Chapter 3: Copyright of Digital Information

I. Why Digital Works are Different

In many instances, there is no difference with respect to copyright law between digital information (including music, videos, and computer software) and traditional works. However, there are some instances where digital works present substantial new problems for copyright.

I.A. The Ease of Copying and Distributing Digital Works

Until digital works, the economic harm done by a copyright infringement was dependent on the cost of carrying out the infringement. To substantially affect the market for a popular novel, the infringement had to involve a large number of copies and a distribution network to deliver and sell the works. A few hand-made copies of a book would have little effect on the worldwide sale of a printed book. Even using a modern photocopier, it takes time and money to make duplicates of a book, and the result is a lower quality than the printed-and-bound original.

An infringer puts that time and money at risk. If the infringement is stopped by a court, the money spent printing the infringing copies is lost because those copies will be destroyed. If the infringer invested in duplicating facilities or for a distribution network, that investment would also likely be lost.

In contrast, a perfect copy of a digital work can be made and sent anywhere in the world with a few mouse-clicks or keystrokes on a personal computer and an Internet account provided by a school or costing only a few dollars a month. In *United States v. LaMacchia*,[1] a college student set up a system for distributing popular software programs such as WordPerfect and Excel on a college machine available to him at no cost. It was alleged that his "scheme caused losses of more than one million dollars to software copyright holders."[2] The economic harm to a copyright owner that can be caused by an infringer in today's digital world is not limited by the cost of creating and distributing duplicates of the original work nor by the quality of the duplicates since they are identical to the original work.

As Napster and other file-sharing systems (and Prohibition and the 55 mph speed limit) have shown, it is difficult for the law to deter behavior that doesn't seem illegal, especially when you can't go after the millions and millions of people who are breaking the law. (File-sharing using Napster was stopped only because it had a central directory that could be shut down by court order.) File-sharing system users don't think of themselves as copyright infringers, and certainly not as worldwide

---

[1] 871 F.Supp. 535, 33 USPQ2d 1978 (D. Mass. 1994).
[2] 871 F.Supp. at 536-537, 33 USPQ2d at 1979.

distributors of illegal copies. The users feel that they were just sharing music that they liked with others who also like the songs. And the ease of doing it (and the many people involved) makes it seem acceptable.

The market for copyrighted works is a substantial part of our economy, and millions of people who just infringe a little can have a definite effect. As noted by the Senate Judiciary Committee:

> The copyright industries are one of America's largest and fastest growing economic assets. According to International Intellectual Property Alliance statistics, in 1996 (when the last full set of figures was available), the U.S. creative industries accounted for 3.65 percent of the U.S. gross domestic product (GDP) – $278.4 billion. In the last 20 years (1977-1996), the U.S. copyright industries' share of GDP grew more than twice as fast as the remainder of the economy – 5.5 percent vs. 2.6 percent. Between 1977 and 1996, employment in the U.S. copyright industries more than doubled to 3.5 million workers – 2.8 percent of total U.S. employment. Between 1977 and 1996 U.S. copyright industry employment grew nearly three times as fast as the annual rate of the economy as a whole – 4.6 percent vs. 1.6 percent. In fact, the copyright industries contribute more to the U.S. economy and employ more workers than any single manufacturing sector, including chemicals, industrial equipment, electronics, food processing, textiles and apparel, and aircraft. More significantly for the WIPO treaties, in 1996 U.S. copyright industries achieved foreign sales and exports of $60.18 billion, for the first time leading all major industry sectors, including agriculture, automobiles and auto parts, and the aircraft industry.[3]

I.B. Copyright Laws are a Bad Fit

The copyright laws work as well for digital works like compact discs (CDs) and digital video discs (DVDs) as they do for phonograph records and movie films or videocassettes. This is not surprising, since when Congress drafted the Copyright Act of 1976, it intended to end the different treatment for works depending on the form or medium in which the work was fixed. Instead, Congress treated any work of authorship fixed in a tangible medium of expression as protected by copyright, stating:

> Under the bill it makes no difference what the form, manner, or medium of fixation may be – whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device "now known or later developed."[4]

But there are times when the copyright laws are a bad fit for digital works. It is not clear which, if any, of the exclusive rights is infringed when a person makes information available to the world using a file-sharing system like Napster. On the other hand, the copyright laws may overprotect digital works by effectively giving the

[3] Sen. Rep. No. 105-190 at 10.
[4] H.R. Rep. No. 94-1476 at 52.

copyright owners the right to control any access or use of the digital work by controlling the intermediate copies that are made as a work is accessed.

I.B.1. File Sharing

Consider the case where somebody places a digital work on a computer so that the public can access it. This could be done by putting it in a file transfer directory, including it as a Web page, or having it in a location that can be accessed by a file-sharing program like Napster. And assume that the digital work is something like a new movie or popular song and the number of downloads is affecting the market value for the original copyrighted work, so it is reasonable for copyright law to give some protection.

Now consider whether he infringed any of the copyright owner's six 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; and
>
> (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.[5]

I.B.1.a. The Public Distribution Right

Since he is essentially distributing the work to anybody accessing his computer system, it's logical to first look at the distribution right.

The Copyright Act of 1976, like its predecessors, is strongly tied to copies that are fixed in some medium of expression. Copyright comes into being the instant that the first copy of an original expression is made. The definitions in Section 101 makes this tie to physical objects clear:

> "Copies" are material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term "copies" includes the material object, other than a phonorecord, in which the work is first fixed.
>
> "Phonorecords" are material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either

[5] 17 U.S.C. §106.

> directly or with the aid of a machine or device. The term "phonorecords" includes the material object in which the sounds are first fixed.[6]

For this discussion, there is no significant difference between copies and phonorecords and we'll refer to them both as "copies." It's also useful to note that the term "copy" refers not only to reproductions of an original, but also to the original itself, so "copy" doesn't mean a duplication of an existing copy but instead a physical object containing the copyrighted work.

Considering our example, according to the definitions in Section 101, "copies are material objects" and he certainly didn't give any material objects to the public, or anyone else for that matter. While this strong tie to physical objects works well for traditional distributions, it doesn't encompass digital works that are electronically transmitted from place to place.

Another problem with looking to the distribution right for any finding of infringement is that it appears to require that somebody else actually get the work off the server before there is any infringement. But in one case, *Hotaling v. Church of Jesus Christ of Latter-Day Saints*,[7] the court held that actual distribution of work was not necessary:

> When a public library adds a work to its collection, lists the work in its index or catalog system, and makes the work available to the borrowing or browsing public, it has completed all the steps necessary for distribution to the public. At that point, members of the public can visit the library and use the work. Were this not to be considered distribution within the meaning of Section 106(3), a copyright holder would be prejudiced by a library that does not keep records of public use, and the library would unjustly profit by its own omission.[8]

I.B.1.b. The Reproduction Right

Perhaps the reproduction right is the one being infringed in the example. He clearly made a copy of the work when he put it on his hard disk for others to access. And it is likely that a copy was made by the person receiving the copyrighted work. But the act we are really trying to proscribe is his making the work available to the world, not making the single copy when he put it on his hard disk. And that copy might not even be an infringement if he was authorized to install the digital work on his computer and simply allowed the world to access that installed copy.

There is an appeal to finding infringement of either the reproduction or the distribution rights, because those are the rights that would have been infringed if he had made physical copies for everybody receiving the work from him, and then distributed them to anybody wanting them. But he has not distributed a physical copy to anybody, and any reproductions beyond the one he put in the file-sharing directory were made by others.

He may, of course, be a contributory infringer if he was aware of the infringing copies being made by others through his making the software accessible to the world. Contributory infringement results when somebody knows of the direct infringement of another and substantially participates in that infringement, such as inducing,

---

[6] 17 U.S.C. §101.

[7] 118 F.3d 199, 43 USPQ2d 1299 (4th Cir. 1997).

[8] 118 F.3d at 203, 43 USPQ2d at 1302.

causing, or materially contributing to the infringing conduct. But while courts have used this approach to find liability, it would be far better if any liability for infringement came from something he did directly, rather than for the act of another.

I.B.1.c. The Adaptation Right

It would clearly be a stretch to say that he has infringed the adaptation right by preparing a derivative work. As defined in Section 101:

> A "derivative work" is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a "derivative work."[9]

In this case, any copies made were exact copies of the copyrighted work, rather than works "based on" the copyrighted work, and so they are not derivative works.

I.B.1.d. The Public Performance Rights

It would also be a stretch to consider his action as infringing the right "to perform the copyrighted work publicly." Section 101 says:

> To "perform" a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible.[10]

He didn't "recite, render, play, dance, or act" the digital work. He just put it on his hard disk and allowed other people access to it. Again, he might be a contributory infringer if somehow the person who accesses the work on the server later recites, renders, plays, dances, or acts out the work, but it is always unappealing to have to resort to an indirect infringement theory.

I.B.1.e. The Public Display Right

With a little creative reading what he may have infringed is the right "to display the copyrighted work publicly." Section 101 says:

> To "display" a work means to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images nonsequentially.[11]

The display right doesn't seem to have been infringed by placing a digital work on a machine where it is available to the public, but Section 101 also provides two other important definitions:

> To perform or display a work "publicly" means–

---

[9] 17 U.S.C. §101.
[10] 17 U.S.C. §101.
[11] 17 U.S.C. §101.

> (1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or
>
> (2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.[12]

and:

> To "transmit" a performance or display is to communicate it by any device or process whereby images or sounds are received beyond the place from which they are sent.[13]

Clearly, the work can be transmitted to the public, or at least to members of the public one at a time, after the work has been placed in a publicly-accessible directory on a computer. And if the principle that a distribution takes place when all steps necessary for a distribution have been completed is also applied to the display of a work, then there is an argument that the person displayed the work when he put a copy of it in a place where anybody could "look" at it by accessing it.

The problem with that argument is that what has been transmitted is the work itself, not an image of the work. The provisions were really intended to cover the display of a work of art to the public by showing an image of it on a telecast or similar transmission. And any transmission is likely the result of the actions of the user receiving the work, not the one who made the work available on the file-sharing system.

One also has to be careful using a creative argument to try to find infringement of one of the six exclusive rights because there may be an equally-creative argument that there is not infringement found in the special exceptions in the copyright laws. In this case, he may not have infringed the display right because of an exception found in Section 110:

> Notwithstanding the provisions of section 106, the following are not infringements of copyright: . . .
> (5)(A) . . . communication of a transmission embodying a performance or display of a work by the public reception of the transmission on a single receiving apparatus of a kind commonly used in private homes, unless –
>
> (i) a direct charge is made to see or hear the transmission; or
>
> (ii) the transmission thus received is further transmitted to the public.[14]

The personal computer used to received the digital work using the file-sharing system is certainly "a single receiving apparatus of a kind commonly used in private homes." Many, if not most, file-sharing system users download the digital works to their home computers. And it's not much more of a stretch to say that what he is doing is a "communication of a transmission" as it is that he is showing a copy of the work as required to infringe the display right.

---

[12] 17 U.S.C. §101.
[13] 17 U.S.C. §101.
[14] 17 U.S.C. §110(5)(A).

I.B.1.f. What Can Be Done

For the file-sharing example, none of the six exclusive rights really fit the situation and most likely a contributory infringement argument would have to be made. Yet it seems that there should be a direct copyright infringement, since there is little difference in the effect to the copyright owner between distributing a work worldwide through a file-sharing system and distributing the same work by making and distributing physical copies.

It would be best if Congress amended the copyright laws to directly address infringement by those placing copyrighted works on file-sharing systems. A possible approach for such an amendment is suggested by the WIPO Copyright Treaty's new "Right of Communication to the Public":

> . . . authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.[15]

Congress could either add a seventh exclusive right to Section 106, or could enhance one of the existing exclusive rights such as public distribution. The latter may be preferable, since then any existing licenses permitting the distribution of a work would cover both physical and electronic distributions.

I.B.2. Intermediate Copies

There are reproductions of a digital work being made when that work is used on a computer or when it is transmitted through a network. Intermediate copies are made when the work is read from a disk into the computer's memory so that it can be executed or be used as data by an executing program. Other intermediate copies are made in buffers as the work is being sent and received on a network, and in the memory of the routers that are used to pass the information along the network. The world of digital works encompasses countless intermediate copies as the works are being seen, heard, or used.

This can be particularly troublesome for Internet service providers that operate servers and routers where copies are being made, since copyright infringement is generally a "strict liability" civil offense. The intent or knowledge of the infringer is considered only in determining whether an infringement is also a criminal violation (under Section 506,[16] all criminal infringements must be "willful") or in determining damages (under Section 504,[17] statutory damages are increased for willful infringement and reduced if the "infringer was not aware and had no reason to believe that his or her acts constituted an infringement of copyright"). While this may make sense for publishers or distributors of recordings or paper copies, where they can see what is passing through their control as it was being distributed, it is essentially impossible for a service provider to monitor all the bits that are being copied at its installation and to know whether a copy is infringing or was permitted by the copyright owner or by law.

---

[15] WIPO Copyright Treaty, Art. 8.
[16] 17 U.S.C. §506.
[17] 17 U.S.C. §504.

I.B.2.a. A New Right to Control Access and Use?

Since in most instances, intermediate copies need to be made to use a digital work, a strict reading of the reproduction right can turn into a right to control the access to, or use of, a digital work. United States copyright has never given the copyright owner the right to control the personal use an owner of a copyrighted work, such as requiring the payment of a fee for each time a book is read or a painting is viewed. Yet, that could be the result if you require permission of the copyright owner for every reproduction of a digital work.

What, then, gives the person who lawfully has a digital work the right to make the intermediate copies necessary to use the work? Generally, there is an exhaustion doctrine in intellectual property law that says that once there has been an authorized sale without restriction, the patent or copyright owner's further rights are exhausted with respect to the item sold, and that item can be used or resold by its purchaser without permission of the patent or copyright owner. For copyright, this doctrine is codified in as Section 109, the so-called "first sale" provision:

> Notwithstanding the provisions of section 106(3) [the distribution right], the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.[18]

Unfortunately for permitting the making of intermediate digital copies, the language is tied to physical copies and affects only the distribution right. And none of the other statutory exceptions to the exclusive rights of a copyright owner are applicable, either, except for a limited one for computer programs in Section 117.[19] .

I.B.2.b. Transitory Duration?

Perhaps a solution would be to consider the intermediate copies created during the use of a digital work as of transitory duration. Then, according to Section 101, they would not be considered fixed and would not come under the reproduction right.

> A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.[20]

This seems particularly reasonable for the copies made in data communications routers as a message is passed from network to network and for the memory copy made when a computer program is loaded from disk. But copyright owners are concerned that if you say that works stored in computer memory aren't fixed, then people can download songs from a pirate music site and no copies have been made and therefore there is no infringement unless they are later written to a disk. (Of course, if the distribution right is extended to cover transmissions or making a work available to the public, then there would be a direct infringement by the pirate music site.)

---

[18] 17 U.S.C. §109(a).
[19] 17 U.S.C. §117.
[20] 17 U.S.C. §101.

But the leading case addressing whether intermediate copies are of transitory duration found that they weren't. In *MAI v. Peak*,[21] the Ninth Circuit ruled that the copying of a computer program, or other digital work, from a disk drive into the computer's memory met the fixation requirement of the reproduction right. There was some question whether the computer's memory, because its contents are lost when the computer is turned off, was sufficiently permanent to be considered fixed, but the Ninth Circuit found that computer programs, when read into memory, are fixed for purposes of copyright. And because there was nothing particular to computer programs in their reasoning, it applies equally to all digital works.

Although the "transitory duration" argument may have been a way to allow the intermediate copies created when digital works are accessed, the decision in *MAI v. Peak* means that some other approach must be found.

I.B.2.c. Fair Use?

It appears that we are left with that old standby that allows a court to find that something that appears to be an infringement should be allowed anyway to benefit society: fair use. But not every use that somebody would like to make is a fair use. The Supreme Court, in *Campbell v. Acuff-Rose Music*,[22] said:

> The enquiry here may be guided by the examples given in the preamble to Section 107, looking to whether the use is for criticism, or comment, or news reporting, and the like. The central purpose of this investigation is to see, in Justice Story's words, whether the new work merely "supersedes the objects" of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is "transformative." Although such transformative use is not absolutely necessary for a finding of fair use, the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works. Such works thus lie at the heart of the fair use doctrine's guarantee of breathing space within the confines of copyright, and the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use.[23]

But the Supreme Court also found, in its five-to-four Betamax decision,[24] that recording a broadcast television program on a video cassette recorder (VCR) for playback at a later time ("time-shifting") is a fair use because of its noncommercial nature and lack of real harm to the market of something that is essentially provided to viewers for free.

Although the Court mentioned that the VCR could also be used for building a library of past television shows, it didn't rule on whether that went beyond simple time-shifting or was a fair use in its own right. It's not clear whether the idea that time-shifting is a fair use is based on the user's simply viewing the broadcast show at some later time, commercials and all, or whether a time-shifting device that removes

---

[21] 991 F.2d 511, 26 USPQ2d 1458 (9th Cir. 1993).
[22] 510 U.S. 569, 29 USPQ2d 1961 (1994).
[23] 510 U.S. at 578-579, 29 USPQ2d at 1965.
[24] Sony v. Universal City Studios, 464 U.S. 417, 220 USPQ 665 (1984).

the commercials or otherwise alters the show as broadcast is still a fair use. And if the television show were available on demand from the copyright owner, would the argument finding time-shifting a fair use still hold, or would time-shifting merely be a way of superseding the copyright owner's on-demand service?

Fair use, as codified in Section 107,[25] requires us to consider four separate factors in determining whether a use is not an infringement. When we look at the four factors for intermediate copies, we get:

1. Purpose and character of the use: The use is generally not transformative in any way, being an exact copy. But for intermediate copies, the use is necessary for the expected use of the work.
2. Nature of the work: Many digital works, and in particular songs and movies, are primarily expressive rather than factual, so this factor likely goes against the user.
3. Amount of the work copied: Generally, the whole work or a substantial part of the work is being copied, so this goes against the user.
4. Effect on the market: There is little, and perhaps no, effect if the use is necessary for the personal use of something that the user already legally has, as is the case with intermediate copies.

If more weight is given to the effect on the market and the purpose of the use, which is often what is done, then intermediate copies might be a fair use.

But relying on fair use may cause other problems. The Copyright Office noted, in their report on first sale,[26] that there is an unanticipated interaction between first sale and fair use. If I record a TV movie for time-shifting, the Betamax decision holds that such recording is a fair use. But now, I'm the owner of a particular lawful copy, and under Section 109[27] get to sell it. This is clearly not the result intended, but it shows the problem of relying on fair use to justify acceptable behavior, rather than having a specific exception.

I.B.2.d. What Can Be Done

Congress has already provided an example of what should be done to address intermediate copies. For computer programs, Section 117 provides special permissions:

> It is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:
>
> (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
>
> (2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.[28]

---

[25] 17 U.S.C. §107.
[26] United States Copyright Office, Digital Millennium Copyright Act Section 104 Report, http://www.copyright.gov/reports/studies/dmca/dmca_study.html.
[27] 17 U.S.C. §109.
[28] 17 U.S.C. §117.

There is some question about whether a person who gets a packaged computer program from a store is the "owner of a copy" (which is what one expects to be after buying a program) or just a "licensee" of the program (as the software vendor generally claims in a "shrink-wrap license"). However, Section 117 indicates Congress's recognition that intermediate copies need to be made to use a computer program, and that such reproductions are not infringing copies.

But Section 117 is limited to computer programs, which are defined in Section 101 as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result."[29] While an argument can be made that any digital information (data, music, document) can be considered instructions that bring about a certain result in a computer, such as showing a picture or playing a song, such an expansive reading would read out any limitation in the definition and so isn't reasonable.

It would be far better for Congress to provide a specific exception to the copyright owner's exclusive rights for uses of digital works that virtually everybody believe are legitimate (except for those copyright owners trying to bootstrap a level of control because the access and use of digital works require the making of intermediate copies). In addition to the special treatment for intermediate copies of computer programs in Section 117, Congress has provided special treatment for noncommercial copying of musical recordings[30] as well as a variety of other uses of copyrighted works.[31] Having clear rules for digital works would help conscientious users avoid copyright infringement, allow teaching people what they should or shouldn't do, allow fair use to return to its original purpose of protecting productive and transformational uses, and avoid unintended consequences caused by the interaction of fair use determinations with other provisions of the copyright laws.

II. Protecting Digital Information

II.A. The Audio Home Recording Act

Congress first addressed copyright and digital information in the 1992 Audio Home Recording Act (AHRA).[32] The AHRA was the result of years of discussions and hearings on how to address digital copies of sound recordings, which could provide the perfect copies feared by the record companies. As with most copyright legislation, the result was a grand compromise, with Congress trying to address the legitimate concerns of every party in the negotiations.

What the copyright owners got was a mandatory copy management system that had to be included on every digital audio recording device or digital audio interface device.[33] The Serial Copy Management System allows the making of unlimited copies from an original digital recording but prevents any copies being made from those copies. To compensate copyright owners and featured performers, a royalty is required for every digital audio recording device and digital audio recording medium sold.[34]

---

[29] 17 U.S.C. §101.
[30] 17 U.S.C. §1008.
[31] *See* 17 U.S.C. §§108-122.
[32] 17 U.S.C. §1001 *et seq.*
[33] 17 U.S.C. §1002.
[34] 17 U.S.C. §1003.

The computer industry got left alone. The definition of a digital audio recording device requires that it be "designed and marketed for the primary purpose of . . . making a digital audio copied recording for private use,"[35] and digital audio recording medium excluded any medium primarily marketed or used "for the purpose of making copies of nonmusical literary works, including computer programs and databases."[36]

Consumers got a statement regarding their rights to make copies of musical recordings, although the user provision of Section 1008 certainly isn't a model of clarity:

> No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.[37]

Because of the exceptions given the computer industry, Section 1008 does not apply to most copying on a personal computer (PC) of a music compact disc (CD). The user provision applies only to copying using "such a device or medium," which limits the provision to an act where "a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium" is employed. In the CD copying neither an analog recording device nor an analog recording medium is used.

Section 1001 gives some non-intuitive definitions, but it is clear that a "digital audio recording device" is not a PC, since a PC is not "designed or marketed for the primary purpose of . . . making a digital audio copied recording for private use."[38] The original CD is not a "digital audio recording medium" because it "embodies a sound recording at the time it is first distributed by the importer or manufacturer." Neither is the output CD, if it is one of the normal ones you buy at a computer or office supply store because it is "primarily marketed and most commonly used by consumers . . . for the purpose of making copies of nonmusical literary works, including computer programs or data bases." There are blank CD media sold for making digital audio recordings, where the required royalty has been paid, and their use would bring a user within the protection against an infringement suit if the copy that is made is for noncommercial use.

The Serial Copy Management System is a part of every digital audio tape (DAT) drive, and also any CD writer that is not part of a computer system. But because neither of those devices achieved any consumer popularity, the Audio Home Recording Act didn't meet the expectations of the copyright owners, although it did clarify that analog copies of musical recordings made for a noncommercial use were not copyright infringements.

---

[35] 17 U.S.C. §1001(3).
[36] 17 U.S.C. §1001(4).
[37] 17 U.S.C. §1008.
[38] *See* Recording Industry Association ofAmerica v. Diamond Multimedia, 180 F.3d 1072, 51 USPQ2d 1115 (9th Cir. 1999).

II.B. The White Paper

II.C. Digital Sound Recordings

III. What Not to Protect

As important as what is protected by copyright is what isn't protected. Since the use of a digital work generally involves the making of many intermediate copies, such as from disk to computer memory or from router to router, an all-encompassing reproduction right could effectively give the copyright owner the right to control all uses of the digital work. It could also make a network service provider an infringer when there is no practical way for that service provider to know of the infringement or control it.

III.A. The Court Decisions

III.A.1. *Netcom*

III.A.2. When a Service Provider Will Be Liable

III.B. Congress Codifies the Decisions

In 1998, Congress updated the copyright laws by passing the Digital Millennium Copyright Act (DMCA).[69] In the report that accompanied the Senate version of the bill, the Committee on the Judiciary stated the reasons why Congress needed to act:

> 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.
>
> At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. For example, service providers must make innumerable electronic copies by simply transmitting information over the Internet. Certain electronic copies are made to speed up the delivery of information to users. Other electronic copies are made in order to host World Wide Web sites. Many service providers engage in directing users to sites in response to inquiries by users or they volunteer sites that users may find attractive.

[69] Pub. L. 105-304, 112 Stat. 2860.

> Some of these sites might contain infringing material. In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.[70]

Content providers had pushed for a bill to better protect their copyrights in the digital world, along the lines of the recommendations of the White Paper. But there were many substantial objections from users and service providers that the White Paper proposals tipped the balance too much in favor of the content providers, since the White Paper proposed strong measures protecting the technology that prevents copying of digital information while not providing exceptions for normal and necessary copying. When the bills implementing the White Paper recommendations went nowhere after they were introduced in Congress, the Clinton Administration and the content providers worked hard for the adoption of a new treaty extending the Berne Convention to address digital works. But because that treaty required changes to the copyright act before it could be ratified, particularly in the areas of rights management information (digital copyright notices) and technological protection measures, the ball was back in Congress's court.

Because the general acceptance of the *Netcom*[71] decision made it clear that service providers should not be the deep pockets to compensate the copyright owners when one of their users infringed a copyright, the content providers were willing to discuss a compromise. That would eventually lead to the codification of a number of safe harbors and the ratification of the WIPO Copyright Treaty.

III.B.1. The Four Safe Harbors

In the DMCA, Congress provided a series of safe harbors for network service providers. The term "safe harbor" is a nautical metaphor, indicating a place where a ship will be safe from stormy weather. But as in the case of a ship, being outside a safe harbor does not mean that you are in danger. It just means that your safety is not assured. Each DMCA safe harbor substantially limits the liability for copyright infringement. Each is separate, and if you fall within any one, your liability is limited. And even if you don't meet the requirements of one of the safe harbors, that is not an indication that you are infringing a copyright. Other defenses, such as fair use, still remain available.

The four safe harbors provided by Congress, in the following subsections of Section 512,[72] are:

(a) Transitory digital network communications
(b) System caching
(c) Information residing on systems or networks at the direction of users
(d) Information location tools

Each of these safe harbors represent a particular aspect of the normal operation of the Internet that Congress wanted to protect and promote, albeit with some limitations. Each has a set of particular conditions, all of which must be met to enjoy the protection of that safe harbor. You don't get to pick and choose from the different safe harbors to create a new one. Each safe harbor addresses a different aspect of

---

[70] Sen. Rep. No. 105-190 at 8.
[71] 907 F.Supp. 1361, 37 USPQ2d 1545 (N.D. Cal. 1995).
[72] 17 U.S.C. §512.

potential copyright liability, and meeting the conditions of any one is sufficient to receive protection for the acts included in that safe harbor, even if the same act would not meet the requirements of another safe harbor.

Just because a service provider does not qualify for any of the safe harbors does not mean that it might not have a defense to a charge of copyright infringement. Subsection (l) makes it clear that the safe harbors are not intended to list all defenses, nor is conduct outside the safe harbors an indication that the service provider must be infringing.

> The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.[73]

Even though the DMCA became law in 1998, there have been very few court cases that interpret its language. Until there are more cases, the best guidance can be found in the congressional reports that accompanied its passage.

III.B.2. Benefits of Being in the Safe Harbor

Each of the safe harbors begins the same way:

> A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of [the particular act covered by the safe harbor].

The safe harbors don't say that an act by a service provider is not an infringement, like the many exceptions to the exclusive rights of a copyright owner that are detailed starting with Section 107[74] in Chapter 1 of the Copyright Act. Instead, they go to the penalties against a service provider for any infringement. A service provider can still be found to have infringed a copyright, even within the safe harbor. Congress was concerned that it might be difficult to get an injunction against a service provider when that service provider was not an infringer.

Congress felt that it was important for a court to be able to order a service provider to help in stopping an ongoing infringement. But the scope of such an injunction is limited by subsection (j). When a service provider is acting as a "mere conduit" carrying the communications of others, and meets all the conditions of Subsection (a),[75] a court can grant injunctions only in one or both of the following forms:

> (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

[73] 17 U.S.C. §512(l).
[74] 17 U.S.C. §§107-122.
[75] 17 U.S.C. §512(a).

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.[76]

For all the other safe harbors, the following injunctive relief is available:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.[77]

Congress was concerned that injunctions not become burdensome for service providers, and it indicated a number of factors to be considered by a court when deciding whether to grant an injunction and in determining its scope:

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.[78]

Finally, Congress made it clear that injunctions were not to be granted without proper notice to a service provider, so that the service provider can determine the true nature of any alleged infringement and contest the issuance of an injunction, except under very exceptional circumstances.

Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

---

[76] 17 U.S.C. §512(j)(1)(B).
[77] 17 U.S.C. §512(j)(1)(A).
[78] 17 U.S.C. §512(j)(2).

III.B.3. Notice-and-Takedown Procedures

III.B.3.a. Notice

To balance the safe harbor protections given service providers, Congress developed notice-and-takedown procedures, detailed in Subsections 512(c)(3),[79] 512(f),[80] and 512(g).[81] These procedures provide an alternative to a copyright owner going to court to get a temporary order requiring a service provider to remove allegedly-infringing material from that service provider's system.

When an infringing digital work is available on the Internet, time is of the essence in blocking public access to it. If it is not blocked quickly, additional copies can be made at Internet sites all over the world. Even an expedited request for a temporary order blocking the work may take far too long. One thing discussed during the formulation of Section 512 was the idea of a specialized tribunal – "cyber magistrates" – that could quickly determine if material on the Internet was infringing and order its removal. While that could be done by having administrative law judges in the Copyright Office, since the Copyright Office is under the Library of Congress (which is part of the legislative branch), it was felt that it would be too much of a distortion of the Constitution's separation of powers to have a judicial function performed by an administrative agency within the legislature.

Instead, Congress instituted a "voluntary" notice-and-takedown system (perhaps less than voluntary, because a service provider has to participate in it in order to take advantage of all the safe harbors except for "mere conduit") so that allegedly-infringing material is removed quickly, and then any infringement can be adjudicated in a copyright infringement suit.

The notice-and-takedown system starts with a service provider designating an agent to receive notices.

> The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its Web site in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:
>
> (A) the name, address, phone number, and electronic mail address of the agent.
>
> (B) other contact information which the Register of Copyrights may deem appropriate.
>
> The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.[82]

This is done by filing a simple form with the Copyright Office. Once that is done, copyright owners who believe that their works are available on a service provider's system can send a notice to that service provider at the address available in an online

---

[79] 17 U.S.C. §512(c)(3).
[80] 17 U.S.C. §512(f).
[81] 17 U.S.C. §512(g).
[82] 17 U.S.C. §512(c)(2).

database on the Copyright Office's Web site. Not just any allegation of infringement is a proper notice. Congress spelled out particular information that the notice must contain.

> To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:
>
> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
>
> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.[83]

It is important that the copyright owner clearly identify the copyrighted work that is alleged to be infringing, so that the service provider's subscriber can determine whether it is infringing or not, as required in clause (ii). It is equally important that the copyright owner particularly point out where the service provider can find the alleged infringing material. General allegations of infringement are not sufficient, nor does the service provider have to hunt for the material if it has not been properly identified.

Congress specified that the notice has to *substantially* comply with the notice requirements above. Minor errors or omissions do not make the notice defective. The important question is whether the notice is sufficient so that the service provider can locate the information to be taken down without undue effort and without taking down substantially more than is alleged to infringe.

The Fourth Circuit, in *ALS Scan v. RemarQ Communities*,[84] considered the adequacy of a notice that simply indicated that two newsgroups consisting of many different articles infringed ALS Scan's copyrights.

> In this case, ALS Scan provided RemarQ with information that (1) identified two sites created for the sole purpose of publishing ALS

[83] 17 U.S.C. §512(c)(3).
[84] 239 F.3d 619, 57 USPQ2d 1996 (4th Cir. 2001).

> Scan's copyrighted works, (2) asserted that virtually all the images at the two sites were its copyrighted material, and (3) referred RemarQ to two web addresses where RemarQ could find pictures of ALS Scan's models and obtain ALS Scan's copyright information. In addition, it noted that material at the site could be identified as ALS Scan's material because the material included ALS Scan's "name and/or copyright symbol next to it." We believe that with this information, ALS Scan substantially complied with the notification requirement of providing a representative list of infringing material as well as information reasonably sufficient to enable RemarQ to locate the infringing material.[85]

The notice provided by ALS Scan is most likely at the outer limits of meeting the substantial notice requirements, meeting them only because of the particular circumstances of the alleged infringement. The allegedly-infringing material was in two newsgroups – "alt.als" and "alt.binaries.pictures.erotica.als" – whose names themselves indicate that they were related to ALS Scan's works. Had a copyright owner made an allegation of infringing material in a more general newsgroup – say, "misc.int-property" – the substantial identification of the allegedly-infringing works would have to specify the particular postings in the newsgroup.

Also, because ALS Scan indicated that the allegedly-infringing images contained its name and copyright notice and furnished the service provider with a way to confirm that an image was one of ALS Scan's, the Fourth Circuit felt that the spirit of the requirement of clause (ii) to identify a particular work or give a list of representative works was substantially met. That would not be the case, for example, if the allegedly-infringing works, such as MP3 files on a music-sharing system, had not contained a copyright notice.

Clause (v) requires the person giving notice to have "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law" and to state that in the notice. Included within "not authorized by . . . the law" includes uses that are permitted by the various sections of the Copyright Act, including fair use.

Finally, clause (vi) requires that a statement must be included "that the information in the notification is accurate" and "that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed." The second part of the statement must be made "under penalty of perjury."[86]

In addition, Section 512(f) establishes a civil liability when there is any misrepresentation in a notice.

> Any person who knowingly materially misrepresents under this section—
>
> (1) that material or activity is infringing, or
>
> (2) that material or activity was removed or disabled by mistake or misidentification,
>
> shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright

---

[85] 239 F.3d at 625, 57 USPQ2d at 2002.

[86] *See* 18 U.S.C. §1008.

> owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.[87]

The subscriber and the service provider can both sue the content owner making the notice that misrepresents that the material was infringing, and recover not only their damages but also all costs of their suit including their attorneys' fees. Congress made it clear why this provision was included in Section 512:

> This subsection is intended to deter knowingly false allegations to service providers in recognition that such misrepresentations are detrimental to rights holders, service providers, and Internet users.[88]

III.B.3.b. Takedown

Once a service provider wanting to avail itself of the safe harbors of 512(b) (system caching), 512(c) (information residing on systems or networks at the direction of users), or 512(d) (information location tools) knows that its system has infringing material, that service provider must expeditiously remove or block access to the allegedly-infringing material. That knowledge can come from a proper notice from the copyright owner, or when the service provider is aware of facts or circumstances from which infringing activity is apparent. It is not necessary for a service provider to police its users, or guess that something may be an infringement.

Sometimes, a notice from a copyright owner falls short of the requirements for a proper notice. That notice does not give the service provider either actual knowledge of the infringement or awareness of facts or circumstances that suggest infringement.

> A notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.[89]

If that were not the rule, then it could be argued that any notification, no matter how insubstantial, would provide knowledge to the service provider of the alleged infringement and require takedown to remain in the safe harbor, thereby gutting the notice requirements. However, a service provider cannot just ignore a faulty notice.

> In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).[90]

---

[87] 17 U.S.C. §512(f).
[88] Sen. Rep. No. 105-190 at 49.
[89] 17 U.S.C. §512(c)(3)(B)(i).
[90] 17 U.S.C. §512(c)(3)(B)(ii).

III.B.3.c. Put-back

In general, a service provider is not liable to its subscribers because of the removal or access-blocking when it is done in good faith because it has received a proper notice or knows on its own that the material is infringing.

> A service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.[91]

Note that the liability exclusion covers only the "disability of access to, or removal of, material or activity claimed to be infringing." It does not sanction a wholesale removal of a subscriber's material, particularly material that does not infringe, unless that is necessary to disable access to, or remove, the allegedly-infringing material.

For a service provider to benefit from that provision, it is necessary that it "takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material" and respond to a counter notification from the subscriber whose material was taken down by sending the copyright owner who originally filed the notice a copy of the counter notification, informing him that the service provider "will replace the removed material or cease disabling access to it in 10 business days." Then the service provider

> replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.[92]

In other words, the service provider must notify the subscriber of any takedown, and if the subscriber contests the takedown, must restore the material within 14 business days. That provides the copyright owner time to file an infringement suit and get a temporary injunction ordering the continued removal of, or blockage of access to, the alleged infringing material.

> The put back procedures were added as an amendment to this title in order to address the concerns of several members of the Committee that other provisions of this title established strong incentives for service providers to take down material, but insufficient protections for third parties whose material would be taken down.[93]

While the service provider has to make a reasonable effort to notify the user of any material taken down, extraordinary effort is not required.

> The Committee intends that "reasonable steps" include, for example, sending an e-mail notice to an e-mail address associated with a posting, or if only the subscriber's name is identified in the posting, sending an e-mail to an e-mail address that the subscriber submitted with its

---

[91] 17 U.S.C. §512(g)(1).
[92] 17 U.S.C. §512(g)(2)(C).
[93] Sen. Rep. No. 105-190 at 50.

> subscription. The Committee does not intend that this subsection impose any obligation on service providers to search beyond the four corners of a subscriber's posting or their own records for that subscriber in order to obtain contact information. Nor does the Committee intend to create any right on the part of subscribers who submit falsified information in their postings or subscriptions to complain if a service provider relies upon the information submitted by the subscriber.[94]

Similar to the specific requirements for a copyright owner's notice, there are specific requirements for the counter notification:

> To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:
>
> (A) A physical or electronic signature of the subscriber.
>
> (B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.
>
> (C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.
>
> (D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.[95]

Again, Section 512(f) establishes a civil liability when there is any misrepresentation in a notice:

> Any person who knowingly materially misrepresents under this section—
>
> (1) that material or activity is infringing, or
>
> (2) that material or activity was removed or disabled by mistake or misidentification,
>
> shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.[96]

---

[94] Sen. Rep. No. 105-190 at 50.
[95] 17 U.S.C. §512(g)(3).
[96] 17 U.S.C. §512(f).

III.B.3.d. DMCA subpoenas [New]

The treatise does not discuss the special subpoena provisions of the DMCA that a content owner can used to obtain the name and address of a user from an Internet Service Provider. In particular, 17 U.S.C. 512(h) provides that a subpoena could be requested from the clerk of any United States District Court, without the requirement of filing a copyright infringement suit:

> (1) Request. — A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.
> (2) Contents of request — The request may be made by filing with the clerk—
> (A) a copy of a notification described in subsection (c)(3)(A);
> (B) a proposed subpoena; and
> (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

Congress included this provision so that it would not be necessary for a copyright owner to file a "John Doe" lawsuit to obtain the name of a user, which might then have to be dismissed and refiled in the proper venue after the location of the user was determined, thereby lowering litigation costs that might eventually have to be paid by the user. Critics have said that it would allow stalkers to pretend to be a copyright owner in order to get the name and address of a user, because there is no effective review of the subpoena request by the court clerk.

On December 19, 2003, the Court of Appeals for the DC Circuit, in *RIAA v. Verizon*, held that the subpoena provisions were not applicable to service providers acting as "mere conduits," since the notice provision makes no sense in that context.

III.B.4. Mere Conduits for Others' Communications

Subsection (a), the "mere conduit" provision, covers copies that must necessarily be made during digital communications, and covers only intermediate carriers of the communications, not the originators or recipients of the communications. They must not select, alter, or save the material in the communications. They are simply serving as conduits for carrying the communications of others. Congress provided a restricted definition for mere conduit service providers:

> an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[97]

In contrast, service providers for all the other safe harbor provisions include not only the mere conduit service providers, but also providers of "of online services or network access, or the operator of facilities therefore."[98]

As the Senate Judiciary Committee explained, this safe harbor

---

[97] 17 U.S.C. §512(k)(1)(A).
[98] 17 U.S.C. §512(k)(1)(B).

> applies to service providers transmitting, routing, or providing connections for material, and some forms of intermediate and transient storage of material in the course of performing these functions. For example, in the course of moving packets of information across digital online networks, many intermediate and transient copies of the information may be made in routers and servers along the way. Such copies are created as an automatic consequence of the transmission process. In this context, "intermediate and transient" refers to such a copy made and/or stored in the course of a transmission, not a copy made or stored at the points where the transmission is initiated or received.[99]

This safe harbor applies when a service provider is "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections" and when five specific requirements that describe the nature of a mere conduit are met. These requirements make it clear that the service provider is simply carrying material for another and is not exercising any control over the material other than trying to get it to its final destination.

> (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
>
> (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
>
> (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
>
> (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
>
> (5) the material is transmitted through the system or network without modification of its content.[100]

The Senate Judiciary Committee elaborated on these provisions:

> The Committee intends the term "selection of the material" in subsection (a)(2) to reflect an editorial function of determining what material to send, or the specific sources of material to place online (e.g., a radio station), rather than "an automatic technical process" of responding to a command or request, such as one from a user, an Internet location tool, or another network. The term "automatic response to the request of another" is intended to encompass a service provider's actions in responding to requests by a user or other networks, such as requests to forward e-mail traffic or to route

[99] Sen. Rep. No. 105-190 at 41.
[100] 17 U.S.C. §512(a).

> messages to a mailing list agent (such as a Listserv) or other discussion group. The Committee intends subsection (a)(4) to cover copies made of material while it is en route to its destination, such as copies made on a router or mail server, storage of a web page in the course of transmission to a specific user, store and forward functions, and other transient copies that occur en route. The term "ordinarily accessible" is intended to encompass stored material that is routinely accessible to third parties. For example, the fact that an illegal intruder might be able to obtain access to the material would not make it ordinarily accessible to third parties. Neither, for example, would occasional access in the course of maintenance by service provider personnel, nor access by law enforcement officials pursuant to subpoena make the material "ordinarily accessible." However, the term does not include copies made by a service provider for the purpose of making the material available to other users. Such copying is addressed in subsection (b).[101]

Unlike the other safe harbors, this subsection contains no provision for giving notice to the communications provider that leads to the removal of allegedly-infringing material, recognizing the requirement of the safe harbor that any copies not be available "for a longer period than is reasonably necessary for the transmission, routing, or provision of connections."

In addition, any injunction directed at a "mere conduit" service provider is limited by subsection (j) to one or both of the following forms:

> (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
>
> (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.[102]

Again, this represents Congress's understanding that the infringing material passing along the conduit remains only for a limited time and is not generally accessible by others, so the only reasonable relief is the blocking of future transmissions by the actual infringer.

III.B.5. Service Provider Caching

Subsection (b), service provider caching, exempts service providers' making local copies of Web pages so that the pages don't have to be fetched repeatedly over the Internet. Instead the cached copy is sent to their users. Service providers must honor any cache control requests provided by the communications protocol being used so that pages are not cached longer than desired by their creators, must not prevent the returning of information to the page creator about page usage, must honor password or other access controls, and must remove allegedly-infringing material if the material has been removed from its originating site.

---

[101] Sen. Rep. No. 105-190 at 42.
[102] 17 U.S.C. §512(j)(1)(B).

It is important to note that this safe harbor applies only to the caching done by a service provider and not to that done by an end user. Any cached Web pages or pictures on a user's machine would be addressed by fair use, if at all. Section 512 provides safe harbors only to service providers, and then only when the alleged infringing material is not supplied or used by the service provider or its employees.

The safe harbor applies when a service provider is providing "intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider" and:

> (A) the material is made available online by a person other than the service provider;
>
> (B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
>
> (C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.[103]

Again, that is a straightforward description of how a cache operated by a service provider functions. But the caching safe harbor imposes some conditions on the caching system:

> The material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A)[104]

Congress recognized that a true cache holds just a temporary copy of the material so that it can be supplied to a user requesting it without having to fetch a new copy over the network.

> The Committee intends that this restriction apply, for example, so that a service provider who caches material from another site does not change the advertising associated with the cached material on the originating site without authorization from the originating site.[105]

The second requirement under the system caching safe harbor is that

> the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in

[103] 17 U.S.C. §512(b)(1).
[104] 17 U.S.C. §512(b)(2)(A).
[105] Sen. Rep. No. 105-190 at 43.

> paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies[106]

This means that a service provider must comply with any standard cache control protocols, such as those specified in the HyperText Transfer Protocol (HTTP) that handles Web pages. Content providers use these rules to assure that outdated versions of a Web page are not supplied to a user from a cache, or to say that information should not be cached. But a content provider can't use the cache controls in an unreasonable fashion.

The third safe harbor requirement is that:

> the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology—
>
> (i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;
>
> (ii) is consistent with generally accepted industry standard communications protocols; and
>
> (iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person; . . .[107]

This requirement recognizes that some Web pages may contain advertising and the content provider is reimbursed by the advertiser based on the number of "hits" (accesses by users) to the page. If the cache simply returned the page to the user, the only hits that would be recorded would be those that read the page in a service provider's cache. The provision encourages groups that set the standards for the Internet to come up with some way of accurately returning information about the usage of cached information to the content provider.

The Senate Judiciary Committee indicated that this requirement

> provides that the service provider shall not interfere with the ability of certain technology that is associated with the work by the operator of the originating site to return to the originating site information, such as user "hit" counts, that would have been available to the site had it not been cached. The technology must: (i) not significantly interfere with the performance of the storing provider's system or network or with intermediate storage of the material; (ii) be consistent with generally accepted industry standard communications protocols applicable to Internet and online communications, such as those approved by the Internet Engineering Task Force and the World Wide Web Consortium; and (iii) not extract information beyond that which would have been

[106] 17 U.S.C. §512(b)(2)(B).
[107] 17 U.S.C. §512(b)(2)(C).

> obtained had the subsequent users obtained access to the material directly on the originating site.[108]

The fourth requirement for the safe harbor is that the person receiving the cached information must be entitled to receive it directly. A cache should not provide a way of bypassing an access control system for the material.

> If the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions.[109]

Finally, the safe harbor imposes its own notice-and-takedown requirement.

> If the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if–
>
> (i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and
>
> (ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.[110]

Congress recognized that the notice-and-takedown for a cached copy should be tied to the notice-and-takedown of the copy that was cached.

> However, this take down obligation does not apply unless the material has previously been removed from the originating site, or the party submitting the notification has obtained a court order for it to be removed from the originating site and notifies the service provider's designated agent of that order. This proviso has been added to subsection (b)(5) because storage under subsection (b) occurs automatically and unless infringing material has been removed from the originating site, the infringing material would ordinarily simply be re-cached.[111]

III.B.6. Stored User Information

Subsection (c) covers information stored by users on a service provider's system. It codifies the general principles of the *Netcom* decision, giving specific requirements for any notice and what actions must be taken. To remain in this safe harbor, the

---

[108] Sen. Rep. No. 105-190 at 43.
[109] 17 U.S.C. §512(b)(2)(D).
[110] 17 U.S.C. §512(b)(2)(E)
[111] Sen. Rep. No. 105-190 at 43.

service provider must not have actual knowledge of the infringing material before it receives notice, or must not be "aware of facts or circumstances from which infringing activity is apparent." After receiving proper notice, the service provider must act "expeditiously to remove, or disable access to, the material." The service provider cannot "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity." In other words, this safe harbor is available only to service providers that might be contributory infringers but are not vicarious infringers.

The Senate Judiciary Committee explained the nature of this safe harbor:

> Subsection (c) limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider. Examples of such storage include providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users.[112]

The safe harbor is available to a service provider who provides "storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider" and meets the following conditions:

> (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; . . .[113]

In addition, the notice-and-takedown requirements must be followed by the service provider, so that material alleged to infringe will be removed promptly and before it becomes too widespread.

Congress was particularly concerned with the knowledge standard that should apply to a service provider in the safe harbor. On one hand, it did not want to require that service providers police their users, looking for copyright infringements. On the other hand, it did not want service providers to turn a blind eye to obvious infringements. It described the knowledge requirement above as

> met either by actual knowledge of infringement or in the absence of such knowledge by awareness of facts or circumstances from which infringing activity is apparent. The term "activity" is intended to mean activity using the material on the system or network. The Committee intends such activity to refer to wrongful activity that is occurring at the site on the provider's system or network at which the material resides, regardless of whether copyright infringement is technically deemed to occur at that site or at the location where the material is received. For

---

[112] Sen. Rep. No. 105-190 at 43.
[113] 17 U.S.C. §512(c)(1).

example, the activity at an online site offering audio or video may be unauthorized public performance of a musical composition, a sound recording, or an audio-visual work, rather than (or in addition to) the creation of an unauthorized copy of any of these works.

Subsection (c)(1)(A)(ii) can best be described as a "red flag" test. As stated in subsection (l), a service provider need not monitor its service or affirmatively seek facts indicating infringing activity (except to the extent consistent with a standard technical measure complying with subsection (h)), in order to claim this limitation on liability (or, indeed any other limitation provided by the legislation). However, if the service provider becomes aware of a "red flag" from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag," the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a "red flag"--in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances--an objective standard should be used.

Subsection (c)(1)(A)(iii) provides that once a service provider obtains actual knowledge or awareness of facts or circumstances from which infringing material or activity on the service provider's system or network is apparent, the service provider does not lose the limitation of liability set forth in subsection (c) if it acts expeditiously to remove or disable access to the infringing material. Because the factual circumstances and technical parameters may vary from case to case, it is not possible to identify a uniform time limit for expeditious action.

Subsection (c)(1)(B) sets forth the circumstances under which a service provider would lose the protection of subsection (c) by virtue of its benefit from and control over infringing activity. In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate business would not be considered to receive a "financial benefit directly attributable to the infringing activity" where the infringer makes the same kind of payment as non-infringing users of the provider's service. Thus, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving a "financial benefit directly attributable to the infringing activity." Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.[114]

[114] Sen. Rep. No. 105-190 at 44-45.

III.B.7. Directories and Links

Subsection (d) covers directories and other ways of locating information on the World Wide Web. This safe harbor is not available to vicarious infringers. And you can't remain in the safe harbor if you link to information that you know or reasonably suspect is infringing. If a court has told you to remove information from your Web site because it likely infringes somebody's copyright, you can't replace it with a pointer to the information stored on another Web site and expect to remain in this safe harbor.

Congress noted the importance to the operation of the Internet of information locating tools:

> Information location tools are essential to the operation of the Internet; without them, users would not be able to find the information they need. Directories are particularly helpful in conducting effective searches by filtering out irrelevant and offensive material. The Yahoo! directory, for example, currently categorizes over 800,000 online locations and serves as a "card catalogue" to the World Wide Web, which over 35,000,000 different users visit each month. Directories such as Yahoo!'s usually are created by people visiting sites to categorize them. It is precisely the human judgment and editorial discretion exercised by these cataloguers which makes directories valuable.
>
> This provision is intended to promote the development of information location tools generally, and Internet directories such as Yahoo!'s in particular, by establishing a safe-harbor from copyright infringement liability for information location tool providers if they comply with the notice and takedown procedures and other requirements of subsection (d). The knowledge or awareness standard should not be applied in a manner which would create a disincentive to the development of directories which involve human intervention. Absent actual knowledge, awareness of infringement as provided in subsection (d) should typically be imputed to a directory provider only with respect to pirate sites or in similarly obvious and conspicuous circumstances, and not simply because the provider viewed an infringing site during the course of assembling the directory.[115]

The requirements for the safe harbor are met if the service provider:

> (1)(A) does not have actual knowledge that the material or activity is infringing;
>
> (B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the

[115] Sen. Rep. No. 105-190 at 49.

material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.[116]

The Senate Judiciary Committee discussed these requirements:

> Subsection (d) applies to referring or linking users to an online location containing infringing material or infringing activity using information location tools. The reference to "infringing activity" is intended to refer to wrongful activity that is occurring at the location to which the link or reference refers, without regard to whether copyright infringement is technically deemed to occur at that location or at the location where the material is received. The term information location tools includes, for example: a directory or index of online sites or material such as a search engine that identifies pages by specified criteria, a reference to other online material such as a list of recommended sites, a pointer that stands for an Internet location or address, or a hypertext link which allows users to access material without entering its address.
>
> Subsection (d) incorporates the notification and take down structure of subsection (c) and applies it to the provision of references and links to infringing sites. A service provider is entitled to the liability limitations of subsection (d) if it: (1) lacks actual knowledge of infringement on the other site, and is not aware of facts or circumstances from which infringing activity in that location is apparent; (2) does not receive a financial benefit directly attributable to the infringing activity on the site, where the service provider has the right and ability to control the infringing activity; and (3) responds expeditiously to remove or disable the reference or link upon receiving a notification of claimed infringement as described in subsection (c)(3). The notification procedures under subsection (d) follow those set forth in subsection (c). However, the information submitted by the complaining party under subsection (c)(3)(A)(iii) is identification of the reference or link to infringing material or activity, and information reasonably sufficient to permit the service provider to locate that reference or link.
>
> Section 512(d) provides a safe harbor that would limit the liability of a service provider that refers or links users to an online location containing infringing material or activity by using "information location tools," such as hyperlink directories and indexes. A question has been raised as to whether a service provider would be disqualified from the safe harbor based solely on evidence that it had viewed the infringing Internet site. If so, there is concern that online directories prepared by human editors and reviewers, who view and classify various Internet sites, would be denied eligibility to the information location tools safe

[116] 17 U.S.C. §512(d).

harbor, in an unintended number of cases and circumstances. This is an important concern because such online directories play a valuable role in assisting Internet users to identify and locate the information they seek on the decentralized and dynamic networks of the Internet.

Like the information storage safe harbor in section 512(c), a service provider would qualify for this safe harbor if, among other requirements, it "does not have actual knowledge that the material or activity is infringing" or, in the absence of such actual knowledge, it is "not aware of facts or circumstances from which infringing activity is apparent." Under this standard, a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to "red flags" of obvious infringement.

For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a "pirate" site of the type described below, where sound recordings, software, movies or books ere available for unauthorized downloading, public performance or public display. Absent such "red flags" or actual knowledge, a directory provider would not be similarly aware merely because it saw one or more well known photographs of a celebrity at a site devoted to that person. The provider could not be expected, during the course of its brief cataloguing visit, to determine whether the photograph was still protected by copyright or was in the public domain; if the photograph was still protected by copyright, whether the use was licensed; and if the use was not licensed, whether it was permitted under the fair use doctrine.

The important intended objective of this standard is to exclude sophisticated "pirate" directories – which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted--from the safe harbor. Such pirate directories refer Internet users to sites that are obviously infringing because they typically use words such as "pirate," "bootleg," or slang terms in their uniform resource locator (URL) and header information to make their illegal purpose obvious to the pirate directories and other Internet users. Because the infringing nature of such sites would be apparent from even a brief and casual viewing, safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate. Pirate directories do not follow the routine business practices of legitimate service providers preparing directories, and thus evidence that they have viewed the infringing site may be all that is available for copyright owners to rebut their claim to a safe harbor.

In this way, the "red flag" test in section 512(d) strikes the right balance. The common-sense result of this "red flag" test is that on-line editors and catalogers would not be required to make discriminating judgments about potential copyright infringement. If, however, an Internet site is obviously pirate, then seeing it may be all that is needed for the service provider to encounter a "red flag." A provider proceeding

in the face of such a red flag must do so without the benefit of a safe harbor.[117]

III.B.8. Other Safe Harbor Requirements

In addition to the specific requirements of each safe harbor, there are some general requirements that a service provider must meet to qualify for any of the safe harbors. These are detailed in subsection (i).

First, a service provider must have

> adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers.[118]

As explained by the Senate Judiciary Committee:

> First, the service provider is expected to adopt and reasonably implement a policy for the termination in appropriate circumstances of the accounts of subscribers of the provider's service who are repeat online infringers of copyright. The Committee recognizes that there are different degrees of online copyright infringement, from the inadvertent to the noncommercial, to the willful and commercial. In addition, the Committee does not intend this provision to undermine the principles of [the protection of privacy of subsection (m)] or the knowledge standard of [notice-and-takedown] subsection (c) by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing. However, those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access.[119]
>
> By "subscribers," the Committee intends to include account holders who are parties with a business relationship to the service provider that justifies treating them as subscribers, for the purposes of section 512, even if no formal subscription agreement exists. Examples include students who are granted access to a university's system or network for digital online communications; employees who have access to their employer's system or network; or household members with access to a consumer online service by virtue of a subscription agreement between the service provider and another member of that household.[120]

The privacy requirements of Subsection (m) are as follows:

> Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—
>
> (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a

---

[117] Sen. Rep. No. 105-190 at 47-49.
[118] 17 U.S.C. §512(i)(1)(A).
[119] Sen. Rep. No. 105-190 at 52.
[120] Sen. Rep. No. 105-190 at 52 n. 24.

> standard technical measure complying with the provisions of subsection (i); or
>
> (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.[121]

The second requirement is that the service provider "accommodates and does not interfere with standard technical measures."[122] A standard technical measure

> means technical measures that are used by copyright owners to identify or protect copyrighted works and—
>
> (A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;
>
> (B) are available to any person on reasonable and nondiscriminatory terms; and
>
> (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

Congress was aware of the efforts toward the development of effective access control and rights management systems, and supported them legislatively in another portion of the DMCA. It would seem paradoxical to support technological measures for copyright infringement control in one section of the law while allowing service providers who interfere with the same technological measures to benefit from the safe harbor provisions.

> The Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age. For that reason, we have included [the subsection], which is intended to encourage appropriate technological solutions to protect copyrighted works. The Committee strongly urges all of the affected parties expeditiously to commence voluntary, interindustry discussions to agree upon and implement the best technological solutions available to achieve these goals.
>
> [The subsection] is explicitly limited to "standard technical measures" that have been developed pursuant to a broad consensus of both copyright owners and service providers in an open, fair, voluntary, multi-industry standards process. The Committee anticipates that these provisions could be developed both in recognized open standards bodies or in ad hoc groups, as long as the process used is open, fair, voluntary, and multi-industry and the measures developed otherwise conform to the requirements of the definition of standard technical measures. A number of recognized open standards bodies have substantial experience with Internet issues.[123]

---

[121] 17 U.S.C. §512(m).
[122] 17 U.S.C. §512(i)(1)(B).
[123] Sen. Rep. No. 105-190 at 52.

III.B.9. Special Rules for Schools

Subsection (e) provides special protection for schools if their faculty or student employees are infringing, by not attributing that infringement to the school in many instances.

> When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if—
>
> (A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;
>
> (B) the institution has not, within the preceding 3-year period, received more than 2 notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and
>
> (C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.
>
> (2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.[124]

This provision was not part of the DMCA as passed by either the House or the Senate but was added by the conference committee as it was considering the final form of the bill.

> However, the conferees recognize that the university environment is unique. Ordinarily, a service provider may fail to qualify for the liability limitations in Title II simply because the knowledge or actions of one of its employees may be imputed to it under basic principles of respondeat superior and agency law. The special relationship which exists between universities and their faculty members (and their graduate student employees) when they are engaged in teaching or research is different from the ordinary employer-employee relationship. Since independence—freedom of thought, word and action—is at the core of academic freedom, the actions of university faculty and graduate student teachers and researchers warrant special consideration in the context of this legislation. This special consideration is embodied in new subsection (e), which provides special rules for determining whether universities, in their capacity as a service provider, may or may not be

[124] 17 U.S.C. §512(e).

liable for acts of copyright infringement by faculty members or graduate students in certain circumstances.

Subsection (e)(1) provides that the online infringing actions of faculty members or graduate student employees, which occur when they are "performing a teaching or research function," will not be attributed to an institution of higher education in its capacity as their employer for purposes of section 512, if certain conditions are met. For the purposes of subsections (a) and (b) of section 512, such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) of section 512 the faculty member's or graduate student's knowledge or awareness of his or her infringing activities will not be attributed to the institution, when they are performing a teaching or research function and the conditions in paragraphs (A) (C) are met.

When the faculty member or the graduate student employee is performing a function other than teaching or research, this subsection provides no protection against liability for the institution if infringement occurs. For example, a faculty member or graduate student is performing a function other than teaching or research when the faculty member or graduate student is exercising institutional administrative responsibilities, or is carrying out operational responsibilities that relate to the institution's function as a service provider. Further, for the exemption to apply on the basis of research activity, the research must be a genuine academic exercise—i.e. a legitimate scholarly or scientific investigation or inquiry—rather than an activity which is claimed to be research but is undertaken as a pretext for engaging in infringing activity.

In addition to the "teaching or research function" test, the additional liability protections contained in subsection (e)(1) do not apply unless the conditions in paragraphs (A) through (C) are satisfied. First, paragraph (A) requires that the infringing activities must not involve providing online access to instructional materials that are "required or recommended" for a course taught by the infringing faculty member and/or the infringing graduate student within the last three years. The reference to "providing online access" to instructional materials includes the use of e-mail for that purpose. The phrase "required or recommended" is intended to refer to instructional materials that have been formally and specifically identified in a list of course materials that is provided to all students enrolled in the course for credit; it is not intended, however, to refer to the other materials which, from time to time, the faculty member or graduate student may incidentally and informally bring to the attention of students for their consideration during the course of instruction.

Second, under paragraph (B) the institution must not have received more than two notifications of claimed infringement with respect to the particular faculty member or particular graduate student within the last three years. If more than two such notifications have been received, the institution may be considered to be on notice of a pattern of infringing conduct by the faculty member or graduate student, and the

limitation of subsection (e) does not apply with respect to the subsequent infringing actions of that faculty member or that graduate student. Where more than two notifications have previously been received with regard to a particular faculty member or graduate student, the institution will only become potentially liable for the infringing actions of that faculty member or that graduate student. Any notification of infringement that gives rise to a cause of action for misrepresentation under subsection (f) does not count for purposes of paragraph (B).

Third, paragraph (C) states that the institution must provide to the users of its system or network – whether they are administrative employees, faculty, or students – materials that accurately describe and promote compliance with copyright law. The legislation allows, but does not require, the institutions to use relevant informational materials published by the U.S. Copyright Office in satisfying the condition imposed by paragraph (C).[125]

IV. Protection Through Technology

IV.A. Why Technology, Why Laws?

Since it is impossible to sue every copyright infringer because of the cost of such suits (and the resentment and backlash they can generate), the dream of entertainment content owners is for the device that can stop any possible infringement using a technology-based access or copy control mechanism. This would also avoid messy questions like whether a copy would be permitted as a fair use or not since, if such a technology-based mechanism could work properly, anything permitted by the copy control mechanism would be permissible, and anything not permissible would be blocked by the copy control mechanism.

Such a device will always remain a dream because permissible copying under fair use can't possibly be determined by a machine, no matter how sophisticated. The Supreme Court, in *Harper & Row v. Nation Enterprises*,[126] found that the copying of approximately 300 words from a full-length book was not a fair use; the Ninth Circuit, in *Sega v. Accolade*,[127] found that the copying of an entire computer program was. The seeming inconsistency between these two decisions stems from how the copy was eventually used, something that cannot be determined by a mechanism that allows or disallows copying or access.

But copy and access controls can successfully stop some illegal copying and make other copying appear just shady enough so that most people will avoid doing it. In the absence of clear rules in the copyright laws as to what is permissible and what is not for digital works, whether copying can be done easily with standard hardware and software will seem to many as reasonable guidance. Though the perfect technology-based protection mechanism would be able to protect any work without the need for copyright or other laws, the addition of a limited law to keep people from

---

[125] H.R. Rep. No. 105-796 at 74-75.
[126] 471U.S. 539, 225 USPQ 1073 (1985).
[127] 977 F.2d 1510, 24 USPQ2d 1561 (9th Cir. 1992).

distributing devices that circumvent the protection means that the protection mechanism can be simpler, less expensive, and less intrusive.

IV.B. Past Technological Protections

IV.C. The White Paper

IV.D. The WIPO Copyright Treaty

IV.E. Technological Protections and the DMCA

After the adoption of the WIPO Copyright Treaty, the focus again shifted to having Congress pass legislation to protect copy control and rights management systems. But this time, it was under the banner of having to ratify and implement the WIPO Copyright Treaty, to provide an example to the other countries in the world.

The Internet service providers were also in a better position, because the content providers really wanted the WIPO Copyright Treaty. While the Clinton Administration and the content providers proposed anticircumvention and rights management provisions without exceptions for conduct that should not be violations, Congress added a number of specific exceptions to the DMCA addressing important aspects of the Internet. The result was the safe harbor limitations to copyright infringement suits against service providers, codified in Section 512.[140]

The anticircumvention and rights management provisions are an attempt to support in law reasonable techniques for protecting a copyrighted work. They outlaw the use and distribution of tools that can get around such protection techniques. It is not necessary for the technique to be invulnerable to all attacks, because the vast majority of people will not have easy access to the tools that could circumvent the protection.

These provisions are related to, but separate from, copyright. Even the name for the improper act is different – you "infringe" a copyright, but you "violate" the anticircumvention or rights management provisions. Therefore, if you circumvent a protection system, you violate the anticircumvention provisions even if your eventual use of the copyrighted work is not an infringement because it is a fair use or falls within another exception.

The penalties for circumventing a protection measure are much like copyright infringement: civil actions yielding injunctions and monetary damages (either actual or statutory) and criminal penalties with fines up to $1,000,000 and imprisonment of up to ten years for repeat offenses. But while that seems draconian, in reality the federal sentencing guidelines limit the penalties, with the maximum only for the most egregious violations causing millions of dollars in damages.

While the DMCA was being considered by Congress, beginning in 1997 and ending with it becoming law in October 1998, many opponents predicted that it would have dire consequences. But in the over-three-years since its enactment, there have been only a few cases brought under it, and most of those in instances of high-profile anticircumvention activities. While future cases will give a clearer interpretation of the DMCA's provisions, right now the best guidance to understanding them comes from the congressional reports that accompanied the DMCA's passage.

---

[140] 17 U.S.C. §512.

IV.E.1. The Trafficking Provisions

Perhaps the most important of the anticircumvention provisions in terms of their actual effect are those outlawing trafficking in circumvention technology. While not required by the WIPO Copyright Treaty, which addresses only actual circumventions, these provisions may be more effective at stopping most unlawful circumventions by limiting the tools available to people than suing a large number of circumventors.

Section 1201(a)(2) deals with trafficking in things that circumvent any "technological measure that effectively controls access to a work" protected by copyright.

> 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.[141]

There are a number of terms with special meanings:

> (A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and
>
> (B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.[142]

Subsection (b) provides prohibition similar to that of Section 1201(a)(2), except for circumvention of a measure that "effectively protects a right of a copyright owner," rather than "effectively controls access to a work."

> 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 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

[141] 17 U.S.C. §1201(a)(2).
[142] 17 U.S.C. §1201(a)(3).

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.[143]

And again, similar definitions for the special terms:

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) 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.[144]

The technological measure does not need to be flawless in its protection in order to be protected. Instead, the provisions are intended to protect mechanisms that are simple, like the Audio Home Recording Act's Serial Copy Management System, which uses only two bits of control information (one to indicate it is a work to be protected, the other indicating that it is an original copy) but is effective since there are no legal digital audio recording devices that don't honor the system.

The practical, common-sense approach taken by H.R. 2281 is that if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work, or to control copying, distribution, public performance, or the exercise of other exclusive rights in a work, then the "effectiveness" test is met, and the prohibitions of the statute are applicable. This test, which focuses on the function performed by the technology, provides a sufficient basis for clear interpretation. It applies equally to technologies used to protect access to works whether in analog or digital formats.[145]

Congress indicated that even a simple password control could be an effective technological measure.

For example, if unauthorized access to a copyrighted work is effectively prevented through use of a password, it would be a violation of this section to defeat or bypass the password and to make the means to do so, as long as the primary purpose of the means was to perform this kind of act.[146]

In fact, there is no need to protect a technological measure that is so good that it cannot be circumvented. Instead, you want to use the law to allow technological measures that are simple and inexpensive. As an analogy, imagine what your home doors would look like if there were no laws against burglary and you had to use only technology to protect your new, big-screen television. Instead, because there is a law

---

[143] 17 U.S.C. §1201(b)(1).
[144] 17 U.S.C. §1201(b)(2).
[145] H.R. Judiciary Comm. Print 105-6 at 10.
[146] Sen. Rep. No. 105-190 at 11.

against "circumventing" a locked door, most people get by with an inexpensive lock, even though an expert could open it with little difficulty.

Not requiring perfect access controls also eliminates a problem that could hurt the adoption of new technologies such as DVDs. Assume that the original DVDs used a protection mechanism that was uncrackable at the time they were introduced. Then, at some later time, a way to crack the protection mechanism is discovered. If there is no law against trafficking in the circumvention method, the only way for content producers to continue to protect their works is to go to a new protection mechanism for the works sold in the future. But that means that people who bought original DVD players will not be able to play the new works, since they are protected with a different mechanism. They would have to purchase a new player (or pay for an upgrade to their existing player) to play the new works. Although this continual obsolescence might seem wonderful for DVD player manufacturers, it is more likely that people would simply not buy a DVD player if they thought that it would play only past releases and not new movies.

Just because somebody constructs or distributes something that could circumvent a protection method does not mean that he or she has violated the trafficking provisions. The "technology, product, service, device, component, or part thereof" must fall into one of three categories before there is a violation.

> (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.[147]

This mean that, for example, a disk block editor that can change any bits stored on a hard disk would not normally be a circumvention device because it was written to help with disk administration and repair and not primarily for circumvention. But if somebody starts selling the disk block editor by saying how it can be used to circumvent a protection mechanism, that would run afoul of (C).

The "primarily designed or produced" and "only limited commercially significant purpose or use" tests are different from the "substantial noninfringing use" that the Supreme Court stated in its 1984 *Sony v. Universal City Studios* decision.[148]

In that case, because there were no statutory contributory or vicarious infringement provisions in the Copyright Act, the Supreme Court imported the ones from the patent statute.

> If vicarious liability is to be imposed on petitioners in this case, it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make authorized copies of copyrighted material. There is no precedent in the law of the copyright for the imposition of vicarious liability on

[147] 17 U.S.C. §1201(a)(2).
[148] 464U.S. 417, 220 USPQ 665 (1984).

> such a theory. The closest analogy is provided by the patent law cases to which it is appropriate to refer because of the historic kinship between patent law and copyright law.[149]

The patent act specifically recognizes inducement of infringement[150] and contributory infringement.[151] For contributory infringement, all that is necessary is the selling of a component of the patented invention that is "not a staple article or commodity of commerce suitable for substantial noninfringing use." This would include, for example, the standard electronic parts that might be used to construct a patented device.

> We recognize there are substantial differences between the patent and copyright laws. But in both areas the contributory infringement doctrine is grounded on the recognition that adequate protection of a monopoly may require the courts to look beyond actual duplication of a device or publication to the products or activities that make such duplication possible. The staple article of commerce doctrine must strike a balance between a copyright holder's legitimate demand for effective – not merely symbolic – protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.[152]

The problem with using this standard for the trafficking provisions is that there is almost always a substantial noninfringing use because fair use generally permits the quotation of limited portions of a copyrighted work in a new work. Patent law does not have a comparable fair use provision, so its criteria for contributory infringement don't have the loophole that exists when the same criteria is applied to copyrighted works.

Instead, Congress explicitly stated the criteria to be considered when deciding whether a person is trafficking in a circumvention device or is promoting a legitimate product, so it is not necessary to import tests from the patent laws that may be questionable for determining whether something that can be used to circumvent a protection measure has other uses that should allow its distribution.

IV.E.2. Accessing Through Circumvention

Unlike Section 1201(b),[153] which forbids trafficking in devices used to infringe one of the copyright owner's exclusive rights, Section 1201(a)(2)[154] is directed at trafficking in devices used to access a work protected by a technological measure. But since there was no prohibition against such access, and it would be strange to prohibit the distribution of a device that doesn't perform an illegal activity, Congress created a new violation as Section 1201(a)(1):

---

[149] 464 U.S. at 439, 220 USPQ at 677.
[150] 35 U.S.C. §271(b).
[151] 35 U.S.C. §271(c).
[152] 464 U.S. at 442, 220 USPQ at 678.
[153] 17 U.S.C. §1201(b).
[154] 17 U.S.C. §1201(a)(2).

> No person shall circumvent a technological measure that effectively controls access to a work protected under this title.[155]

Until then, it had not been illegal to access a copyrighted work as long as there was not an infringement associated with that access. One could access the information in a book by reading it without infringing the copyright on that book.

The prohibition against trafficking in a device to circumvent an access control seemed to Congress necessary to prevent a huge loophole in the anticircumvention provisions that would allow the distribution of circumvention devices that contained a warning against using them for copyright infringement, even though that would be the likely result. Any effectiveness of the anticircumvention provisions comes from preventing circumvention devices or programs from being readily available to non-technical people in a way that seems to legitimize them, not from stopping every circumvention device.

The creation of what is essentially a new right of copyright owners to control access to technology-protected works is not completely divorced from existing copyright law. Digital works are different from traditional copyrighted works in that intermediate copies are often required to see or hear the work. If a work is encrypted as part of a technological protection mechanism, then it is likely that an intermediate plain-text copy of the protected work will be created. And that intermediate copy stored in the memory of the computer used to access the work infringes the reproduction right[156] if it is without the authorization of the copyright owner and not permitted by law.

But Congress was also concerned that people might take advantage of the inability to access material that is protected by a technological measure to improperly protect material. For example, a content provider might add a small copyrighted portion to a work in the public domain, such as a capsule description to a court decision, and protect the whole thing with an access control system. Any access would be a violation of Section 1201[a][1](A),[157] and would also be technologically impossible for most people because the trafficking provision of Section 1201(a)(2)[158] means that there would be no ready source of tools to get around such a technological measure.

Congress addressed this in two ways. First, it provided a number of exceptions to the provisions against access and trafficking to address particular circumstances where it felt that the public good would be served. Second, it provided for a procedure, detailed in Section 1201(a), by which the Librarian of Congress could exempt certain classes of works from the circumvention ban.

> Given the threat of a diminution of otherwise lawful access to works and information, the Committee on Commerce believes that a "fail-safe" mechanism is required. This mechanism would monitor developments in the marketplace for copyrighted materials, and allow the enforceability of the prohibition against the act of circumvention to be selectively waived, for limited time periods, if necessary to prevent a

---

[155] 17 U.S.C. §1201(a)(1)(A).
[156] See *MAI v. Peak*, 991 F.2d 511, 26 USPQ2d 1458 (9th Cir. 1993).
[157] 17 U.S.C. §1201(a)(1)(A).
[158] 17 U.S.C. §1201(a)(2).

> diminution in the availability to individual users of a particular category of copyrighted materials.[159]

The factors to be considered by the Register of Copyrights, who makes a recommendation to the Librarian of Congress after consultation with the Assistant Secretary for Communications and Information of the Department of Commerce, are

> (i) the availability for use of copyrighted works;
>
> (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
>
> (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
>
> (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and
>
> (v) such other factors as the Librarian considers appropriate.[160]

Classes of works are exempted by the Librarian of Congress for a three-year period, and there is a new review every three years. The ban on using circumvention devices (but not their distribution) was delayed for two years (until October 28, 2000), to allow for the first review.

During the first review, the Librarian of Congress received comments from the public and determined that two classes of works should be exempted from the prohibition against the use of circumvention devices:

> 1. Compilations consisting of lists of websites blocked by filtering software applications; and
>
> 2. Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence.[161]

During the second rulemaking cycle, these two exemptions were refined and two new exemptions were added:

> (1) Compilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of email.
>
> (2) Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete.
>
> (3) Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in

---

[159] H.R. Rep. No. 105-551 part 2 at 36.
[160] 17 U.S.C. §1201(a)(1)(C).
[161] Recommendation of the Register of Copyrights and Determination of the Librarian of Congress, 65 Fed. Reg. 64555 (October 27, 2000).

that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.

(4) Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format.

Three definitions were also added:

(1) “Internet locations” are defined to include domains, uniform resource locators (URLs), numeric IP addresses or any combination thereof.

(2) “Obsolete” shall mean “no longer manufactured or reasonably available in the commercial marketplace.”

(3) “Specialized format,” “digital text” and “authorized entities” shall have the same meaning as in 17 U.S.C. §121.

During the third rulemaking cycle, which concluding in November 2006, one of the previous exemptions remained essentially unchanged, two had limiting language added, and one was dropped. Although the exemption for compilations of blocked Internet locations was one of the original two exemptions and continued in a more restricted form in the second round, the proponents of the exemption made no factual showing in the third round that the exemption was still necessary nor that the exemption had been used.

The fourth exemption remains essentially the same.

4. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format.

What had previously been the second exemption is now the third, with a definition of when a dongle becomes obsolete added.

3. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.

What had previously been the third exemption is now the third, but is now limited to preservation and archival activities only.

2. Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.

Finally, three new exemptions were added.

> 1. Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.
>
> 5. Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.
>
> 6. Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

In the past, the Copyright Office has restricted the exemptions to particular classes of works, rather than particular uses, as it felt the statute required. This time, both exemptions 1 and 2 further restrict a class of works to a particular use. And it must be remembered that the exemptions are only for the circumvention of an access control mechanism covered by section 1201(a)(1). It does not provide an exemption for the provision of a tool used for such circumvention, which could be a violation of section 1201(a)(2), nor for circumvention that results in infringement, which would be a violation of section 1201(b).

For more information about these exemptions, and the proceedings leading up to them, see: http://www.copyright.gov/1201/

IV.E.3. Distinction From Copyright

It is important to understand that although the anticircumvention and rights management provisions of the DMCA are closely related to copyright, in that they apply to works protected by copyright, but they are separate from copyright law (except for being codified in the same title of the United States Code). Even the words used to characterize the unlawful acts are different – you "infringe" a copyright, but "violate" the anticircumvention or rights management provisions.

Congress made it clear that it didn't intend these provisions, and the case law that develops from them, to affect the copyright statutes and their case law.

> (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.
>
> (2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.[162]

IV.E.4. Fair Use

At the time the anticircumvention provisions were being debated, there was concern that they would negate fair use of a copyrighted work, because if you cannot

[162] 17 U.S.C. §1201(c).

access the underlying copyrighted work without violating the anticircumvention provisions, you can't make a fair use of the work. But if you allow circumvention when the use is fair, there is no way to block the distribution of circumvention devices, since everybody selling them would say that they are to be used only for noninfringing activities (and wink when they say it).

The anticircumvention provision does not negate fair use of material that is protected by an access control mechanism. While it may stop a creator of a new work from copying from the protected work with a couple of clicks of a mouse, it can't stop that creator from retyping the passage. The Second Circuit, in *Universal City Studios v. Corley*,[163] stated:

> 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, 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.[164]

In *United States. v. Elcom*,[165] a recent district court decision regarding the criminal liability of a Russian company that was distributing a program for circumventing the protection mechanism for Adobe electronic books, the trial judge (who had also written the decision in the landmark *Netcom* case[166] as well as a

---

[163] 273 F.3d 429, 60 USPQ2d 1953 (2d Cir. 2001).
[164] 273 F.3d at 459, 60 USPQ2d at 1973-1974.
[165] 203 F.Supp.2d 1111, 62 USPQ2d 1736 (N.D. Cal. 2002).
[166] 907 F.Supp. 1361, 37 USPQ2d 1545 (N.D. Cal. 1995).

number of other computer-technology-related cases) reached the same conclusion as the Second Circuit: that the DMCA does not eliminate fair use, although it might make it less convenient. He also upheld the DMCA against a number of constitutional and other challenges.

Any restrictions imposed by technological measures supported by the DMCA are unlikely to prevent the creation of works for "criticism, comment, news reporting, teaching, scholarship, or research"[167] that are transformative rather than simply copies, held to be a touchstone for fair use by the Supreme Court in *Campbell v. Acuff-Rose Music*.[168] The creation of a transformative work that is truly a fair use is not an infringement of copyright, and therefore does not run afoul of Section 1201(b)[169] even if a protection mechanism is circumvented. And, since "to invoke the fair use exception, an individual must possess an authorized copy of a literary work,"[170] the creator of the transformative work can simply look at that copy while creating his transformative work, which should not require circumvention in violation of Section 1201(a)(1).[171]

IV.E.5. What Anticircumvention Isn't

Congress also added two other subsections saying what the anticircumvention provisions were not, just for good measure.

> (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).
>
> (4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.[172]

Paragraph (3) is particularly important, since it makes it clear that there is no design mandate in the anticircumvention provisions except not to produce a circumvention device. The mere fact that a technological measure has been developed does not require manufacturers of existing equipment or developers of new equipment to include that technological measure in their product, as long as they avoid acts that would be considered trafficking in a circumvention device.

Some content providers, unhappy with the compromises made in the DMCA, are now supporting legislation that would mandate a protection mechanism for every digital device that can reproduce copyrighted works (which is just about every device that contains a microprocessor that can load a program or data into its memory).[173] It

---

[167] See 17 U.S.C. §107.
[168] 510U.S. 569, 29 USPQ2d 1961 (1994).
[169] 17 U.S.C. §1201(b).
[170] *Atari v. Nintendo*, 975 F.2d 832, 843, 24 USPQ2d 1015, 1024 (Fed. Cir. 1992).
[171] 17 U.S.C. §1201(a)(1).
[172] 17 U.S.C. §1201(c).
[173] See, for example, the Consumer Broadband and Digital Television Promotion Act, S. 2048, introduced in the 107th Congress.

is unlikely that such a protection mechanism would be any more effective than the anticircumvention provisions of the DMCA as long as there were still computers that did not have the mandated protection mechanism. And it is economically unfeasible to replace each of the hundreds of millions of personal computers in the world.

Paragraph (4) is just window dressing, since Congress can't pass a law that diminishes the rights of free speech or a free press and have it upheld in court, much as it sometimes may want to.

IV.E.6. Rights Management Information

The second aspect of the WIPO Copyright Treaty addressed in the DMCA is the protection of rights management information. The corresponding provision in the DMCA is codified as Section 1202:

> No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement:
>
> (1) provide copyright management information that is false, or
>
> (2) distribute or import for distribution copyright management information that is false.
>
> (b) Removal or Alteration of Copyright Management Information.– No person shall, without the authority of the copyright owner or the law:
>
> (1) intentionally remove or alter any copyright management information,
>
> (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or
>
> (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law, knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.[174]

It defines "copyright management information" as

> any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:
>
> (1) The title and other information identifying the work, including the information set forth on a notice of copyright.
>
> (2) The name of, and other identifying information about, the author of a work.

[174] 17 U.S.C. §1202(a).

(3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.

(4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.

(5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.

(6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.[175]

At the present time, there are few, if any, rights management systems. Perhaps the most interesting use for rights management information today is as a trigger for an access control mechanism, such that the copyright owner can specify the types of accesses that are to be allowed or blocked. As such, rights management is closely related to access control.

IV.E.7. Permitted Circumventions

A number of specific exceptions to the anticircumvention provisions are given in Subsections (d) through (j), including exceptions for libraries and educational institutions, law enforcement, reverse engineering, encryption research, and security testing. As with the DMCA safe harbor provisions, these are very specific exceptions and to fall within that exception, a work must meet all of its requirements.

IV.E.7.a. Law Enforcement, Content Filters, and Privacy

When the Administration first proposed the anticircumvention and rights management provisions, there were no exceptions. Opponents to the legislation seized on this, pointing out that the provisions would cripple law enforcement, since it would become illegal, for example, to access digital information kept by organized crime or a terrorist if it were protected by an access control mechanism.

The opponents likely felt that this would cause the proponents to drop the legislation, propose a substantially different approach, or change the legislation to allow any lawful access. Instead, the Administration simply added an exception, both to anticircumvention (Section 1201(e)) and to rights management (Section 1202(d)), directed specifically at law enforcement:

> This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States,a State, or a political

[175] 17 U.S.C. §1202(c).

subdivision of a State, or a person acting pursuant to a contract with the United States,a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.[176]

Another fear that was raised by the opponents is that the anticircumvention provision would somehow prevent blocking of harmful information to minors. That was then addressed by Section 1201(h):

> In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—
>
> (1) does not itself violate the provisions of this title; and
>
> (2) has the sole purpose to prevent the access of minors to material on the Internet.[177]

Yet another horror raised by the opponents was that the anticircumvention provision would make it impossible to protect personal information. And again, an exemption addressing the problem was added, in this case Section 1201(i):

> (1) Circumvention Permitted.— Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—
>
> (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;
>
> (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;
>
> (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and
>
> (D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.
>
> (2) Inapplicability to Certain Technological Measures.—
>
> This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.[178]

---

[176] 17 U.S.C. §1201(e), §1202(d).
[177] 17 U.S.C. §1201(h).
[178] 17 U.S.C. §1201(i).

IV.E.7.b. Libraries and Educational Institutions

Perhaps the least useful exception to the anticircumvention provisions is the one provided to nonprofit libraries, archives, and educational institutions in Section 1201(d).

> (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph—
>
> (A) may not be retained longer than necessary to make such good faith determination; and
>
> (B) may not be used for any other purpose.
>
> (2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.
>
> (3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)—
>
> (A) shall, for the first offense, be subject to the civil remedies under section 1203; and
>
> (B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).
>
> (4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.
>
> (5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be—
>
> (A) open to the public; or
>
> (B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.[179]

It is hard to imagine a narrower provision, and one less useful to libraries. It allows them to circumvent an access control mechanism only to determine whether they want to acquire the protected work. They can circumvent the control mechanism only to get access to the work and not to infringe any of the exclusive rights of the copyright owner, since the exception applies only to Section 1201(a)(1)(A). They have to do the circumvention all on their own, because there are no legal circumvention devices under Sections 1201(a)(2) and 1201(b). And they can't help another library do a similar circumvention. All-in-all, a pretty useless exception.

---

[179] 17 U.S.C. §1201(d).

This is probably because the library community concentrated on opposing the passage of the DMCA, rather than working to improve it with provisions that would overcome, or at least limit, the problems that they perceived, as well as suggesting approaches that would help libraries so that the overall effect of the DMCA on libraries would be positive.

For example, they could have worked for a provision that an unprotected copy of any work protected by an access control mechanism had to be deposited in the Library of Congress, so that the information would not be lost in the future if there were no longer devices that supported the access control mechanism. While such a deposit cannot be required for copyright protection under the non-formalities Berne Convention, Congress made it clear that the anticircumvention and rights management provisions of the DMCA were only related to copyright, and not to copyright protection itself.

IV.E.7.c. Reverse Engineering

A group that did know what they wanted as an exception, and got it, was the people who were concerned that technological controls could block access to a computer program that was being reverse engineered to find out how it worked, and allow it to interoperate with other computer programs. In *Sega v. Accolade*,[180] the Ninth Circuit had found that such reverse engineering was a fair use, even though verbatim copies of the entire code for a game or game console were made as intermediate steps in the reverse engineering. There had been some controversy over whether *Sega v. Accolade* and a similar decision from the Federal Circuit, *Atari v. Nintendo*,[181] were correctly decided, but Congress endorsed their holdings in the DMCA's legislative history.[182]

> (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program 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 the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.
>
> (4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.[183]

While this provision applies only to circumventing an access control, and not circumventing a protection system to infringe one of the exclusive rights, that is all that was needed by the reverse engineers. They already had their court decisions that, if properly done, reverse engineering was a fair use and so wouldn't violate any rights protected by a control mechanism under 1201(b). And because a rights management

---

[180] 977 F.2d 1510, 24 USPQ2d 1561 (9th Cir. 1992).
[181] 975 F.2d 832, 24 USPQ2d 1015 (Fed. Cir. 1992).
[182] Sen. Rep. No. 105-190 at 32.
[183] 17 U.S.C. §1201(f).

system on its own, and not working in conjunction with an access control mechanism, still allowed the viewing of the program being reverse engineered, they didn't need an exception to Section 1202.

They also got an exception to the trafficking provisions, and the right to share the information they learned:

> (2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.
>
> (3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.[184]

IV.E.7.d. Encryption Research

The Senate Judiciary Committee felt strongly that the provisions of the DMCA should not be used to stifle the very encryption research that led to the technological measures the DMCA would now protect.

> The purpose of the Committee in proposing enactment of section 1201 is to improve the ability of copyright owners to prevent the theft of their works, including by applying technological protection measures. The effectiveness of such measures depends in large part on the rapid and dynamic development of better technologies, including encryption-based technological protection measures. The development of encryption sciences requires, in part, ongoing research and testing activities by scientists of existing encryption methods, in order to build on those advances, thus promoting and advancing encryption technology generally.
>
> The goals of section 1201 would be poorly served if these provisions had the undesirable and unintended consequence of chilling legitimate research activities in the area of encryption. It is the view of the Committee, after having conducted extensive consultations, and having examined a number of hypothetical situations, that Section 1201 should not have such an unintended negative effect.
>
> It is the view of the Committee that generally available encryption testing tools would not be made illegal by this Act. Each of those tools has a legitimate and substantial commercial purpose – testing security and effectiveness – and are not prohibited by Section 1201. In addition,

[184] 17 U.S.C. §1201(f).

the testing of specific encryption algorithms would not fall within the scope of 1201, since mathematical formulas as such are not protected by copyright. Thus, testing of an encryption algorithm or program that has multiple uses, including a use as a technical protection measure for copyrighted works, would not fall within the prohibition of section 1201(a) when that testing is performed on the encryption when it is in a form not implemented as a technical protection measure. Similarly, the testing of encryption technologies developed by or on behalf of the government of the United States,would not violate section 1201 since copyright does not subsist in such subject matter. Finally, there are many situations in which encryption research will be undertaken with the consent or at the direction of the copyright owner and therefore will not give rise to any action under section 1201.[185]

While the Senate Judiciary Committee goes on to provide illustrations of encryption research that it believes would not be violations, and the reasons why, as discussions progressed on the DMCA it was felt that a specific exception for encryption research should be included.

(1) Definitions.-For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible Acts of Encryption Research.— Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in Determining Exemption.— In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner

[185] Sen. Rep. No. 105-190 at 15.

reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

(4) Use of Technological Means for Research Activities.- Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).[186]

The test attempts to differentiate between people performing legitimate encryption research and those claiming that they are promoting encryption research when they are simply distributing a circumvention program. It is impossible to draw a bright line here, and any attempt may simply provide a road map for those wanting to distribute circumvention technology to find a loophole they can exploit. However, in most cases it will not be difficult for a court, viewing all the evidence, to determine whether the activity is legitimate.

At one end of the spectrum is the scientific paper that indicates that a particular mechanism has been cracked and indicates the general approach used such that another encryption researcher can understand the technique. At the other end is a circumvention program distributed with little or no commentary on how it works. The easier it is for non-technical person to take the distributed result and use it for circumvention, the less it falls within the encryption research exception.

Note that the encryption research exception applies only to circumventing an access control mechanism in violation of Section 1201(a)(1)(A), as is the case for the reverse engineering exception. However, unlike the reverse engineering exception, the encryption research exception does not provide an exception to the trafficking provisions of Sections 1201(a)(2) or 1201(b), which can be a problem when a computer program resulting from the research is distributed, or Section 1202, which could be violated by encryption research aimed at removing a digital watermark used for rights management. One hopes that the courts will look at Congress' stated desire to protect

[186] 17 U.S.C. §1201(g).

legitimate encryption research and not find a violation of any of the DMCA provisions when such research clearly meets the encryption research test.

Just to be on the safe side, Congress also asked the Copyright Office and the Commerce Department to determine whether these provisions were adequate to protect encryption research.

> Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—
>
> (A) encryption research and the development of encryption technology;
>
> (B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and
>
> (C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.
>
> The report shall include legislative recommendations, if any.[187]

The results of this joint study can be found at:

http://www.loc.gov/copyright/reports/studies/

The study's conclusions were as follows:

> Of the 13 comments received in response to the Copyright Office's and NTIA's solicitation, not one identified a current, discernable impact on encryption research and the development of encryption technology; the adequacy and effectiveness of technological protection for copyrighted works; or protection of copyright owners against the unauthorized access to their encrypted copyrighted works, engendered by Section 1201(g). Every concern expressed, or measure of support articulated, was prospective in nature, primarily because the prohibition and its attendant exceptions will not become operative until October 28, 2000.Given the forward-looking nature of the comments and the anticipated effective date of the section at issue, any conclusion would be entirely speculative. As such, we conclude that it is premature to suggest alternative language or legislative recommendations with regard to Section 1201(g) of the DMCA at this time.[188]

It is likely that there were no actual problems that could be identified in the one-year time frame for the report that Congress established, because there were few access control mechanisms in use and too little time for problems to surface. Already, the Recording Industry Association of America (RIAA) has sent a threatening letter[189] to a university professor who was about to publish a paper discussing his cryptographic research in removing digital watermarks from musical recordings, causing him to withdraw his paper from the conference. The RIAA later said that it

---

[187] 17 U.S.C. §1201(g)(5).

[188] United States Copyright Office, Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act, http://www.copyright.gov/reports/studies/dmca_report.html (May 2000).

[189] Letter from Matthew Oppenheim, dated April 9, 2001, http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html.

didn't mean to threaten him, and the paper was presented at another conference, but such acts can certainly chill legitimate encryption research.[190]

There was no acknowledgment in the RIAA's letter of the special exception provided by Congress for encryption researchers. In fact, it was more concerned about the perceived violation of the agreement for the contest to remove the digital watermarks than for a specific violation of the DMCA, although the possibility of a DMCA violation is also mentioned.

A paper to be presented at a scientific conference that doesn't give step-by-step instructions on how to circumvent an access control mechanism is just what Congress intended to protect by the encryption research exception. Of course, the fact that somebody claims to be an encryption researcher doesn't necessarily mean that the exception applies. A paper that basically says, "Here's a program that you can run to circumvent this access control mechanism" should fall outside the encryption research exception. It will be up to the courts to determine where particular activities fall, but in many cases, it will be clear from the context of the activity.

Congress needs to monitor whether legitimate encryption research is being chilled, and make it clear that there will be remedial legislation, both to clarify and extend the encryption research exception and to provide sanctions against those who misuse the DMCA to scare legitimate researchers who will withdraw a paper or stop their research rather than face legal expenses in defending their activities. Though Congress provided in Section 1203(b) for the award of attorney's fees and costs to a prevailing party, that is limited to suits brought claiming a violation of the anticircumvention or rights management provisions, and might not be available in a declaratory judgment action where a researcher who has received a threatening letter seeks to clarify that his work is not a violation.

With traditional intellectual property, like patents and copyrights, an owner places his intellectual property at risk when he litigates an alleged infringement, or even when he writes a threatening letter that leads to a declaratory judgment action, because the patent might be found invalid or the copyright unenforceable in the litigation. There is no similar risk to somebody who misrepresents that a legal act is a violation of the DMCA. Perhaps there should be, to discourage misuse of the DMCA in threatening letters.

IV.E.7.e. Code as Speech

Restrictions on the dissemination of encryption research results raise the question of whether a computer program is protected speech, and what protection it deserves. The question is complicated because the same code conveys valuable information to those familiar with computer programming and controls the function of a machine.

In the first appellate decision interpreting provisions of the DMCA, *Universal City Studios v. Corley*,[191] the Second Circuit addressed the "code as speech" question:

> 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.*,

---

[190] An archive of information about the case can be found at http://www.eff.org/Legal/Cases/Felten_v_RIAA/.

[191] 273 F.3d 429, 60 USPQ2d 1953 (2nd Cir. 2001).

> 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.
>
> 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.[192]

The court, after discussing the scope of the First Amendment's protection for speech, particularly for scientific writings, goes on:

> 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

[192] 273 F.3d at 445-446, 60 USPQ2d at 1963-1964 (citations omitted).

> 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).[193]

But having determined that code is speech does not answer the question of what protection it enjoys. Even though the First Amendment to the Constitution says that "Congress shall make no law . . . abridging the freedom of speech," the reality is not so absolute. Congress has passed many laws that restrict speech, such as forbidding a company from providing fraudulent financial information to prospective investors.

As the court noted:

> 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."[194]

In the case before the Second Circuit, the operator of a Web site had posted a copy of a program called DeCSS that circumvented the Content Scrambling System (CSS) used to protect movies on a DVD:

> 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

[193] 273 F.3d at 447-448, 60 USPQ2d at 1964-1965.
[194] 273 F.3d at 450, 60 USPQ2d at 1966 (citations omitted).

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.[195]

A similar finding that the DMCA did not unconstitutionally restrict free speech was reached in a preliminary ruling in *U.S. v. Elcom*,[196] the criminal trial of a Russian software company that distributed a program capable of circumventing the protection for Adobe electronic books.

---

[195] 273 F.3d at 453-455, 60 USPQ2d at 1969-1970 (citations omitted).
[196] 203 F.Supp.2d 1111, 62 USPQ2d 1736 (N.D. Cal. 2002).

IV.E.7.f. Security Testing

The final exception addresses security testing of computer systems, and is much like the reverse engineering and encryption research exceptions in that it applies only to the circumvention of an access control mechanism. The provision was added in the conference between the Senate and House that developed the final language for the DMCA, after they saw that the encryption research exception might be too narrow to allow some legitimate security testing:

> The conferees recognize that technological measures may also be used to protect the integrity and security of computers, computer systems or computer networks. It is not the intent of this act to prevent persons utilizing technological measures in respect of computers, computer systems or networks from testing the security value and effectiveness of the technological measures they employ, or from contracting with companies that specialize in such security testing.
>
> Thus, in addition to the exception for good faith encryption research contained in Section 1201(g), the conferees have adopted Section 1201(j) to resolve additional issues related to the effect of the anti-circumvention provision on legitimate information security activities. First, the conferees were concerned that Section 1201(g)'s exclusive focus on encryption-related research does not encompass the entire range of legitimate information security activities. Not every technological means that is used to provide security relies on encryption technology, or does so to the exclusion of other methods. Moreover, an individual who is legitimately testing a security technology may be doing so not to advance the state of encryption research or to develop encryption products, but rather to ascertain the effectiveness of that particular security technology.
>
> The conferees were also concerned that the anti-circumvention provision of Section 1201(a) could be construed to inhibit legitimate forms of security testing. It is not unlawful to test the effectiveness of a security measure before it is implemented to protect the work covered under title 17. Nor is it unlawful for a person who has implemented a security measure to test its effectiveness. In this respect, the scope of permissible security testing under the Act should be the same as permissible testing of a simple door lock: a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner that he or she sees fit—for example, by installing the lock on the front door and seeing if it can be picked. What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock.[197]

The provision is limited to authorized testing, and the results of the testing should be conveyed to the system operator to assist in making the system more secure. It is not an excuse to post the results, or the techniques used to crack a system, to the public.

---

[197] H.R. Rep. No. 105-796 at 66-67.

(1) Definition.— For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible Acts of Security Testing.— Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in Determining Exemption.— In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of Technological Means for Security Testing.— Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2), provided such technological means does not otherwise violate section (a)(2).[198]

[198] 17 U.S.C. §1201(j).