective fair users is scanty and fails adequately to address the issues."

Third, the Appellants have provided no support for their premise that fair use of DVD movies is constitutionally required to be made by copying the original work in its original format. Their examples of the fair uses that they believe others will be prevented from making all involve copying in a digital format those portions of a DVD movie amenable to fair use, a copying that would enable the fair user to manipulate the digitally copied portions. One example is that of a school child who wishes to copy images from a DVD movie to insert into the student's documentary film. 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. Although the Appellants insisted at oral argument that they should not be relegated to a "horse and buggy" technique in making fair use of DVD movies, [36] the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie. 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 unconstitutional limitation of fair use. A film critic making fair use of a movie by quoting selected lines of dialogue has no constitutionally valid claim that the review (in print or on television) would be technologically superior if the reviewer had not been prevented from using a movie camera in the theater, nor has an art student a valid constitutional claim to fair use of a painting by photographing it in a museum. Fair use

has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original.

Conclusion

We have considered all the other arguments of the Appellants and conclude that they provide no basis for disturbing the District Court's judgment. Accordingly, the judgment is affirmed.

United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002)

ORDER DENYING DEFENDANT'S MOTIONS TO DISMISS THE INDICTMENT ON CONSTITUTIONAL GROUNDS

On April 1, 2002, the court heard defendant Elcom Ltd.'s motions to dismiss the indictment for violation of due process and on First Amendment grounds. The government opposed the motions. The court has considered the papers submitted by the parties and amici curiae and had the benefit of oral argument on the motions, and for the reasons set forth below, defendant's motions to dismiss the indictment are denied.

BACKGROUND

1. The Technology: eBooks and the AEBPR

Adobe Systems is a software company headquartered in San Jose, California. Adobe's Acrobat eBook Reader product provides the technology for the reading of books in digital form (i.e., electronic books, or "ebooks") on personal computers. Use of the Adobe eBook format allows publishers or distributors of electronic books to control the subsequent distribution of the ebook, typically by limiting the distribution to those who pay for a copy. These restrictions are imposed by the publisher's use of the Adobe Content Server, which allows the publisher to grant or withhold a range of privileges from the consumer. For example, the ebook publisher may choose whether the consumer will be able to copy the ebook, whether the ebook can be printed to paper (in whole, in part, or not at all), whether the "lending function" is enabled to allow the user to lend the ebook to another computer on the same network of computers, and whether to permit the ebook to be read audibly by a speech synthesizer program. When a consumer purchases an ebook formatted for Adobe Acrobat eBook Reader from an Internet website, the ebook is downloaded directly to the consumer's computer from the ebook distributor's Adobe Content Server. The ebook is accompanied by an electronic "voucher" which is recognized and read by the Adobe Acrobat eBook Reader, which then "knows" that the copy of the ebook can only be read on the computer onto which it has been downloaded. Thus, typically, the purchaser of an ebook may only read the ebook on the computer onto which the ebook was downloaded but may not e-mail or copy the ebook to another computer. The user may or may not be able to print the ebook in paper form or have it audibly read by the computer.

The indictment alleges that "when an ebook purchased for viewing in the Adobe eBook Reader format was sold by the publisher or distributor, the publisher or distributor of the ebook could authorize or limit the purchaser's ability to copy, distribute, print, or have the text read audibly by the computer. Adobe designed the eBook Reader to permit the management of such digital rights so that in the ordinary course of its operation, the eBook Reader effectively permitted the publisher or distributor of the ebook to restrict or limit the exercise of certain copyright rights of an owner of the copyright for an ebook distributed in the eBook Reader format."

Defendant Elcomsoft Company Ltd. ("Elcomsoft") developed and sold a product known as the Advanced eBook Processor ("AEBPR"). AEBPR is a Windows-based software program that allows a user to remove use restrictions from Adobe Acrobat PDF files and files formatted for the Adobe eBook Reader. The program allows a purchaser of an eBook Reader formatted electronic book to convert the format to one that is readable in any PDF viewer without the use restrictions imposed by the publisher. Thus, the restrictions imposed by the publisher are stripped away, leaving the ebook in a "naked PDF" format that is readily copyable, printable, and easily distributed electronically. The conversion accomplished by the AEBPR program enables a purchaser of an ebook to engage in "fair use" of an ebook without infringing the copyright laws, for example, by allowing the lawful owner of an ebook to read it on another computer, to make a back-up copy, or to print the ebook in paper form. The same technology, however, also allows a user to engage in copyright infringement by making and distributing unlawful copies of the ebook. Defendant was indicted for alleged violations of Section 1201(b)(1)(A) and (C) of the Digital Millennium Copyright Act ("DMCA") for allegedly trafficking in and marketing of the AEBPR.

2. The DMCA

Congress enacted the DMCA following the adoption of the World Intellectual Property Organization Copyright Treaty as an expansion of traditional copyright law in recognition of the fact that in the digital age, authors must employ protective technologies in order to prevent their works from being unlawfully copied or exploited. As described by one court:

> In December 1996, the World Intellectual Property Organization ("WIPO"), held a diplomatic conference in Geneva that led to the adoption of two treaties. Article 11 of the relevant treaty, the WIPO Copyright Treaty, provides in relevant part that contracting states "shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."
>
> The adoption of the WIPO Copyright Treaty spurred continued Congressional attention to the adaptation of the law of copyright to the digital age. Lengthy hearings involving a broad range of interested parties both preceded and succeeded the Copyright Treaty. . . . [A] critical focus of Congressional consideration of the legislation was the conflict between those who opposed anti-circumvention measures as inappropriate extensions of copyright impediments to fair use and those who supported them as essential to proper protection of copyrighted materials in the digital age. The DMCA was enacted in October 1998 as the culmination of this process.

Through the DMCA, Congress sought to prohibit certain efforts to unlawfully circumvent protective technologies, while at the same time preserving users' rights of fair use. Some understanding of the interplay between copyright and fair use is essential to understanding the issues confronting Congress and the issues presented here. Fair use and copyright are discussed in more detail below, but in brief, copyright grants authors the exclusive right to make and distribute copies of their original works of authorship but the doctrine of fair use permits a certain amount of copying for limited purposes without infringing the copyright, notwithstanding the exclusive rights of the copyright owner.

As part of the balance Congress sought to strike in protecting the rights of copyright owners while preserving fair use, Congress enacted three new anti-circumvention prohibitions, Section 1201(a)(1), Section 1201(a)(2) and Section 1201(b). The first two provisions target circumvention of technological measures that effectively control access to a copyrighted work; the third targets circumvention of technological measures that impose limitations on the use of protected works.

With regard to the first category, Congress banned both the act of circumventing access control restrictions as well as trafficking in and marketing of devices that are primarily designed for such

circumvention. Specifically, Section 1201(a)(1)(A) provides that "no person shall circumvent a technological measure that effectively controls access to a work protected under this title." Thereafter, Section 1201(a)(2) provides that:

> no person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title [17 U.S.C. § 1 et seq.]; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

The third prohibition, however, addresses a different circumvention, specifically, circumventing a technological measure that imposes limitations on the use of a copyrighted work, or in the words of the statute, that "effectively protects the right of a copyright owner." Using language quite similar to Section 1201(a)(2), the Act provides that:

> no person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title [17 U.S.C.A. § 1 et seq.] in a work or a portion thereof;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Unlike Section 1201(a), however, Congress did not ban the act of circumventing the use restrictions. Instead, Congress banned only the trafficking in and marketing of devices primarily designed to circumvent the use restriction protective technologies. Congress did not prohibit the act of circumvention because it sought to preserve the fair use rights of persons who had lawfully acquired a work. In fact, Congress expressly disclaimed any intent to impair any person's rights of fair use: "Nothing in this section shall affect rights, remedies, or defenses to copyright infringement, including fair use, under this title [17 U.S.C.A. § 1 et seq.]." Thus, circumventing use restrictions is not unlawful, but in order to protect the rights of copyright owners while maintaining fair use, Congress banned trafficking in devices that are primarily designed for the purpose of circumventing any technological measure that "effectively protects a right of a copyright owner," or that have limited commercially significant purposes other than circumventing use restrictions, or that are marketed for use in circumventing the use restrictions.

The difficulty is created by Section 1201(b)'s use of the phrase "effectively protects a right of a copyright owner" to define the prohibited device because the rights of a copyright owner are intertwined with the rights of others. The rights of a copyright owner include the exclusive rights to reproduce the copyrighted work, to prepare derivative works based upon the copyrighted work, to distribute copies by sale or otherwise, to perform the copyrighted work publicly, and to display the copyrighted work publicly. Exceptions to the copyright owner's exclusive rights are set forth in 17 U.S.C. §§ 107-120. One of those exceptions is that the copyright owner loses control over the disposition of a copy of a work upon the sale or transfer of the copy. Thus, once a published copy is sold, the copyright owner has no right to restrict

the further sale or transfer of that copy. In addition, one of the most significant exceptions to the rights of a copyright owner is the doctrine of fair use.

Fair use is a defense to copyright infringement, allowing a certain amount of direct copying for certain uses, without the permission of the copyright owner and notwithstanding the copyright owner's exclusive rights. Section 107 provides that the fair use of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship or research is not an infringement of a copyright. Section 107 also sets forth a series of factors for determining whether any particular use is a "fair use," including: "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." There is no bright line test for determining whether any particular use is a "fair use" or is instead an act of copyright infringement, and each use requires a case-by-case determination.

The interplay between fair use and copyright weaves throughout defendant's motions to dismiss. The parties dispute whether Congress banned, or intended to ban, all circumvention tools or instead banned only those circumvention devices that would facilitate copyright infringement, and if, as a result, the DMCA is unconstitutionally vague. The parties also dispute whether, because of its effect on the fair use doctrine, the DMCA is an unconstitutional infringement upon the First Amendment and whether Congress had the power to enact the legislation. It is to these issues the court will next turn.

DISCUSSION

Defendant's two motions to dismiss the indictment challenge the constitutionality of the DMCA on a number of grounds. Defendant contends that Section 1201(b) is unconstitutionally vague as applied to Elcomsoft and therefore violates the Due Process Clause of the Fifth Amendment. Defendant also contends that Section 1201(b) violates the First Amendment on several grounds: because it constitutes a content-based restriction on speech that is not sufficiently tailored to serve a compelling government interest, because it impermissibly infringes upon the First Amendment rights of third parties to engage in fair use, and because it is too vague in describing what speech it prohibits, thereby impermissibly chilling free expression. Finally, defendant contends that Congress exceeded its constitutional power in enacting the DMCA, and that the Act is therefore unconstitutional. Each argument will be addressed.

1. Fifth Amendment Due Process Challenge

Defendant first contends that Section 1201(b) is unconstitutionally vague as applied to Elcomsoft because it does not clearly delineate the conduct which it prohibits. A statute violates the Due Process Clause of the Fifth Amendment if its prohibitions are not clearly defined. Vagueness may invalidate a statute for either of two reasons: first, the statute may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits, and second, the statute may authorize or encourage arbitrary and discriminatory enforcement. "'It is established that a law fails to meet the requirements of the Due Process Clause if it is so vague and standardless that it leaves the public uncertain as to the conduct it prohibits . . . .'" A criminal statute is not vague if it provides adequate notice of the prohibited conduct in terms that a reasonable person of ordinary intelligence would understand.

Defendant argues that the DMCA bans only those tools that are primarily designed to circumvent usage control technologies in order to enable copyright infringement. Defendant reaches this conclusion because Congress did not ban the act of circumventing use control technologies and expressly refused to do so in order to avoid treading on legitimate fair use. Defendant thus argues that:

> the legislative history and the language of the DMCA establish that Congress did not prohibit the act of circumventing usage control technologies. For reasons directly related to that

> decision, it also did not ban *all* tools which might be used to circumvent usage control technologies. Congress sought to prohibit only those tools which are intended to be used to circumvent usage control technologies for the purpose of copyright infringement. Section 1201(b) does not provide a constitutionally adequate notice of this prohibition.

From the premise that Congress has banned only those tools that are intended to circumvent usage control technologies for the purpose of copyright infringement, defendant then argues that the statute is unconstitutionally vague. "Section 1201(b) is doomed to inherent vagueness because not all tools are banned, and the language of the statute renders it impossible to determine which tools it in fact bans." Defendant argues that because of the nature of the interplay between copyright owners' rights and fair use, any circumvention of a usage control technology for a legitimate purpose—such as for a fair use—must invariably involve circumvention of a technology that "protects the right of a copyright owner." Accordingly, there is no way for a manufacturer to know whether its tool is lawful. Moreover, this statutory vagueness leads to arbitrary enforcement.

The government's opposition brief does not directly address defendant's argument that some circumvention tools are prohibited while other circumvention tools are allowed. At the hearing, however, the government contended that the DMCA imposes a blanket ban on all circumvention tools. According to the government, Section 1201(b) does not prohibit only those tools that circumvent usage controls for the purpose of facilitating copyright infringement; the statute also prohibits tools that circumvent usage controls for the purpose of enabling fair use. Thus, if all tools that are primarily designed or produced for the purpose of circumventing protections afforded by technological measures are banned, the statute is not impermissibly vague.

Thus, the court's initial task is to determine whether the DMCA bans trafficking in all circumvention tools, regardless of whether they are designed to enable fair use or to facilitate infringement, or whether instead the statute bans only those tools that circumvent use restrictions for the purpose of facilitating copyright infringement. If all circumvention tools are banned, defendant's void-for-vagueness challenge necessarily fails.

The court must first consider the statutory language enacted by Congress. Despite defendant's repeated citations to the legislative history, if the language of the statute is clear, there is no need to resort to the legislative history in order to determine the statute's meaning. Section 1201(b) provides that:

> no person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof, that —
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title [17 U.S.C.A. § 1 et seq.] in a work or a portion thereof . . . .

The section is comprised of three parts: 1) trafficking in "any technology," "product," "service," "device," "component" or "part thereof"; 2) that is "primarily designed or produced for the purpose of circumventing protection afforded by a technological measure"; and 3) a technological measure that "effectively protects a right of a copyright owner" under the copyright statute.

The first element targets "any technology, product, service, device, component, or part thereof." This language is not difficult to decipher and is all-encompassing: it includes any tool, no matter its form, that is primarily designed or produced to circumvent technological protection.

Next, the phrase "circumvent protection afforded by a technological measure" is expressly defined in the statute to mean: "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."

Finally, the statute provides that "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." The rights of a copyright owner are specified in 17 U.S.C. § 106. These include the exclusive rights:

> (1) to reproduce the copyrighted work in copies or phonorecords;

> (2) to prepare derivative works based upon the copyrighted work;
>
> (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
>
> (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
>
> (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
>
> (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

Putting Section 1201(b)(2)(B) together with Section 106, a technological measure "effectively protects the right of a copyright owner" if, in the ordinary course of its operation, it prevents, restricts or otherwise limits the exercise of any of the rights set forth in Section 106, such as the rights to reproduce the work, prepare derivative works, distribute copies of the work, perform the work publicly or by digital audio transmission, or display the work publicly.

Taken in combination, Section 1201(b) thus prohibits trafficking in any tool that avoids, bypasses, removes, deactivates, or otherwise impairs any technological measure that prevents, restricts or otherwise limits the exercise of the right to reproduce the work, prepare derivative works, distribute copies of the work, perform the work publicly or by digital audio transmission, or display the work publicly. In short, the statute bans trafficking in any device that bypasses or circumvents a restriction on copying or performing a work. Nothing within the express language would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use. The statute does not distinguish between devices based on the uses to which the device will be put. Instead, all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement. Thus, as the government contended at oral argument, Section 1201(b) imposes a blanket ban on trafficking in or the marketing of any device that circumvents use restrictions.

Because the statutory language is clear, it is unnecessary to consider the legislative history to determine congressional intent or the scope of the statute. Nevertheless, statements within the legislative history support the interpretation reached above. Congress was concerned with promoting electronic commerce while protecting the rights of copyright owners, particularly in the digital age where near exact copies of protected works can be made at virtually no cost and distributed instantaneously on a worldwide basis. Congress recognized that "most acts of circumventing a technological copyright protection measure will occur in the course of conduct which itself implicates the copyright owners rights," i.e., acts of infringement. Accordingly,

> paragraph (b)(1) prohibits manufacturing, importing, offering to the public, providing, or otherwise trafficking in certain technologies, products, services, device, components, or parts thereof that can be used to circumvent a technological protection measure that effectively protects a right of a copyright owner under title 17 in a work or portion thereof. . . . Like paragraph (a)(2), this provision is designed to protect copyright owners . . . .

Congress thus recognized that most uses of tools to circumvent copy restrictions would be for unlawful infringement purposes rather than for fair use purposes and sought to ban all circumvention tools that "can be used" to bypass or avoid copy restrictions.

Defendant relies heavily on congressional intent to preserve fair use but that congressional intent does not change the analysis. The Act expressly disclaims any intent to affect the rights, remedies, limitations, or defenses to copyright infringement, including the right of fair use. Congress' expressed intent to preserve the right of fair use is not inconsistent with a ban on trafficking in circumvention technologies, even those that could be used for fair use purposes rather than infringement. Fair use of a copyrighted work continues to be permitted, as does circumventing use restrictions for the purpose of

engaging in a fair use, even though engaging in certain fair uses of digital works may be made more difficult if tools to circumvent use restrictions cannot be readily obtained.

The inescapable conclusion from the statutory language adopted by Congress and the legislative history discussed above is that Congress sought to ban all circumvention tools because most of the time those tools would be used to infringe a copyright. Thus, while it is not unlawful to circumvent for the purpose of engaging in fair use, it is unlawful to traffic in tools that allow fair use circumvention. That is part of the sacrifice Congress was willing to make in order to protect against unlawful piracy and promote the development of electronic commerce and the availability of copyrighted material on the Internet.

Accordingly, there is no ambiguity in what tools are allowed and what tools are prohibited because the statute bans trafficking in or the marketing of all circumvention devices. Moreover, because all circumvention tools are banned, it was not necessary for Congress to expressly tie the use of the tool to an unlawful purpose in order to distinguish lawful tools from unlawful ones. Thus, the multi-use device authorities cited by defendant, such as the statutes and case law addressing burglary tools and drug paraphernalia, offer defendant no refuge. The law, as written, allows a person to conform his or her conduct to a comprehensible standard and is thus not unconstitutionally vague. Therefore, defendant's motion to dismiss the indictment on due process grounds is denied.

2. First Amendment Challenges

Defendant asserts several First Amendment challenges, arguing that the DMCA violates the First Amendment as applied to the sale of the AEBPR, that the DMCA violates the First Amendment because it infringes the First Amendment rights of third parties, and that the DMCA violates the First Amendment because it is impermissibly vague, thus chilling otherwise protected speech. As an initial matter, however, the government contends that review under the First Amendment is unnecessary. The government offers two arguments: 1) the statute bans the sale of technology and the sale of technology is not "speech"; and 2) the AEBPR, in object code form, is not speech protected by the First Amendment. Neither argument is persuasive.

First, the government erroneously contends that the DMCA does not implicate the First Amendment because defendant's sale of circumvention technology is not speech. While selling is the act giving rise to potential criminal liability under Section 1201(b), the DMCA bans trafficking in the AEBPR, software which at some level contains expression, thus implicating the First Amendment. As noted by defendant in reply, the government could not ban the sale of newspapers without implicating the First Amendment, even if newspapers themselves were not banned. First Amendment scrutiny is triggered because the statute bans the sale of something that at some level contains protected expression.

Second, the government contends that computer code is not speech and hence is not subject to First Amendment protections. The court disagrees. Computer software is expression that is protected by the copyright laws and is therefore "speech" at some level, speech that is protected at some level by the First Amendment. While there is some disagreement over whether object code, as opposed to source code, is deserving of First Amendment protection, the better reasoned approach is that it is protected. Object code is merely one additional translation of speech into a new, and different, language. As the *Reimerdes* court explained:

> It cannot be seriously argued that any form of computer code may be regulated without reference to First Amendment doctrine. The path from idea to human language to source code to object code is a continuum. As one moves from one side to the other, the levels of precision and, arguably, abstraction increase, as does the level of training necessary to discern the idea from the expression. Not everyone can understand each of these forms. Only English speakers will understand English formulations. Principally those familiar with the particular programming language will understand the source code expression. And only a relatively small number of skilled programmers and computer scientists will understand the

> machine readable object code. But each form expresses the same idea, albeit in different ways.
>
> All modes by which ideas may be expressed or, perhaps, emotions evoked—including speech, books, movies, art, and music—are within the area of First Amendment concern. As computer code—whether source or object—is a means of expressing ideas, the First Amendment must be considered before dissemination may be prohibited or regulated. In that sense, computer code is covered, or as sometimes said, "protected" by the First Amendment. But that conclusion still leaves for determination the level of scrutiny to be applied in determining the constitutionality of regulation of computer code.
>
> Accordingly, it is appropriate to consider defendant's First Amendment challenges.

A. Whether the DMCA Violates the First Amendment as Applied to the Sale of AEBPR

Defendant first argues that the DMCA, as applied to the sale of defendant's AEBPR, violates the First Amendment. Defendant's argument is structured as follows: computer code is speech protected by the First Amendment; the DMCA regulates that speech based upon its content because it bans the code that conveys a certain message (i.e., circumventing use restrictions); content-based regulations must be narrowly tailored; the DMCA is not narrowly tailored; ergo, the DMCA is unconstitutional.

In opposition, the government argues that under the appropriate level of scrutiny, the DMCA does not violate the First Amendment as applied to the sale of the AEBPR. The government argues that strict scrutiny is not appropriate because the statute does not target speech and is content-neutral with respect to speech. Under intermediate scrutiny, the government has legitimate interests in promoting electronic commerce and in protecting the rights of copyright owners, and the statute is sufficiently tailored to achieve those objectives without unduly burdening free speech.

In order to determine whether the DMCA violates the First Amendment as applied to the sale of the AEBPR, the court must first determine the appropriate level of scrutiny to apply to the statute. As a general matter, content-based restrictions on speech are permissible only if they serve a compelling state interest and do so by the least restrictive means. On the other hand, if a statute or regulation is content-neutral, it

> will be sustained if "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." To satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests. "Rather, the requirement of narrow tailoring is satisfied 'so long as the . . . regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.'" Narrow tailoring in this context requires, in other words, that the means chosen do not "burden substantially more speech than is necessary to further the government's legitimate interests."

When speech and non-speech elements are combined in a single course of conduct, a sufficiently important government interest in regulating the non-speech element can justify incidental intrusions on First Amendment freedoms.

The principal inquiry in determining whether a statute is content-neutral is whether the government has adopted a regulation of speech because of agreement or disagreement with the message it conveys. The government's purpose is the controlling consideration. Here, the parties have pointed to no portion of the legislative history that demonstrates a congressional intent to target speech because of its expressive content. Rather, Congress sought ways to further electronic commerce and protect intellectual property rights, while at the same time protecting fair use. In order to balance these priorities, Congress sought to ban trafficking in any technology or device that could be used to circumvent technological restrictions that served to protect the rights of copyright owners.

Defendant contends that because this occurs in a digital arena, the technological measures necessarily involve computer code and, thus, necessarily implicate speech protected by the First Amendment. Defendant further argues that the regulation is not content-neutral because it only bans a certain type of speech—speech that allows the circumvention of protection measures—and therefore that strict scrutiny must be applied. "Indeed, it is precisely the content of the code that causes the government to regulate it."

Defendant's argument, however, stretches too far. In the digital age, more and more conduct occurs through the use of computers and over the Internet. Accordingly, more and more conduct occurs through "speech" by way of messages typed onto a keyboard or implemented through the use of computer code when the object code commands computers to perform certain functions. The mere fact that this conduct occurs at some level through expression does not elevate all such conduct to the highest levels of First Amendment protection. Doing so would turn centuries of our law and legal tradition on its head, eviscerating the carefully crafted balance between protecting free speech and permissible governmental regulation.

On its face, the statute does not target speech. Section 1201(b) bans trafficking in devices, whether software, hardware, or other. Thus, strict scrutiny is not appropriate in the absence of any suggestion that Congress sought to ban particular speech, qua speech. Courts that have considered the issue in the context of the DMCA have determined that Congress was not concerned with suppressing ideas but instead enacted the anti-trafficking measures because of the function performed by the code. Thus, to the extent that the DMCA targets computer code, Congress sought to ban the code not because of what the code says, but rather because of what the code does.

Defendant contends that these authorities are wrongly decided and that it is impossible to regulate the "functional" aspects of computer code without necessarily regulating the content of the expressive aspects of the code. Divorcing the function from the message, however, is precisely what the courts have done in other contexts, for example, in determining what portions of code are protectable by copyright and what uses of that same code are permitted as fair uses.

Accordingly, the court concludes that intermediate scrutiny, rather than strict scrutiny, is the appropriate standard to apply. Under this test, the regulation will be upheld if it furthers an important or substantial government interest unrelated to the suppression of free expression, and if the incidental restrictions on First Amendment freedoms are no greater than essential to the furtherance of that interest. By this standard, a statute is constitutional as long as it "promotes a substantial governmental interest that would be achieved less effectively absent the regulation" and the means chosen do not burden substantially more speech than is necessary to further the government's legitimate interests.

1) The Governmental Interests

In this case, there are two asserted governmental interests: preventing the unauthorized copying of copyrighted works and promoting electronic commerce. As noted in the House Report:

> The debate on this legislation highlighted two important priorities: promoting the continued growth and development of electronic commerce; and protecting intellectual property rights. These goals are mutually supportive. A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment. And a plentiful supply of intellectual property—whether in the form of software, music, movies, literature, or other works—drives the demand for a more flexible and efficient electronic marketplace.

Congress recognized that a primary threat to electronic commerce and to the rights of copyright holders was the plague of digital piracy. The Senate Report notes:

> Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy.

> Legislation implementing the treaties provides this protection and creates the legal platform for launching the global digital on-line marketplace for copyrighted works. It will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius. It will also encourage the continued growth of the existing off-line global marketplace for copyrighted works in digital format by setting strong international copyright standards.

Congress has elsewhere expressed its concern over the state of intellectual property piracy:

> Notwithstanding [penalties for copyright infringement] copyright piracy of intellectual property flourishes, assisted in large part by today's world of advanced technologies. For example, industry groups estimate that counterfeiting and piracy of computer software cost the affected copyright holders more than $11 billion last year (others believe the figure is closer to $20 billion). In some countries, software piracy rates are as high as 97% of all sales. The U.S. rate is far lower (25%) but the dollar losses ($2.9 billion) are the highest worldwide. The effect of this volume of theft is substantial: lost U.S. jobs, lost wages, lower tax revenue, and higher prices for honest purchasers of copyrighted software. Unfortunately, the potential for this problem to worsen is great.
>
> These governmental interests are both legitimate and substantial.

2) Whether Section 1201(b) is Sufficiently Tailored

The next step is to determine whether these governmental interests would be promoted less effectively absent the regulation and whether the means chosen burden substantially more speech than is necessary to further the government's interests.

Without the ban on trafficking in circumvention tools, the government's interest in promoting electronic commerce, preserving the rights of copyright holders, and preventing piracy would be undermined. The absence of effective technological restrictions to prevent copyright infringement would inevitably result in even more rampant piracy, with a corresponding likely decrease in the willingness of authors and owners of copyrighted works to produce them in digital form or make the works available on-line. Thus, there is little question that the governmental interests would be promoted less effectively in the absence of the regulation. Nevertheless, there is substantial disagreement between the parties with regard to whether or not the regulation "substantially burdens more speech than is necessary" to achieve the government's interests.

Defendant contends that the DMCA burdens substantially more speech than is necessary to protect copyright holders from digital copyright pirates. First, defendant contends that it was not necessary to ban all circumvention tools, because those tools can serve legitimate purposes. Congress had other options more narrowly tailored to prevent the harm sought: it could have made the penalties for infringement more severe or it could have criminalized the use of the Internet to distribute infringing copies. Second, defendant argues that the DMCA fails to pass constitutional review because

> the government's approach to the DMCA effectively eliminates fair use, limits noninfringing uses and prevents access to material in the public domain and uncopyrightable material protected by "technological measures." Many of these uses are themselves protected expression and none of them constitute copyright infringement. The anti-trafficking provisions of the DMCA do not "respond precisely to the substantive problem which legitimately concerned" [Congress] and that it therefore do [sic, does] not comport with the First Amendment.

The government responds that there are numerous exceptions to the DMCA that demonstrate that the DMCA is sufficiently tailored to withstand intermediate scrutiny:

> Congress carefully balanced, *inter alia*, the needs of law enforcement and other government agencies, computer programmers, encryption researchers, and computer security specialists against the serious problems created by circumvention technology. That defendant

> Elcomsoft's conduct did not fall within the exceptions does not suggest, let alone prove, the DMCA sweeps to broadly.

Defendant's arguments are not persuasive. 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.

For example, nothing in the DMCA prevents anyone from quoting from a work or comparing texts for the purpose of study or criticism. It may be that from a technological perspective, the fair user my find it more difficult to do so—quoting may have to occur the old fashioned way, by hand or by re-typing, rather than by "cutting and pasting" from existing digital media. Nevertheless, the fair use is still available. Defendant has cited no authority which guarantees a fair user the right to the most technologically convenient way to engage in fair use. The existing authorities have rejected that argument.

In the same vein, the DMCA does not "prevent access to matters in the public domain" or allow any publisher to remove from the public domain and acquire rights in any public domain work. Nothing within the DMCA grants any rights to anyone in any public domain work. A public domain work remains in the public domain and no party has any intellectual property right in the expression of that work. A flaw in defendant's argument is that it presumes that the only available version of a public domain work is an electronic, technology-protected, version. If a work is in the public domain, any person may make use of that expression, for whatever purposes desired. To the extent that a publisher has taken a public domain work and made it available in electronic form, and in the course of doing so has also imposed use restrictions on the electronic version, the publisher has not gained any lawfully protected intellectual property interest in the work. The publisher has only gained a technological protection against copying that particular electronic version of the work.

The situation is little different than if a publisher printed a new edition of Shakespeare's plays, but chose to publish the book on paper that was difficult to photocopy. Copy protection measures could be employed, similar to what is now commonly done on bank checks, so that the photocopy revealed printing that is otherwise unnoticeable on the original, perhaps rendering the text difficult to read on the photocopy Would the publisher have thus recaptured Shakespeare's plays from the public domain? No, the publisher has gained no enforceable rights in the works of Shakespeare; all that has happened is that the purchaser of the copy-protected book would be unable to easily make a photocopy of that particular book.

Publishing a public domain work in a restricted format does not thereby remove the work from the public domain, even if it does allow the publisher to control that particular electronic copy. If this is an evil in the law, the remedy is for Congress to prohibit use or access restrictions from being imposed upon public domain works. Or perhaps, if left to the market, the consuming public could decline to purchase public domain works packaged with use restrictions.

In addition, the alternatives proposed by defendant—enacting more severe penalties for copyright infringement—may not be as effective at preventing widespread copyright infringement and electronic piracy as is banning the trafficking in or the marketing of the tools that allow piracy to thrive. Congress certainly could have approached the problem by targeting the infringers, rather than those who traffic in the tools that enable the infringement to occur. However, it is already unlawful to infringe, yet piracy of intellectual property has reached epidemic proportions. Pirates are world-wide, and locating and prosecuting each could be both impossible and ineffective, as new pirates arrive on the scene. But, pirates and other infringers require tools in order to bypass the technological measures that protect against unlawful copying. Thus, targeting the tool sellers is a reasoned, and reasonably tailored, approach to "remedying the evil" targeted by Congress. In addition, because tools that circumvent copyright protection measures for the purpose of allowing fair use can also be used to enable infringement, it is

reasonably necessary to ban the sale of all circumvention tools in order to achieve the objectives of preventing widespread copyright infringement and electronic piracy in digital media. Banning the sale of all circumvention tools thus does not substantially burden more speech than is necessary.

Under intermediate scrutiny, it is not necessary that the government select the least restrictive means of achieving its legitimate governmental interest. By its very nature, the intermediate scrutiny test allows some impingement on protected speech in order to achieve the legitimate governmental objective. A sufficiently important government interest in regulating the targeted conduct can justify incidental limitations on First Amendment freedoms. Having considered the arguments asserted by the parties, the court finds that the DMCA does not burden substantially more speech than is necessary to achieve the government's asserted goals of promoting electronic commerce, protecting copyrights, and preventing electronic piracy.

B. Overbreadth Challenge: Does the DMCA Substantially Burden the First Amendment Rights of Others?

Defendant next asserts a facial challenge to the DMCA, contending that the statute is overbroad because it infringes upon the First Amendment rights of third parties. In a facial challenge on overbreadth grounds, the challenger contends that the statute at issue is invalid because it is so broadly written that it infringes unacceptably on the First Amendment rights of third parties. "A statute will be declared unconstitutional only if the court finds 'a "realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court.'" The overbreadth must be not only 'real, but substantial as well, judged in relation to the statute's plainly legitimate sweep.'" Defendant contends that the DMCA is unconstitutionally overbroad on two grounds: first, the statute impairs the First Amendment right to access non-copyrighted works; and second, the statute precludes third parties from exercising their rights of fair use.

The fatal flaw in defendant's argument, however, is that facial attacks on overbreadth grounds are limited to situations in which the statute or regulation by its terms regulates spoken words or expressive conduct. In *Roulette v. City of Seattle*, Ninth Circuit noted that "the Supreme Court has entertained facial freedom-of-expression challenges only against statutes that, 'by their terms,' sought to regulate 'spoken words,' or patently 'expressive or communicative conduct' such as picketing or handbilling." Reviewing Supreme Court precedent, the Ninth Circuit concluded that "the lesson we take from *Broadrick* and its progeny is that a facial freedom of speech attack must fail unless, at a minimum, the challenged statute 'is directed narrowly and specifically at expression or conduct commonly associated with expression.'" Because the statute at issue in Roulette was addressed to conduct that was not commonly associated with expression—sitting or lying on sidewalks—the Ninth Circuit rejected the facial attack on the ordinance.

Under Roulette, defendant's facial attack on the DMCA necessarily fails. By its terms, the statute is directed to trafficking in or the marketing of "any technology, product, service, device, component, or part thereof," that circumvents usage control restrictions. The statute is not directed "narrowly and specifically at expression or conduct commonly associated with expression." Software as well as hardware falls within the scope of the Act, as does any other technology or device. Accordingly, an overbreadth facial challenge is not available.

Even if the DMCA were to be considered a statute directed at conduct commonly associated with expression and the court were to consider the merits of the facial challenge, however, defendant's argument is ultimately unsuccessful. In order to prevail on a facial overbreadth challenge, defendant must establish that there is a realistic danger that the First Amendment rights of third parties will be significantly compromised. Defendant bases its argument on the assertion that the DMCA "significantly compromises" the First Amendment rights of third parties in two ways: 1) it impacts third parties' rights to access public domain and non-copyrighted works; and 2) it impacts the fair use rights of third parties, which it contends are protected by the First Amendment. Assuming for the sake of discussion that these

asserted rights are protected by the First Amendment, an issue which is not clear, defendant's challenge nevertheless fails because the DMCA does not substantially impair those rights.

Defendant first argues that the DMCA "runs afoul of the First Amendment because it places almost unlimited power in the hands of copyright holders to control information, including information that is not even protected by copyright. Society has a strong interest in the free flow of such information." Thus, according to defendant, because society has a strong interest in the free flow of such information which is based in the First Amendment, the DMCA violates the First Amendment by allowing others to impair that interest.

The argument is not compelling. Bellotti recognized that the First Amendment extends beyond protection of the press and the self-expression of individuals and includes prohibiting the government from limiting the stock of information from which members of the public may draw. Assuming for the sake of argument that it would violate the First Amendment for the government to grant exclusive copyright-like rights in works that have already entered the public domain, that situation is not presented here. The hole in defendant's argument is that the DMCA does not grant anyone exclusive rights in public domain works or otherwise non-copyrighted expression. A public domain work remains in the public domain. Any person may use the public domain work for any purpose—quoting, republishing, critiquing, comparing, or even making and selling copies. Publishing the public domain work in an electronic format with technologically imposed restrictions on how that particular copy of the work may be used does not give the publisher any legally enforceable right to the expressive work, even if it allows the publisher to control that particular copy.

Similarly, with regard to the argument that fair use rights are impaired, as discussed above, the DMCA does not eliminate fair use or substantially impair the fair use rights of anyone. Congress has not banned or eliminated fair use and nothing in the DMCA prevents anyone from quoting from a work or comparing texts for the purpose of study or criticism. The fair user may find it more difficult to engage in certain fair uses with regard to electronic books, but nevertheless, fair use is still available.

Defendant makes much of the right to make a back-up copy of digital media for personal use, holding this right up as an example of how the DMCA eliminates fair use. Defendant relies heavily on *Recording Industry Association of America v. Diamond Multimedia Systems*, for the assertion that the right to make a copy of electronic media for personal, noncommercial use, is a paradigmatic fair use consistent with the Copyright Act. But, defendant overstates the significance and holding of that decision. The Ninth Circuit was not presented with, and did not hold, that the right to make a copy for personal use is protected as a fair use right or protected as a right guaranteed by the Constitution. Rather, the Ninth Circuit was discussing the Audio Home Recording Act of 1992 and the statutory exemption for home taping which protects all noncommercial copying by consumers of digital and analog musical recordings. The court held that copying for personal, noncommercial use was consistent with the Audio Home Recording Act's main purpose of facilitating personal use.

Courts have been receptive to the making of an archival copy of electronic media in order to safeguard against mechanical or electronic failure. Making a back-up copy of an ebook, for personal noncommercial use would likely be upheld as a non-infringing fair use. But the right to make a back-up copy of "computer programs" is a statutory right, expressly enacted by Congress in Section 117(a), and there is as yet no generally recognized right to make a copy of a protected work, regardless of its format, for personal noncommercial use. There has certainly been no generally recognized First Amendment right to make back-up copies of electronic works. Thus, to the extent the DMCA impacts a lawful purchaser's "right" to make a back-up copy, or to space-shift that copy to another computer, the limited impairment of that one right does not significantly compromise or impair of the First Amendment rights of users so as to render the DMCA unconstitutionally overbroad.

C. Whether the DMCA Is Unconstitutionally Vague Under the First Amendment

Defendant's final First Amendment challenge is that the DMCA is unconstitutionally vague under the First Amendment because it "provokes uncertainty among speakers" about precisely what speech is prohibited. Defendant argues that "the DMCA criminalizes the manufacture and sale of a device that 'is *primarily designed* or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title' if the device has 'only *limited commercially significant purpose* or use other than to circumvent a technological measure.'" Defendant's premise is that the DMCA regulates expression based at least in part upon the motive of the speaker, specifically, the purpose for which the program was primarily designed and the extent to which there was a commercially significant purpose in doing so other than the circumvention of copyrighted works. In order to determine if the code violates the DMCA, the seller must assess all possible uses of the technology and determine which are the "*significant purpose[s]*" and what it is "primarily" designed to do.

In opposition, the government argues that the statutory language "primarily designed or produced for" is substantially similar to language that has been upheld in other cases, citing the Supreme Court's decisions in *Village of Hoffman Estates v. The Flipside, Hoffman Estates, Inc.*, and *Posters 'N' Things, Ltd. v. United States*, as well as the Second Circuit's decision in *Richmond Boro Gun Club, Inc. v. City of New York*. The government does not address defendant's argument that the "limited commercially significant purpose" phrase renders the statute impermissibly vague, nor does it address the vagueness argument in the context of the alleged impermissible chilling effect on First Amendment rights.

In reply, defendant argues that this statute is distinguishable from the drug paraphernalia statute at issue in *Flipside*, because

> it should be obvious that it is considerably easier to determine if an item was "designed or marketed for use with illegal drugs" than if it was "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under" Title 17 of the United States Code. The challenged provision in *Flipside* requires only a rudimentary knowledge of illegal drug use. The DMCA, by contrast, requires knowledge of (a) the primary and secondary uses of immensely sophisticated technology, (b) whether the technology "effectively" controls access *vis a vis* other controls, and (c) knowledge of the provisions of Title 17 of the United States Code, which regulates copyrights including its provision as they relate to fair use. The DMCA, to put it mildly, is significantly more difficult to understand, and thus more vague.

Once again, defendant's arguments are not persuasive. The primary flaw in defendant's argument is that the court rejects the contention that the DMCA is a content-based restriction on speech and thus *Reno v. ACLU* is inapplicable. *Reno v. ACLU* involved a challenge to the Communications Decency Act's provisions that sought to protect minors from harmful material on the Internet. The CDA sought to protect children from the primary harmful effects of "indecent" and "patently offensive" speech and was thus a content-based blanket restriction on speech. Among the challenged provisions was the knowing transmission of "obscene or indecent" messages to any recipient under 18 years of age and the knowing sending or displaying to a person under 18 years of age any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The Court held that the statutory language—"indecent" and "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs"—was unconstitutionally vague in the absence of statutory definitions, and as a result would "provoke uncertainty among speakers about how the two standards relate to each other and just what they mean" thereby causing a chilling effect on free speech. Here, by contrast, the DMCA is not a content-based restriction on speech and its restrictions do not "provoke uncertainty among speakers" about what speech is permitted and what speech is prohibited. The statute is not unconstitutionally vague in violation of the First Amendment.

In addition, defendant's attempt to distinguish Flipside and the other authorities is not persuasive, and ultimately, Flipside and Posters 'N' Things are controlling. The "primarily designed for" and "marketed for use" language is not unconstitutionally vague. Similarly, the "has only limited commercially significant purpose other than to circumvent protection afforded by a technological measure that effectively protects the right of a copyright owner under this title" is also not unconstitutionally vague. Section 106 sets forth the rights of a copyright owner; Section 107 sets forth the criteria for the fair use exception. Together with the definitions contained in Section 1201(b)(2), the DMCA's prohibition on trafficking in technologies that circumvent use and copy restrictions is sufficiently clear to withstand a vagueness attack.

3. Congressional Authority to Enact the DMCA

Defendant's final challenge is that Congress exceeded its authority in enacting the DMCA and that, as a result, the statute is unconstitutional. The federal government is one of enumerated powers and Congress may exercise only those powers granted to it. The Constitution contains several express grants of power to Congress, among them the Intellectual Property Clause and the Commerce Clause.

Under the Intellectual Property Clause, Congress is empowered "to promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." This power, while broad, is not unlimited. More than a century ago, the Supreme Court held that Congress could not exercise its Intellectual Property power to grant exclusive rights in matters other than "writings" or "discoveries" such that the Trademark Act of 1876 was not a proper exercise of Congress' Intellectual Property power. Congress may not, for example, grant exclusive rights to writings that do not constitute original works of authorship. Similarly, the Intellectual Property Clause limits Congress' powers so that patents may only be granted in new inventions that are not obvious in view of the existing art and Congress may not authorize the issuance of a patent whose effects are to remove existing knowledge from the public domain.

Under the Commerce Clause, Congress' power is quite broad. Congress may regulate the use of the channels of interstate commerce; may regulate and protect the instrumentalities of interstate commerce, including persons or things in interstate commerce; and may regulate those activities having a substantial relation to, or which substantially affect, interstate commerce. Once again, however, the power is not unlimited and Congress does not have the authority to legislate matters that are of such a local character that there is too remote a connection to interstate commerce. Both parties also agree that, as broad as Congress' Commerce Power is, Congress may not use that power in such a way as to override or circumvent another constitutional restraint.

Defendant argues that Congress exceeded its powers under the Intellectual Property Clause in enacting the DMCA. The government responds that Congress used its Commerce Power to regulate trafficking in devices for gain. Thus, the issue presented is whether the DMCA was within Congress' Commerce Power, generally, and if so, whether Congress was nevertheless prohibited from enacting the DMCA because of other restraints on Congress' power imposed by the Intellectual Property Clause.

With regard to the first issue, Congress plainly has the power to enact the DMCA under the Commerce Clause. "The commerce power 'is the power to regulate; that is, to prescribe the rule by which commerce is to be governed. This power, like all others vested in Congress, is complete in itself, may be exercised to its utmost extend, and acknowledges no limitations, other than are prescribed by the Constitution.'" The DMCA prohibits conduct that has a substantial effect on commerce between the states and commerce with foreign nations. Trafficking in or the marketing of circumvention devices "for gain," as proscribed by Sections 1201(b) and 1204, has a direct effect on interstate commerce. To the extent that circumvention devices enable wrongdoers to engage in on-line piracy by unlawfully copying and distributing copyrighted works of authorship, the sale of such devices has a direct effect on suppressing the market for legitimate copies of the works. Accordingly, there is a rational basis for

concluding that the regulated activity sufficiently affects interstate commerce to establish that Congress had authority under the Commerce Clause to enact the legislation.

The more difficult question, however, is whether Congress was nevertheless precluded from enacting the DMCA by restraints imposed by the Intellectual Property Clause. The Eleventh Circuit was presented with this same issue in the context of the anti-bootlegging statute in *Moghadam.* The statute in that case prohibited persons from making unauthorized recordings of live performances, in effect, granting copyright-like protection to live performances. The defendant challenged the constitutionality of the statute, contending that the Intellectual Property power extended only to "writings" and "inventions," and that a live performance was not a "writing." The government argued that the statute was a valid exercise of Congress' Commerce Power. In a well-reasoned opinion, the Eleventh Circuit first analyzed Supreme Court precedents that could be read to conflict with each other and then resolved the tension in those cases to decide the case before it.

> We note that there is some tension between the former line of cases (*Heart of Atlanta Motel*, the *Trade-Mark Cases* and *Authors League [of America, Inc. v. Oman])* and the *Railway Labor Executives* case. The former cases suggest that in some circumstances the Commerce Clause can be used by Congress to accomplish something that the [Intellectual Property Clause] might not allow. But the *Railway Labor Executives* case suggests that in some circumstances the Commerce Clause cannot be used to eradicate a limitation placed upon Congressional power in another grant of power.

The court then resolved the tension as follows:

> We take as a given that there are some circumstances, as illustrated by *Railway Labor Executives*, in which the Commerce Clause cannot be used by Congress to eradicate a limitation placed upon Congress in another grant of power. For the reasons that follow, we hold that the instant case is not one such circumstance. We hold that the [Intellectual Property] Clause does not envision that Congress is positively forbidden from extending copyright-like protection under other constitutional clauses, such as the Commerce Clause, to works of authorship that may not meet the fixation requirement inherent in the term "Writings." The grant itself is stated in positive terms, and does not imply any negative pregnant that suggests that the term "Writings" operates as a ceiling on Congress' ability to legislate pursuant to other grants. Extending quasi-copyright protection to unfixed live musical performances is in no way inconsistent with the [Intellectual Property] Clause, even if that Clause itself does not expressly authorize such protection. Quite the contrary, extending such protection actually complements and is in harmony with the existing scheme that Congress has set up under the [Intellectual Property] Clause. A live musical performance clearly satisfies the originality requirement. Extending quasi-copyright protection also furthers the purpose of the [Intellectual Property] Clause to promote the progress of the useful arts by securing some exclusive rights to the creative author. . . .
>
> For the foregoing reasons, we conclude that extending copyright-like protection in the instant case is not fundamentally inconsistent with the fixation requirement of the [Intellectual Property] Clause. By contrast, the nonuniform bankruptcy statute at issue in *Railway Labor Executives* was irreconcilably inconsistent with the uniformity requirement of the Bankruptcy Clause of the Constitution.

Accordingly, Moghadam provides an instructive guide and analytical framework for resolving the constitutional question posed. If the statute passed by Congress "is not fundamentally inconsistent with" the Intellectual Property clause and is otherwise within Congress' Commerce Power to enact, then the statute is not an unconstitutional exercise of congressional power. On the other hand, if the statute is "irreconcilably inconsistent" with a requirement of another constitutional provision, then the enactment exceeds congressional authority even if otherwise authorized by the Commerce Clause. With this teaching in mind, the court turns to the DMCA and the Intellectual Property Clause.

The first issue is to determine whether the DMCA is "not fundamentally inconsistent" with the purpose of the Intellectual Property Clause. The purpose of the Intellectual Property Clause is to promote the useful arts and sciences. Thus, the government is empowered to grant exclusive rights to inventors and authors in their respective inventions and original works of authorship, for limited times. This allows the inventor/author a reasonable time in which to reap the economic fruits of his or her inventive or creative labor. As a result of this economic incentive, people are encouraged to engage in inventive and originally expressive endeavors, thereby promoting the arts and sciences. In addition, because the grant of property rights is to be of limited duration, the public will generally benefit, once the exclusive rights expire and the invention or expression becomes dedicated to the public.

According to the government's brief, the DMCA and its legislative history demonstrate that Congress' intent was to protect intellectual property rights and thus promote the same purposes served by the Intellectual Property Clause. The government specifically argues that

> as reflected in the legislative history of the DMCA, Congress recognized that while the purpose of the DMCA was to protect intellectual property rights, the means of doing so involved a dramatic shift from the regulation of the use of information to the regulation of the devices by which information is delivered. For this reason, the legislators viewed the legislation as "paracopyright" legislation that could be enacted under the Commerce Clause. Such a step by Congress to protect the market for digital content as an action under the Commerce Clause cannot be said to override Constitutional restraints of the Intellectual Property Clause, because Congress' fundamental motivation was to protect rights granted under the Intellectual Property Clause in the digital world. Congress recognized that traditional intellectual property laws regulating the use of information border on unenforceable in the digital world; only regulation of the devices by which information is delivered will successfully save constitutionally guaranteed intellectual property rights.

The argument carries some weight. Protecting the exclusive rights granted to copyright owners against unlawful piracy by preventing trafficking in tools that would enable widespread piracy and unlawful infringement is consistent with the purpose of the Intellectual Property Clause's grant to Congress of the power to "promote the useful arts and sciences" by granting exclusive rights to authors in their writings. In addition, Congress did not ban the use of circumvention tools out of a concern that enacting such a ban would unduly restrict the fair use doctrine and expressly sought to preserve fair use. Therefore, on the whole, the DMCA's anti-device provisions are not fundamentally inconsistent with the Intellectual Property Clause.

The second half of the analysis is to determine whether the DMCA is nevertheless "irreconcilably inconsistent" with a limitation contained within the Intellectual Property Clause. Here, defendant and the amici curiae make several arguments, some of which have already been addressed. Defendant and the amici curiae contend that the DMCA is irreconcilably inconsistent with the Intellectual Property Clause because: 1) the Act eliminates fair use; 2) the Act allows publishers to recapture works from the public domain and obtain copyright-like protection in those works; and 3) the Act violates the "limited times" clause by effectively granting copyright owners perpetual rights to protect their works.

The first two contentions have been addressed, and rejected, above. While the DMCA may make certain fair uses more difficult for digital works of authorship published with use restrictions, fair use has not been eliminated. Similarly, the argument that Congress' ban on the sale of circumvention tools has the effect of allowing publishers to claim copyright-like protection in public domain works is tenuous and unpersuasive. Nothing within the DMCA grants any rights to anyone in any public domain work. A public domain work remains in the public domain and any person may make use of the public domain work for any purpose.

Finally, the DMCA does not allow a copyright owner to effectively prevent an ebook from ever entering the public domain, despite the expiration of the copyright. Upon the expiration of the copyright, there is no longer any protectable intellectual property right in the work's expression. The expression may be copied, quoted, republished in new format and sold, without any legally enforceable restriction on

the use of the expression. The publisher/copyright owner has no right to prevent any user from using the work any way the user prefers. At best, the publisher has a technological measure embedded within the digital product precluding certain uses of that particular copy of the work and, in many cases, the user/purchaser has acquiesced in this restriction when purchasing/licensing the work. The essence of a copyright is the legally enforceable exclusive rights to reproduce and distribute copies of an original work of authorship, to make derivative works, and to perform the work publicly, for a limited period of time. None of those rights is extended beyond the statutory term merely by prohibiting the trafficking in or marketing of devices primarily designed to circumvent use restrictions on works in electronic form.

Accordingly, the DMCA does not run afoul of any restraint on Congress' power imposed by the Intellectual Property Clause. Section 1201(b) of the DMCA was within Congress' Commerce Power to enact, and because it is not irreconcilably inconsistent with any provision of the Intellectual Property Clause, Congress did not exceed its constitutional authority in enacting the law.

CONCLUSION

For the foregoing reasons, defendant's motions to dismiss the indictment on constitutional grounds are DENIED.

Lexmark International, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004)

SUTTON, Circuit Judge. This copyright dispute involves two computer programs, two federal statutes and three theories of liability. The first computer program, known as the "Toner Loading Program," calculates toner level in printers manufactured by Lexmark International. The second computer program, known as the "Printer Engine Program," controls various printer functions on Lexmark printers.

The first statute, the general copyright statute, has been with us in one form or another since 1790 and grants copyright protection to "original works of authorship fixed in any tangible medium of expression," but does not "extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery". The second federal statute, the Digital Millenium Copyright Act (DMCA), was enacted in 1998 and proscribes the sale of products that may be used to "circumvent a technological measure that effectively controls access to a work" protected by the copyright statute.

These statutes became relevant to these computer programs when Lexmark began selling discount toner cartridges for its printers that only Lexmark could re-fill and that contained a microchip designed to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not re-filled. In an effort to support the market for competing toner cartridges, Static Control Components (SCC) mimicked Lexmark's computer chip and sold it to companies interested in selling remanufactured toner cartridges.

Lexmark brought this action to enjoin the sale of SCC's computer chips and raised three theories of liability in doing so. Lexmark claimed that SCC's chip copied the Toner Loading Program in violation of the federal copyright statute. It claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Toner Loading Program. And it claimed that SCC's chip violated the DMCA by circumventing a technological measure designed to control access to the Printer Engine Program.

After an evidentiary hearing, the district court decided that Lexmark had shown a likelihood of success on each claim and entered a preliminary injunction against SCC. As we view Lexmark's prospects for success on each of these claims differently, we vacate the preliminary injunction and remand the case for further proceedings.

I.

A.

The Parties. Headquartered in Lexington, Kentucky, Lexmark is a leading manufacturer of laser and inkjet printers and has sold printers and toner cartridges for its printers since 1991. Lexmark is a publicly traded corporation and reported $4.8 billion in revenue for 2003.

Static Control Components is a privately held company headquartered in Sanford, North Carolina. Started in 1987, it currently employs approximately 1,000 workers and makes a wide range of technology products, including microchips that it sells to third-party companies for use in remanufactured toner cartridges.

The Two Computer Programs. The first program at issue is Lexmark's "Toner Loading Program," which measures the amount of toner remaining in the cartridge based on the amount of torque (rotational force) sensed on the toner cartridge wheel. The Toner Loading Program relies upon eight program commands—"add," "sub" (an abbreviation for subtract), "mul" (multiply), "pct" (take a percent), "jump," "if," "load," and "exit"—to execute one of several mathematical equations that convert the torque reading into an approximation of toner level. If the torque is less than a certain threshold value, the program executes one equation to calculate the toner level, and if the torque equals or exceeds that threshold, the program executes a different equation to calculate the toner level. The exact code of the Toner Loading Program varies slightly for each printer model, and this case involves two versions of the program—one for Lexmark's T520 and T522 printer models and another for Lexmark's T620 and T622 printer models. The Toner Loading Program for the T520/522 printers comprises 33 program instructions and occupies 37 bytes of memory, while the Toner Loading Program for the T620/622 printers comprises 45 program commands and uses 55 bytes of memory. To illustrate the modest size of this computer program, the phrase "Lexmark International, Inc. vs. Static Control Components, Inc." in ASCII format would occupy more memory than either version of the Toner Loading Program. The Toner Loading Program is located on a microchip contained in Lexmark's toner cartridges.

The second program is Lexmark's "Printer Engine Program." The Printer Engine Program occupies far more memory than the Toner Loading Program and translates into over 20 printed pages of program commands. The program controls a variety of functions on each printer—e.g., paper feed and movement, and printer motor control. Unlike the Toner Loading Program, the Printer Engine Program is located within Lexmark's printers.

Lexmark obtained Certificates of Registration from the Copyright Office for both programs. Neither program is encrypted and each can be read (and copied) directly from its respective memory chip.

Lexmark's Prebate and Non-Prebate Cartridges. Lexmark markets two types of toner cartridges for its laser printers: "Prebate" and "Non-Prebate." Prebate cartridges are sold to business consumers at an up-front discount. In exchange, consumers agree to use the cartridge just once, then return the empty unit to Lexmark; a "shrink-wrap" agreement on the top of each cartridge box spells out these restrictions and confirms that using the cartridge constitutes acceptance of these terms. Non-Prebate cartridges are sold without any discount, are not subject to any restrictive agreements and may be re-filled with toner and reused by the consumer or a third-party remanufacturer.

To ensure that consumers adhere to the Prebate agreement, Lexmark uses an "authentication sequence" that performs a "secret handshake" between each Lexmark printer and a microchip on each Lexmark toner cartridge. Both the printer and the chip employ a publicly available encryption algorithm known as "Secure Hash Algorigthm-1" or "SHA-1," which calculates a "Message Authentication Code" based on data in the microchip's memory. If the code calculated by the microchip matches the code calculated by the printer, the printer functions normally. If the two values do not match, the printer returns an error message and will not operate, blocking consumers from using toner cartridges that Lexmark has not authorized.

SCC's Competing Microchip. SCC sells its own microchip—the "SMARTEK" chip—that permits consumers to satisfy Lexmark's authentication sequence each time it would otherwise be performed, *i.e.*, when the printer is turned on or the printer door is opened and shut. SCC's advertising boasts that its chip breaks Lexmark's "secret code" (the authentication sequence), which "even on the fastest computer available today . . . would take **Years** to run through all of the possible 8-byte combinations to break." SCC sells these chips to third-party cartridge remanufacturers, permitting them to replace Lexmark's chip with the SMARTEK chip on refurbished Prebate cartridges. These recycled cartridges are in turn sold to consumers as a low-cost alternative to new Lexmark toner cartridges.

Each of SCC's SMARTEK chips also contains a copy of Lexmark's Toner Loading Program, which SCC claims is necessary to make its product compatible with Lexmark's printers. The SMARTEK chips thus contain an identical copy of the Toner Loading Program that is appropriate for each Lexmark printer, and SCC acknowledges that it "slavishly copied" the Toner Loading Program "in the exact format and order" found on Lexmark's cartridge chip. A side-by-side comparison of the two data sequences reveals no differences between them.

The parties agree that Lexmark's printers perform a second calculation independent of the authentication sequence. After the authentication sequence concludes, the Printer Engine Program downloads a copy of the Toner Loading Program from the toner cartridge chip onto the printer in order to measure toner levels. Before the printer runs the Toner Loading Program, it performs a "checksum operation," a "commonly used technique" to ensure the "integrity" of the data downloaded from the toner cartridge microchip. Under this operation, the printer compares the result of a calculation performed on the data bytes of the transferred copy of the Toner Loading Program with the "checksum value" located elsewhere on the toner cartridge microchip. If the two values do not match, the printer assumes that the data was corrupted in the program download, displays an error message and ceases functioning. If the two values do match, the printer continues to operate.

The Lawsuit. On December 30, 2002, Lexmark filed a complaint in the United States District Court for the Eastern District of Kentucky seeking to enjoin SCC (on a preliminary and permanent basis) from distributing the SMARTEK chips. The complaint contained three theories of liability. First, Lexmark alleged that SCC violated the copyright statute by reproducing the Toner Loading Program on its SMARTEK chip. Second, it alleged that SCC violated the DMCA by selling a product that circumvents access controls on the Toner Loading Program. Third, it alleged that SCC violated the DMCA by selling a product that circumvents access controls on the Printer Engine Program.

B.

The district court initially concluded that Lexmark had established a likelihood of success on its copyright infringement claim for SCC's copying of its Toner Loading Program. Computer programs are "literary works" entitled to copyright protection, the court reasoned, and the "requisite level of creativity" necessary to establish the originality of the programs "is extremely low." Because the Toner Loading Program could be written in multiple ways, the district court added, SCC had not rebutted the presumption of validity created by Lexmark's copyright registration for the Toner Loading Program.

In coming to this conclusion, the district court rejected each of the defenses asserted by SCC. First, the district court determined that the Toner Loading Program was not a "lock-out code" (and unprotectable because its elements are dictated by functional compatibility requirements) since "the use of any Toner Loading Program could still result in a valid authentication sequence and a valid checksum." But even if the Toner Loading Program were a "lock-out code," the district court believed copyright infringement had still taken place because "'security systems are just like any other computer program and are not inherently unprotectable.'" Second, the court rejected SCC's fair use defense in view of the commercial purpose of the copying, the wholesale nature of the copying and the effect of the copying on the toner cartridge market. Third, the district court rejected SCC's argument that Lexmark was

"misusing" the copyright laws "to secure an exclusive right or limited monopoly not expressly granted by copyright law."

The district court next determined that Lexmark had established a likelihood of success on its two DMCA claims, one relating to the Toner Loading Program, the other relating to the Printer Engine Program. Observing that the anti-trafficking provision of the DMCA, "prohibits any product or device that circumvents a technological measure that prevents unauthorized access to a copyrighted work," the district court concluded that Lexmark had established a likelihood of success that SCC's SMARTEK chip did this very thing. In the district court's view, Lexmark's authentication sequence (not the checksum calculation) constitutes a "technological measure" that "effectively controls access" to two copyrighted works—the Toner Loading Program and the Printer Engine Program. The authentication sequence, it determined, "controls access" because it "controls the consumer's ability to make use of these programs." Because SCC designed the SMARTEK chip to circumvent Lexmark's authentication sequence, because circumvention was the sole commercial purpose of the SMARTEK chip and because SCC markets these chips as performing that function, the court reasoned that SCC likely had violated the DMCA's prohibitions on marketing circumvention devices.

Finally, the district court determined that the DMCA's "reverse engineering" exception to liability did not apply. Under the exception, circumvention devices may be produced and made available to others "solely for the purpose of enabling interoperability of an independently created program with other programs." The court deemed this defense inapplicable because "SCC's SMARTEK microchips cannot be considered independently created computer programs."

Because Lexmark had established a likelihood of success on the merits, the district court presumed irreparable harm, and concluded that the public interest would favor an injunction against SCC. After weighing other potential hardships, the district court concluded that the preliminary injunction should issue.

. . . .

III.

A.

The Constitution expressly gives Congress the power to grant protection to original works of authorship. Relying on that authority, Congress has established the following standard for copyright protection:

> (a) Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression . . . . Works of authorship include the following categories:
>
> (1) *literary works*; (2) musical works . . . ; (3) dramatic works . . .; (4) pantomimes and choreographic works; (5) pictorial, graphic, and sculptural works; (6) motion pictures and other audiovisual works; (7) sound recordings; and (8) architectural works.
>
> (b) In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

The copyright statute grants owners of protected works the exclusive right to use them in certain ways.

As this case comes to the court, the parties agree that computer programs may be entitled to copyright protection as "literary works" under 17 U.S.C. § 101 and may be protected from infringement under 17 U.S.C. § 106. And that is true with respect to a computer program's object code (the binary code—a series of zeros and ones—that computers can read) and its source code (the spelled-out program commands that humans can read).

The parties also agree that Lexmark has registered the Toner Loading Program with the Copyright Office, which is an infringement suit prerequisite, and which constitutes prima facie evidence of the copyright's validity. And the parties agree that SCC shoulders the burden of rebutting the presumptive validity of Lexmark's copyright.

The parties also share common ground when it comes to most of the general principles of copyright infringement applicable to this case. A plaintiff may establish a claim of copyright infringement by showing (1) ownership of a valid copyright in the computer program at issue (here, the Toner Loading Program) and (2) that the defendant copied protectable elements of the work. The first prong tests the originality and non-functionality of the work, both of which are presumptively established by the copyright registration. The second prong tests whether any copying occurred (a factual matter) and whether the portions of the work copied were entitled to copyright protection (a legal matter). If no direct evidence of copying is available, a claimant may establish this element by showing that the defendant had access to the copyrighted work and that the copyrighted work and the allegedly copied work are substantially similar.

As to the first prong, the Supreme Court has instructed that "original . . . means only that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity," even if the work is not a "novel" one. And although constitutionally mandated, the threshold showing of originality is not a demanding one.

But even if a work is in some sense "original" under § 102(a), it still may not be copyrightable because § 102(b) provides that "in no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of [its] form." This provision embodies the common-law idea-expression dichotomy that distinguishes the spheres of copyright and patent law. "Unlike a patent, a copyright gives no exclusive right to the art disclosed; protection is given only to the expression of the idea—not the idea itself." While this general principle applies equally to computer programs, the task of separating expression from idea in this setting is a vexing one. "Compared to aesthetic works, computer programs hover even more closely to the elusive boundary line described in § 102(b)."

In ascertaining this "elusive boundary line" between idea and expression, between process and non-functional expression, courts have looked to two other staples of copyright law—the doctrines of merger and scenes a faire. Where the "expression is essential to the statement of the idea," or where there is only one way or very few ways of expressing the idea, the idea and expression are said to have "merged." In these instances, copyright protection does not exist because granting protection to the expressive component of the work necessarily would extend protection to the work's uncopyrightable ideas as well. For computer programs, "if the patentable process is embodied inextricably in the line-by-line instructions of the computer program, [] then the process merges with the expression and precludes copyright protection."

For similar reasons, when external factors constrain the choice of expressive vehicle, the doctrine of "scenes a faire"—"scenes," in other words, "that must be done"—precludes copyright protection. In the literary context, the doctrine means that certain phrases that are "standard, stock, . . . or that necessarily follow from a common theme or setting" may not obtain copyright protection. In the computer-software context, the doctrine means that the elements of a program dictated by practical realities—*e.g.*, by hardware standards and mechanical specifications, software standards and compatibility requirements, computer manufacturer design standards, target industry practices, and standard computer programming practices—may not obtain protection. As "an industry-wide goal," programming "efficiency" represents an external constraint that figures prominently in the copyrightability of computer programs.

Generally speaking, "lock-out" codes fall on the functional-idea rather than the original-expression side of the copyright line. Manufacturers of interoperable devices such as computers and software, game consoles and video games, printers and toner cartridges, or automobiles and replacement

parts may employ a security system to bar the use of unauthorized components. To "unlock" and permit operation of the primary device (*i.e.*, the computer, the game console, the printer, the car), the component must contain either a certain code sequence or be able to respond appropriately to an authentication process. To the extent compatibility requires that a particular code sequence be included in the component device to permit its use, the merger and scenes a faire doctrines generally preclude the code sequence from obtaining copyright protection.

In trying to discern whether these doctrines apply, courts tend to "focus on whether the idea is capable of various modes of expression." The question, however, is not whether *any* alternatives theoretically exist; it is whether other options practically exist under the circumstances. In order to characterize a choice between alleged programming alternatives as expressive, in short, the alternatives must be feasible within real-world constraints.

The Supreme Court's decision in *Feist* helps to illustrate the point. In *Feist*, the alleged infringer had included 1,309 of the plaintiff's alphabetically-organized telephone book listings in its own telephone directory. The facts comprising these listings, it was clear, theoretically could have been organized in other ways—for instance, by street address or phone number, or by the age or height of the individual. But by virtue of tradition and settled expectations, the familiar alphabetical structure copied by the defendant amounted to the only organizational option available to the defendant. For these reasons, the Supreme Court determined that alphabetical phone listings did not satisfy the low threshold of originality for copyright protection.

One last principle applies here. Even if the prerequisites for infringement are met—the copyright is valid and SCC copied protectable elements of the work—Congress has established a fair use defense to infringement claims to ensure that copyright protection advances rather than thwarts the essential purpose of copyright: "to promote the Progress of Science and useful Arts." Congress has permitted others to use copyright-protected works, "including . . . by reproduction," when courts determine the use to be "fair" according to a non-exhaustive list of factors:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

With respect to computer programs, "fair use doctrine preserves public access to the ideas and functional elements embedded in copyrighted computer software programs."

B.

In applying these requirements to this case, it helps to clarify the terms of debate between the parties. Lexmark claims copyright protection in, and infringement of, the code that composes its Toner Loading Program. It has not alleged that SCC copied any other portion of its chip, including any of the data on which the SHA-1 algorithm—the authentication sequence or "secret handshake"—appear. Presumably that is because SCC replaced Lexmark's SHA-1 function with a different publicly available encryption program to enable interoperability of its chip with Lexmark's printers. Nor does it matter whether SCC copied the Toner Loading Program knowingly or innocently because copyright infringement does not have a scienter requirement. Finally, when it comes to the merits of the infringement claim, the parties primarily debate whether the Toner Loading Program satisfies the originality requirement (prong one), as distinct from whether any copying by SCC is substantially similar to the Lexmark chip (prong two). That is because the parties agree that SCC's SMARTEK chip copied all aspects of the Toner Loading Program.

In our view, the district court committed three related legal errors in determining that Lexmark had a likelihood of prevailing on its copyright claim with respect to the Toner Loading Program. *First*, the district court concluded that, because the Toner Loading Program "could be written in a number of different ways," it was entitled to copyright protection. In refusing to consider whether "external factors

such as compatibility requirements, industry standards, and efficiency" circumscribed the number of forms that the Toner Loading Program could take, the district court believed that the idea-expression divide and accompanying principles of merger and scenes a faire play a role only in the "substantial similarity" analysis and do not apply when the first prong of the infringement test (copyrightability) is primarily at issue. In taking this path, the district court relied on cases invoking Nimmer's pronouncement that the idea-expression divide "constitutes not so much a limitation on the copyrightability of works, as it is a measure of the degree of similarity that must exist between a copyrightable work and an unauthorized copy." And in concluding more generally that the copyrightability of a computer program turns solely on the availability of other options for writing the program, the court relied on several cases from other circuits.

This reasoning, to start with, conflicts with *Feist*. As the Supreme Court's recent decision suggests, one does not satisfy the originality requirement for copyright protection merely by showing that the work could have been put together in different ways. Just as it failed to suffice in *Feist* that the author of the competing telephone book could have organized the listings in some manner other than the individual's last name, so it does not suffice here that SCC could have written the Toner Loading Program in some other way. As in *Feist*, the court must ask whether the alternative ways of putting together the competing work are feasible in that setting.

Nor does Nimmer support the district court's "a number of different ways" reasoning. As a matter of practice, Nimmer is correct that courts most commonly discuss the idea-expression dichotomy in considering whether an original work and a partial copy of that work are "substantially similar" (as part of prong two of the infringement test), since the copyrightability of a work as a whole (prong one) is less frequently contested. But the idea-expression divide figures into the substantial similarity test not as a measure of "similarity"; it distinguishes the original work's protectable elements from its unprotectable ones, a distinction that allows courts to determine whether any of the former have been copied in substantial enough part to constitute infringement. Both prongs of the infringement test, in other words, consider "copyrightability," which at its heart turns on the principle that copyright protection extends to expression, not to ideas. When a work itself constitutes merely an idea, process or method of operation, or when any discernible expression is inseparable from the idea itself, or when external factors dictate the form of expression, copyright protection does not extend to the work.

Neither do the cited cases support the district court's initial frame of reference. *Franklin Computer* and *Formula International* involved copies of Apple's operating system program—a program whose size and complexity is to the Toner Loading Program what the Sears Tower is to a lamppost. Given the nature of the Apple program, it would have been exceedingly difficult to say that practical alternative means of expression did not exist and indeed no defendant in the cases advanced that argument. And *Franklin Computer* and *Whelan Assocs.* do not establish that *any* variation in the modes of expression establishes copyrightability, as they acknowledge the potential relevance of the merger and scenes a faire doctrines. While *E.F. Johnson* rejected the defendant's argument that the computer software program at issue was not protectable because it was needed for "compatibility" with a certain radio system, it did so only after finding that "the exact duplication of the [program] . . . was not the 'only and essential' means of achieving compatibility."

Second, given the district court's mistaken view of the legal standard for distinguishing protectable expression from unprotectable ideas, the constraints on the Toner Loading Program established by the evidence need to be reconsidered. To discern whether "originality" exists in the work, the court should ask whether the ideas, methods of operation and facts of the program could have been expressed in any for mother than that chosen by the programmer, taking into consideration the functionality, compatability and efficiency demanded of the program.

In presenting evidence in support of its motion for a preliminary injunction, Lexmark focused on establishing that the Toner Loading Program could have been written in other ways. Dr. Maggs, Lexmark's expert, described several possible alternatives in his declaration: (1) different constants and equations could be used; (2) a lookup table could be used in lieu of equations; (3) some measure other

than torque could be used to approximate toner level (e.g., the number of pages printed); or (4) the same equations could be used in a different sequence. He concluded that over 50 different programs could be written to substitute for the Toner Loading Program.

Dr. Goldberg, SCC's expert, acknowledged that certain changes could be made to the program, for example, by changing the sequence of elements in the program, or by writing the Toner Loading Program in a different programming language altogether. But Dr. Goldberg conceded this point only as a theoretical matter, as he concluded that functionality and efficiency considerations precluded any material changes to the Toner Loading Program.

Dr. Goldberg concluded that several external constraints limit the options available in designing the Toner Loading Program. For one, the Printer Engine Program that downloads and executes the program understands only a single programming language composed of eight simple commands. For another, the program must consist of only 55 bytes because the printer downloads only these particular bytes. Efficiency considerations and the physical realities of the printer and toner cartridge also restrict the forms that the Toner Loading Program could take. As a result, Dr. Goldberg concluded, these external factors together "dictate the way that the simple toner loading program looks," and the resulting program is a "no-thought translation of the formulas to the language that the internal loading program must be written in, and [the programmer doesn't] have much choice." Dr. Goldberg responded to Dr. Maggs' testimony that the Toner Loading Program could take alternative forms by noting that Dr. Maggs' proposed changes were trivial—that they did not make any "substantial difference to the nature of the program"—or that they were so inefficient and repetitive as to be "ridiculous." Instead, Dr. Goldberg concluded, the Toner Loading Program as it is written is the most "straightforward, efficient, natural way to express the program." By contrast, Dr. Maggs' testimony did not reference any of these functional considerations discussed by Goldberg, meaning that the record fails to establish any affirmative support for the contention that Dr. Maggs' proposed alternatives satisfy the memory restrictions of the program.

Even aside from Dr. Goldberg's testimony that the Toner Loading Program is the most efficient means of calculating toner levels, the alternatives suggested by Dr. Maggs do not appear to support the district court's initial conclusion that the program is expressive. Dr. Maggs' first and third suggestions—that different equations and values or a different means of measuring toner level altogether could have been used—do not appear to represent alternative means of expressing the ideas or methods of operations embodied in the Toner Loading Program; they appear to be different ideas or methods of operation altogether. Selection from among competing ideas or methods of operation generally does not result in copyright-protectable expression. Nor would the use of a "lookup table" appear to differ meaningfully from the use of other equations directly. Instead of executing a mathematical formula on a given input, this program merely "looks up" in a data table the output of that same formula for the given input value. Finally, Dr. Maggs' fourth suggestion—that the same equations could be reordered—does not appear to show originality because such alterations may be too trivial to support a finding of creative expression.

To the extent these alternatives suggest any originality in the Toner Loading Program, at any rate, the quantum of originality may well be de minimis and accordingly insufficient to support the validity of Lexmark's copyright in the work. Because the district court initially looked at these issues and this evidence through the wrong frame of reference, its conclusion that the Toner Loading Program had sufficient originality to obtain copyright protection does not support the preliminary injunction. At the permanent injunction stage of this dispute, we leave it to the district court in the first instance to decide whether the Toner Loading Program has sufficient originality to warrant copyright protection.

Third, and perhaps most significantly, the district court erred in assessing whether the Toner Loading Program functions as a lock-out code. Even if the constraints described by Dr. Goldberg—the programming language, the program size, efficiency concerns—did not dictate the content of the Toner Loading Program, the fact that it also functions as a lock-out code undermines the conclusion that Lexmark had a probability of success on its infringement claim.

The Toner Loading Program, recall, serves as input to the checksum operation that is performed each time the printer is powered on or the printer door is opened and closed (i.e., for toner cartridge replacement). After downloading a copy of the Toner Loading Program to calculate toner levels, the Printer Engine Program runs a calculation—the checksum—using every data byte of the Toner Loading Program as input. The program then compares the result of that calculation with a "checksum value" that is located elsewhere on Lexmark's toner cartridge chip. If any single byte of the Toner Loading Program is altered, the checksum value will not match the checksum calculation result. Only if the checksum value is correspondingly changed to accommodate any alterations in the data bytes will the printer function.

In addition to its general conclusion that external constraints on the program were not relevant, the district court concluded that the checksum operation did not operate as a strict constraint on the content of the Toner Loading Program because "SCC's identical copying of Lexmark's Toner Loading Programs went beyond that which was necessary for compatibility." According to the district court, the program could be altered rather simply, even in view of the checksum operation, because reasonable trial and error of no more than 256 different data combinations would have enabled SCC to discover and encode the correct checksum value on its chip. In reaching this conclusion, the court downplayed the significance of Dr. Goldberg's testimony regarding the importance of contextual information to the ease or difficulty of guessing the correct checksum value, saying that Dr. Goldberg called the task "extraordinarily difficult," then dismissing his testimony without further explanation. Dr. Goldberg, however, did not describe this endeavor as "extraordinarily difficult" but as "*computationally impossible*"—a point that Lexmark did not then, and does not now, refute. Contrary to Judge Feikens' suggestion, moreover, Lexmark offered no evidence to show that the task of "turning off" the checksum operation altogether (without contextual information) would be any different from, or any less arduous than, the task of altering the checksum value to accommodate another program.

The difficulty of deriving the proper checksum value and the corresponding degree to which the checksum operation acts as a constraint on the content of the bytes comprising the Toner Loading Program may be an open question at the permanent injunction phase. But for purposes of the preliminary injunction, Dr. Goldberg's unchallenged testimony that it would be "computationally impossible" to modify the checksum value without contextual information suffices to establish that the checksum operation imposes a compatibility constraint in the most literal sense possible: if any single byte of the Toner Loading Program is altered, the printer will not function. On this record, pure compatibility requirements justified SCC's copying of the Toner Loading Program.

C.

In defense of the district court's decision, Lexmark raises several other arguments, all unavailing. *First*, Lexmark notes that it "creatively inserted" in the Toner Loading Program a computer code representation of its stock ticker symbol, "LXK." Lexmark describes this segment as "non-functional" because it does not translate into source code contributing to the toner-calculating program. It is not clear whether these three letters would support a finding of creative expression in the work as a whole. What is clear is that the bytes containing the "LXK" reference *are* functional in the sense that they, like the rest of the Toner Loading Program, also serve as input to the checksum operation and as a result amount to a lock-out code that the merger and scenes a faire doctrines preclude from obtaining protection.

Second, Lexmark argues that if the Toner Loading Program is not copyrightable, then "most computer programs would not be copyrightable." But the slope of this decision is neither as slippery nor as steep as Lexmark suggests. Most computer programs do not simultaneously operate as a lock-out code that is "computationally impossible" to alter without input from the programmer; and most programs are not as brief as this one.

In reaching this conclusion, we do not mean to say that brief computer programs are ineligible for copyright protection. Short programs may reveal high levels of creativity and may present simple, yet

unique, solutions to programming quandaries. Just as a mathematician may develop an elegant proof, or an author may express ideas in a spare, simple, but creative manner, *see, e.g.*, e.e. cummings, *Selected Poems* (Richard S. Kennedy ed., 1994), so a computer programmer may develop a program that is brief *and* eligible for protection. But unless a creative flair is shown, a very brief program is less likely to be copyrightable because it affords fewer opportunities for original expression.

Third, invoking the Federal Circuit's decision in *Atari I*, Lexmark argues that even if the Toner Loading Program amounts to a lock-out code, it still may be eligible for protection. In *Atari I*, Nintendo developed a program (known as "10NES") that blocked its game console from accepting unauthorized game cartridges. Relying on this program, Nintendo sold game cartridges that generated a data stream that "unlocked" the game console, allowing it to load and run the game. The Federal Circuit determined that the 10NES program was copyrightable despite arguments that the program constituted unprotectable ideas rather than expression and that the merger doctrine precluded copyright protection.

The Federal Circuit's rationale for accepting copyright protection for the 10NES program does not undermine our conclusion because the 10NES program was not a "lock out" code in the same sense that the Toner Loading Program is. In *Atari*, the data bytes of the 10NES program did not themselves do the "unlocking" of the game console; the program, when executed, generated an arbitrary stream of data that in turn enabled the console to function. That same data stream, the court concluded, could have been produced by a number of alternative programs; for this reason, the expression contained in the computer program did not "merge" with the process. Here, by contrast, the data bytes comprising the Toner Loading Program themselves act as the input to the checksum operation that must be successfully completed for the printer to operate. None of these bytes of the program can be altered without impeding printer functionality given the compatibility requirements created by the checksum operation. Compatibility requirements in *Atari*, in short, did not preclude the possibility of substituting other programs for the 10NES, while they do here.

For like reasons, Judge Feikens is correct that a poem in the abstract could be copyrightable. But that does not mean that the poem receives copyright protection when it is used in the context of a lock-out code. Similarly, a computer program may be protectable in the abstract but not generally entitled to protection when used necessarily as a lock-out device.

D.

In view of our conclusion on this preliminary-injunction record that the Toner Loading Program is not copyrightable, we need not consider SCC's fair-use defense. Yet because this defense could regain relevance at the permanent injunction phase of the case (e.g., if further evidence undermines our conclusion that the program is not copyrightable), two related aspects of the district court's discussion deserve comment.

The district court correctly outlined the four factors for determining whether SCC fairly used Lexmark's Toner Loading Program: (1) the purpose and character of the use, including whether it is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. All of these factors except the second, the district court reasoned, counseled against a finding of fair use, and the second factor favored SCC's position only "slightly." As a result, the court concluded, the fair-use defense did not apply.

With respect to the first factor—the purpose of the use—it is true that a profit-making purpose generally militates against a finding of fair use. But it is not the case that *any* profit-making purpose weighs against fair use, as the "crux" of this factor "is not whether the sole motive of the use is monetary gain." The question is whether "the user stands to profit from exploitation of the *copyrighted material* without paying the customary price." In copying the Toner Loading Program into each of its SMARTEK chips, SCC was not seeking to exploit or unjustly benefit from any creative energy that Lexmark devoted

to writing the program code. As in *Kelly*, SCC's chip uses the Toner Loading Program for a different purpose, one unrelated to copyright protection. Rather than using the Toner Loading Program to calculate toner levels, the SMARTEK chip uses the content of the Toner Loading Program's data bytes as input to the checksum operation and to permit printer functionality. Under these circumstances, it is far from clear that SCC copied the Toner Loading Program for its commercial value *as a copyrighted work*—at least on the preliminary-injunction record we have before us.

With respect to the fourth factor—the effect of the use on the value of the copyrighted material—the relevant question likewise is whether the infringement impacted the market for the copyrighted work itself. In *Kelly*, for example, the Ninth Circuit concluded that the fourth factor favored a finding of fair use because the Internet search engine's utilization of the plaintiff's copyrighted images did not harm the value or marketability of the original photos. Here, the district court focused on the wrong market: it focused not on the value or marketability of the Toner Loading Program, but on Lexmark's market for its toner cartridges. Lexmark's market for its toner cartridges and the profitability of its Prebate program may well be diminished by the SMARTEK chip, but that is not the sort of market or value that copyright law protects. Lexmark has not introduced any evidence showing that an independent market exists for a program as elementary as its Toner Loading Program, and we doubt at any rate that the SMARTEK chip could have displaced any value in *this* market.

IV.

A.

Enacted in 1998, the DMCA has three liability provisions. The statute first prohibits the circumvention of "a technological measure that effectively controls access to a work protected [by copyright]." The statute then prohibits selling devices that circumvent access-control measures:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted work];
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a [copyrighted work]; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a [copyrighted work].

The statute finally bans devices that circumvent "technological measures" protecting "aright" of the copyright owner. The last provision prohibits devices aimed at circumventing technological measures that allow some forms of "access" but restrict other uses of the copyrighted work, such as streaming media, which permits users to view or watch a copyrighted work but prevents them from downloading a permanent copy of the work.

The statute also contains three "reverse engineering" defenses. A person may circumvent an access control measure "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 with other programs, and that have not previously been readily available to [that person]." A person "may develop and employ technological means" that are "necessary" to enable interoperability. And these technological means may be made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." All three defenses apply only when traditional copyright infringement does not occur and only when the challenged actions (in the case of the third provision) would not violate other "applicable laws."

In filing its complaint and in its motion for a preliminary injunction, Lexmark invoked the second liability provision—the ban on distributing devices that circumvent access-control measures placed on copyrighted works. According to Lexmark, SCC's SMARTEK chip is a "device" marketed and sold by SCC that "circumvents" Lexmark's "technological measure" (the SHA-1 authentication sequence, not the checksum operation), which "effectively controls access" to its copyrighted works (the Toner Loading Program and Printer Engine Program). Lexmark claims that the SMARTEK chip meets all three tests for liability under § 1201(a)(2): (1) the chip "is primarily designed or produced for the purpose of circumventing" Lexmark's authentication sequence; (2) the chip "has only limited commercially significant purpose or use other than to circumvent" the authentication sequence; and (3) SCC "markets" the chip "for use in circumventing" the authentication sequence. The district court agreed and concluded that Lexmark had shown a likelihood of success under all three provisions.

B.

We initially consider Lexmark's DMCA claim concerning the Printer Engine Program, which (the parties agree) is protected by the general copyright statute. In deciding that Lexmark's authentication sequence "effectively controls access to a work protected under [the copyright provisions]," the district court relied on a definition in the DMCA saying that a measure "effectively controls access to a work" if, "in the ordinary course of operation," it "requires the application of information, or a process or treatment, with the authority of the copyright owner, to gain access to the work." Because Congress did not explain what it means to "gain access to the work," the district court relied on the "ordinary, customary meaning" of "access": "the ability to enter, to obtain, or to make use of". Based on this definition, the court concluded that "Lexmark's authentication sequence effectively 'controls access' to the Printer Engine Program because it controls the consumer's ability to *make use of* these programs."

We disagree. It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code.

The authentication sequence, it is true, may well block one form of "access"—the "ability to . . . make use of" the Printer Engine Program by preventing the printer from functioning. But it does not block another relevant form of "access"—the "ability to [] obtain" a copy of the work or to "make use of" the literal elements of the program (its code). Because the statute refers to "controlling access to a work protected under this title," it does not naturally apply when the "work protected under this title" is otherwise accessible. Just as one would not say that a lock on the back door of a house "controls access" to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house "controls access" to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works. Add to this the fact that the DMCA not only requires the technological measure to "control[] access" but also requires the measure to control that access "effectively," and it seems clear that this provision does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open.

Nor are we aware of any cases that have applied this provision of the DMCA to a situation where the access-control measure left the literal code or text of the computer program or data freely readable. And several cases apply the provision in what seems to us its most natural sense.

Lexmark defends the district court's contrary ruling on several grounds. *First*, it contends that SCC waived this argument by failing to raise it in the district court. The premise of this argument remains unclear. Below, SCC indeed claimed that the DMCA by its terms did not cover its conduct.

While SCC may not have anticipated the district court's specific reliance on the "to make use of" definition of "access" in its preliminary injunction ruling, the district court's ruling also does not say that SCC conceded the point. Under these circumstances, it is well within our discretion to allow SCC to explain why the district court's resolution of this purely legal question—an interpretation of a statute—is mistaken.

Second, Lexmark counters that several cases have embraced a "to make use of" definition of "access" in applying the DMCA. While Lexmark is partially correct, these cases (and others as well) ultimately illustrate the liability line that the statute draws and in the end explain why access to the Printer Engine Program is not covered.

In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution. For example, the encoded data on CDs translates into music and on DVDs into motion pictures, while the program commands in software for video games or computers translate into some other visual and audio manifestation. In the cases upon which Lexmark relies, restricting "use" of the work means restricting consumers from making use of the copyrightable expression in the work. As shown above, the DMCA applies in these settings when the product manufacturer prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material.

The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, "using" or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program's output is purely functional: the Printer Engine Program "controls a number of operations" in the Lexmark printer such as "paper feed[,] paper movement[,] [and] motor control." And unlike the code underlying video games or DVDs, no encryption or other technological measure prevents access to the Printer Engine Program. Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply.

Lexmark next argues that access-control measures may "effectively control access" to a copyrighted work within the meaning of the DMCA even though the measure may be evaded by an "'enterprising end-user.'" Doubtless, Lexmark is correct that a precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work. Otherwise, the DMCA would apply only when it is not needed.

But our reasoning does not turn on the *degree* to which a measure controls access to a work. It turns on the textual requirement that the challenged circumvention device must indeed circumvent *something*, which did not happen with the Printer Engine Program. Because Lexmark has not directed any of its security efforts, through its authentication sequence or otherwise, to ensuring that its copyrighted work (the Printer Engine Program) cannot be read and copied, it cannot lay claim to having put in place a "technological measure that effectively controls access to a work protected under [the copyright statute]."

Nor can Lexmark tenably claim that this reading of the statute fails to respect Congress's purpose in enacting it. Congress enacted the DMCA to implement the Copyright Treaty of the World Intellectual Property Organization, and in doing so expressed concerns about the threat of "massive piracy" of digital works due to "the ease with which [they] can be copied and distributed worldwide virtually instantaneously." As Congress saw it, "copyrighted works will most likely be encrypted and made available to consumers once payment is made for access to a copy of the work.[People] will try to profit from the works of others by decoding the encrypted codes protecting copyrighted works, or engaging in the business of providing devices or services to enable others to do so." Backing with legal sanctions "the

efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections," Congress noted, would encourage copyright owners to make digital works more readily available.

Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected. In fact, Congress added the interoperability provision in part to ensure that the DMCA would not diminish the benefit to consumers of interoperable devices "in the consumer electronics environment."

C.

In view of our conclusion regarding the Printer Engine Program, we can dispose quickly of Lexmark's DMCA claim regarding the Toner Loading Program. The SCC chip does not provide "access" to the Toner Loading Program but replaces the program. And to the extent a copy of the Toner Loading Program appears on the Printer Engine Program, Lexmark fails to overcome the same problem that undermines its DMCA claim with respect to the Printer Engine Program: Namely, it is not the SCC chip that permits access to the Printer Engine Program but the consumer's purchase of the printer. One other point deserves mention. All three liability provisions of this section of the DMCA require the claimant to show that the "technological measure" at issue "controls access to *a work protected under this title*," which is to say a work protected under the general copyright statute. To the extent the Toner Loading Program is not a "work protected under [the copyright statute],"which the district court will consider on remand, the DMCA necessarily would not protect it.

D.

The district court also rejected SCC's interoperability defense—that its replication of the Toner Loading Program data is a "technological means" that SCC may make "available to others" "solely for the purpose of enabling interoperability of an independently created computer program with other programs." In rejecting this defense, the district court said that "SCC's SMARTEK microchips cannot be considered independently created computer programs. [They] serve no legitimate purpose other than to circumvent Lexmark's authentication sequence and . . . cannot qualify as independently created when they contain exact copies of Lexmark's Toner Loading Programs."

Because the issue could become relevant at the permanent injunction stage of this dispute, we briefly explain our disagreement with this conclusion. In particular, the court did not explain why it rejected SCC's testimony that the SMARTEK chips do contain other functional computer programs beyond the copied Toner Loading Program data. The affidavit of Lynn Burchette, an SCC manager, states that "[the SMARTEK] chip has a microprocessor, with software routines we developed that control its operation and function. Our chip supports additional functionality performed by our software beyond that of [the chip on Lexmark's toner cartridges]." And Dr. Goldberg testified that "Static Control has written a substantial amount of software for managing this chip; for not only providing the interoperability features, but also for managing the additional functionality that the [chip manufacturer] provides and which the remanufacturers may want."

Instead of showing why these statements are wrong, Lexmark contends that this is not "credible evidence" that "independently created computer programs" exist on the SMARTEK chip. Yet Lexmark bears the burden of establishing its likelihood of success on the merits of the DMCA claims. Because Lexmark has offered no reason why the testimony of SCC's experts is not "credible evidence" on this point and has offered no evidence of its own to dispute or even overcome the statements of Burchette and Goldberg, SCC also has satisfied the "independently created computer programs" requirement and may benefit from the interoperability defense, at least in the preliminary injunction context.

Lexmark argues alternatively that if independently created programs do exist, (1) they must have existed prior to the "reverse engineering" of Lexmark's Toner Loading Program, and (2) the technological means must be "necessary or absolutely needed" to enable interoperability of SCC's SMARTEK chip with Lexmark's Printer Engine Program. As to the first argument, nothing in the statute precludes simultaneous creation of an interoperability device and another computer program; it just must be "independently" created. As to the second argument, the statute is silent about the degree to which the "technological means" must be necessary, if indeed they must be necessary at all, for interoperability. The Toner Loading Program copy satisfies any such requirement, however, because without that program the checksum operation precludes operation of the printer (and, accordingly, operation of the Printer Engine Program), unless the checksum value located elsewhere on the chip is modified—which appears to be a computational impossibility without the contextual information that Lexmark does not disclose.

Also unavailing is Lexmark's final argument that the interoperability defense in § 1201(f)(3) does not apply because distributing the SMARTEK chip constitutes infringement and violates other "applicable law" (including tortious interference with prospective economic relations or contractual relations). Because the chip contains only a copy of the thus-far unprotected Toner Loading Program and does not contain a copy of the Printer Engine Program, infringement is not an issue. And Lexmark has offered no independent, let alone persuasive, reason why SCC's SMARTEK chip violates any state tort or other state law.

V.

Because Lexmark failed to establish a likelihood of success on any of its claims, whether under the general copyright statute or under the DMCA, we vacate the district court's preliminary injunction and remand the case for further proceedings consistent with this opinion.