**Spectrum Software, Inc**
2730-Q US 1 SOUTH
ST. AUGUSTINE, FL. 32086

904.797.6600 PHONE
904.797.LOCK FAX

February 16, 2000

Mr. David Carson, Esq.
Copyright Office, LM-403
James Madison Memorial Building
101 Independence Av., SE
Washington, DC 20024
1201@loc.gov

re: comments

Dear Mr. Carson,

I have been following the proceedings regarding the Digital Millennium Copyright Act and would like to submit for consideration, information and views on whether non-infringing uses of certain classes of works are adversely affected by the prohibition against circumvention of access control technologies.

Reading the DMCA and its legislative history has raised some areas of concern. As per the summary of the DMCA from the copyright office (http://lcweb.loc.gov/copyright/legislation/dmca.pdf) "Section 1201 divides technological measures into two categories: measures that prevent unauthorized *access* to a copyrighted work and measures that prevent unauthorized *copying* [2] of a copyrighted work. ([2] "Copying" is used in this context as a short-hand for the exercise of any of the exclusive rights of an author under section 106 of the Copyright Act. Consequently, a technological measure that prevents unauthorized distribution or public performance of a work would fall in this second category.)

Making or selling devices or services that are used to circumvent either category of technological measure is prohibited in certain circumstances, described below. As to the act of circumvention in itself, the provision prohibits circumventing the first category of technological measures, but not the second.

This distinction was employed to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumventing a technological measure that prevents copying. By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited."

My understanding of congress's intent in establishing the prohibition on circumvention of access control technologies is for the distribution of software to be controlled over the internet. An example would be selling or distributing a serial number or "crack" that would then create a registered and authorized version of a trial ware program that can be downloaded from the internet, such as Norton Anti Virus. Obviously the person using such information would not be authorized, has not purchased the software and the technology used does not control copying or distribution.

There is something else in the world of computer software called a hardware lock or dongle. What is a hardware lock you ask? (It is also called a dongle, SIM, and key) It is a small device that goes on the back of an IBM compatible computer at the printer port and prevents unauthorized copying or distribution of the software. As a class of work, this would certainly fall under category two. But what of the authorized user?

He has already received authorization to access the work, but this device as implemented, prevents the authorized user from making a functional archival copy of the program because of the anti-distribution device, a fair use. Under title 17 of the United States Code Section 117.a.2, one is permitted to make an archival copy of a computer program, a non-infringing use. The intent of congress and the courts was clear, that if anything happens to the original software program the archival copy can be used and the user can continue with the quiet use and enjoyment of their program. (*Vault v. Quaid*, 847 F.2d 255 (1988). With these hardware lock devices that is not possible and these works cannot be preserved.

**Sec. 117. Limitations on exclusive rights: Computer programs**

- (a) Making of Additional Copy or Adaptation by Owner of Copy. - Notwithstanding the provisions of section 106, **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**.

I am not suggesting that the rights of software manufacturers be ignored. I am a software developer, holder of 6 registered copyrights, a manufacturer and of course, a consumer. If a software manufacturer wants to copy protect their software with a hardware lock so be it, providing the authorized user has a way to use that software in an unencumbered, non-infringing way once they have made a purchase. Circumvention or replacement technologies should be made available to them providing they can provide the proper authentication. There already are exceptions listed in the DMCA, but more specific language and some clarifications would be helpful. Do the rights given in the DMCA to circumvent a technological measure supercede a manufacturers license agreement that may bar all the exceptions the copyright act provides? Is a point and click license agreement going to do the same thing even though there has been no meeting of the minds?

In general, the software I will be referring to is not for a casual user but rather for businesses, those that are in computer-aided design, manufacturing, architectural and the animation industries. They pay from as little as $400 dollars per program to $40,000 and more. Without clarifications, Section 1201 of the DMCA will limit the rights of honest, legitimate computer users and that will cost them millions of dollars as well as harm the industry. I will try to describe just some of these problems as they relate to hardware lock devices below.

## The Problem for the Consumer

There are numerous problems a consumer faces when using these devices, while most manufacturers will replace a damaged lock device, as a general rule they will not simply replace lost or stolen lock devices, they require the end user to purchase another program at whatever the retail cost may be. Hence the archival copy you are entitled to make under 17.117.a.2 is completely worthless because the program will not operate without the lock device. These programs can be quite expensive, a program called 3D Studio Max by AutoDesk™ for example, costs $3000, another called Mastercam™ circumvention of access control technologies by CNC Software, Inc. costs over $13,000, Surfcam™ by Surfware is priced around $22,000! Others are priced even higher. Some companies are honest and up front about their replacement policy such as in the 3D Studio manual-*"To replace a hardware lock that is lost, stolen or destroyed, you need to*

*purchase another copy of 3DS MAX"(pg. 5 setup manual)*, others make no mention of it in their documentation or their web sites. Can you imagine Ford Motor Company telling a consumer, Ford will not replace a lost or stolen ignition key and that the consumer must purchase a new automobile at the regular price? Would anyone tolerate this? This is the case with the computer industry.

Computer theft and damage are a very real concern and if the authorized user of a program has a hardware lock device on the computer they are simply out of luck. According to statistics "26% of all notebook reported losses were due to theft in 1998. An estimated 1.5 million computers were stolen, damaged or otherwise destroyed during 1998. An estimated $2.3 billion in computer equipment was lost, stolen, or damaged by accidents, power surges, natural disasters and other mishaps during 1998. Notebook PC damage continues to dominate accident trends. Reported accidents to notebooks accounted for 49% of total notebook losses." http://www.safeware.com/safeware/pressreleases.htm

Another problem is even if the authorized user can get insurance to cover a lost or stolen lock device, companies cannot afford to be without the use of their software (or more accurately the lock device) until it is repurchased. It can take days or longer to get a new software program with lock from either a dealer or the software manufacturer. Because many of these hardware lock devices have unique information embedded in the device, information such as the end user's name and address for instance, only the manufacturer can program that information into the device. Often the software is related to mission critical work. Not being able to use that software could cost not only dollars but also lives. A company I am familiar with in California uses a software program with a lock device to track nuclear waste, another in Florida uses a hardware locked software program at a water plant.

Some companies and Universities refuse to use software that is protected in this manner. The loss to our students is that schools will be forced to select alternative software that may not be the most common or the best in the field, hence they will not be learning what will really be helping them. For example, Autocad™ is the largest and most used CAD program and often comes with a hardware lock. It is used to design anything from houses to gears. By schools selecting another program that is not dongled, the students really don't learn on the platform they need to which will prepare them for entry into the job market. Even Autodesk's customer satisfaction director Ray Savona has said Autodesk has found these dongle-type hardware lock schemes more annoying than authorization code schemes. *(Ed Foster's article below)*(Lake Forest High School, Felton DE. "*We are currently running several instances of Auto-Cad release 14, and it is becoming increasingly difficult financially to replace hardware locks/programs each time a student decides to remove it. Along with the financial loss goes the down time in the classroom.-S.W."* The University of Virginia , *"ITC will lobby actively with software vendors not to require dongles. This is already happening at the state level…"* http://www.itc.virginia.edu/itcweb/facilities/classrooms/dongleproc.htm. The University of Utah is another example *"ACLIS reserves the right to refuse to install any software package using a copy protection scheme that is incompatible with our networking environment. This includes hardware "dongles" or keys, software with per license serialization, some network copy protection schemes, and other similar techniques. In addition, ACLIS does not support vendor-specific copy protection servers or "dongle" servers."* http://www.micro.cc.utah.edu/hoisve/csoft.html

Because technology changes so fast, business are constantly being bought and sold and some simply are forced to go out of business. If a company goes out of business, there is no one to support the authorized customer when a hardware lock is damaged since it is the manufacturer of the software, not the manufacturer of the hardware lock, that is the only one that can program the dongle. (In addition to the identifying information it contains it also has unique codes that interact with the software that only the developer would know.) Here, a perfectly good software program becomes worthless without the hardware lock and the consumer suffers. *(I purchased software about 2 years ago that came with a hardware lock. The company has since disappeared, closed down 2 web sites, does not answer phones, return phone calls, or respond to faxes since May '99. I am about to loose a reasonable investment and inventory. Can you help? (J.G.)* **and another** *(We are a manufacturer that have a program called "NSEE verify" that was sold through microcompatibles. It has a black dongle*

*block. The company was sold to Preditor software, and Preditor has discontinued this software product, and does not support it any more. We have had hardware lock burnout problems in the past, and almost could not get a replacement block last year. (R.J.)*

In another example, once a company has been acquired, their software program is phased out. After a period of time, the program and lock device is no longer supported because companies want the customer to upgrade to the newer combined product or they are using a different hardware lock device. So even though the software they purchased for $6,000 some five years ago still serves all their needs, because of a damaged lock device they are forced to upgrade to a new product at nearly twice the cost. This says nothing of the costs associated with training employees to use the new computer program. This also can happen when a loyal customer has been using the same version of a program with the dongle for years. ***Emmy Award winner*** *Bill Hendershot, President and founder of Prime Image, Inc. of California had a hardware lock fail …"and we have had no success in dealing with PADS to replace it. They tried to find another old key, but none would work"* To PADS credit however they did try *"some 40 keys at our facility to get our computer to work to no avail. Our PADS system has now been down over 30 days."*

Many of these devices have a limited life span since they use a small proprietary built in battery. When the battery dies, the hardware lock becomes non-functional and once again a program that costs thousands of dollars is worthless if the device cannot be replaced.

While the manufacturers of these devices claim that they are troublefree and transparent to the user they are anything but. These companies are blatantly deceiving the public and their own documents support this! (Rainbow Technologies, Inc.™ incompatibility list-incomp53.doc) Incompatibility problems and hardware conflicts exist, hardware conflicts such as not being compatible with new Hewlett Packard printers…the locks can't support bi-directional communications, the computer is too fast so it can't find the lock, too many lock devices on the parallel port so the lock devices can't be located, the lock device won't work if an SMC chip is present), the driver is not compatible with a new service pack release of Windows NT . (http://support.microsoft.com/support/kb/articles/q157/9/12.asp). In a document by Hewlett Packard, one solution is to remove the hardware lock device,...so now you can print but can not run your program**!** http://www.hp.com/cposupport/multifunction/support_doc/bpu01284.html**.** Sometimes a Hardware lock driver will be updated by a new application, causing the older application not to work. (Autodesk Document: US-LA-TD805390.DOC). It is the consumer that suffers, while they wait for some software genius to figure out what the problem is and how and if it can be fixed, often a process that takes months. One of the lock companies commissioned a study to use the findings as a sales tool against a competitor, the results: "Rainbow documentation and FAQ's on their Website specifically mention security key daisy-chaining constraints, and hardware revision incompatibilities among selected security keys." http://www.dongle.com/hasp/misc/nstl_report_99.html.

## Interoperability

In an age where interoperability between computer platforms is more and more important (PC to MAC or POWER-PC) these devices force us to take a giant step backwards. One customer was referred to me by a "software manufacturer", PADS, who sent the customer a demo of their product which he liked enough to purchase. After the customer purchased it, he was surprised to find that the full working version came with a parallel port hardware lock device. The customer called to inform PADS that a Macintosh computer does not have a parallel port in which to put the lock and that he was running IBM compatible software on his Mac through a program called "Soft Windows". Rather than lose a $4500 sale, the software manufacturer referred him to my company to purchase one of our programs. My software gives the authorized user an alternative to these hardware lock devices by replacing the hardware lock device with a copy-protected software equivalent that is cross platform compatible. (*letter from R.J. Austin, Tx.*)

Several companies view a cross platform solution as important, Insignia Solutions for example has developed SoftWindows for the Power Mac which "allows you to run your Windows and DOS programs and games on your Power Macintosh computer" and SoftWindows for Unix which "allows you to run your Windows and DOS programs and games on your UNIX workstation." They note the importance and cost savings of not having to purchase two separate computers to run both Windows and Mac/Unix software. (http://www.softwindows.com/4.0/support )

With computer software aiding us in more and more tasks, I fear that the external copy protection devices used will disrupt the way we work and the effects will be more and more noticeable. Think of each program you have on your IBM compatible computer, now imagine a hardware lock device, each about two inches square hanging off the printer port. So your word processor, Microsoft Word, could have a lock, your spreadsheet Lotus 123 could have a lock, your database program Paradox could have one and so on. You could not run any of these on a MAC computer. As an example, if you use the 3D Studio program with just some of the enhancement programs available for it, you'd be required to use over 5 separate lock devices for this one application! Some users have told me they have had to cut a 2x4 and place it under the locks to support them. It is not uncommon for a company to use an architectural program like Archicad for design and an animation program like 3D Studio to create virtual walk throughs. Each of these requires at least one hardware lock device. Today laptops are as powerful as any desktop computer and more people than ever before either commute or take their laptops on the road. What is it like having 5 inches of hardware locks sticking out your laptop? *("I have several software packages that utilize a dongle protection and it is becoming quite a hassle to deal with them. At current count, I have 6, count that SIX, dongles that I have to switch out every single day." (C.S. Durham Electric Co. Inc., Durham, NC)*

Does the act of access circumvention affect the value or price of copyrighted works? Not paying for software you are using and are not authorized to use is wrong and deprives a developer the fruits of their labor but we need to distinguish this act from an authorized user gaining access to a product they are authorized to use and have already paid for. Here the only negative impact would be to the company if they were not able to run the program they paid for and were authorized to use. This may be an exception of its own class. The price and value of a product is determined by the quality of the product and the support one receives for it. This is why some companies will pay $22,000 for a software program.

There are others that share my opinions that are far better known than myself. I've attached several articles having to do with hardware lock devices from two of the most respected journalist in the computer industry, Mr. Jim Seymour of PC Week Magazine and Mr. Ed Foster of InfoWorld magazine.

No one wants to see computer software pirated, however there are other ways to protect software besides hardware lock devices such as passcodes, software license files where the program checks for the presence of the file and software protection systems that permit functional archival backups and fair use. Microsoft did not become the largest software company in the world by using hardware locks on their software. The rights of the consumer to use and enjoy the software in a trouble free manner must be of foremost concern whether the technological measure controls access or controls unauthorized copying or distribution. The computer industry needs an alternative to hardware lock devices and the problems they pose and should let the marketplace determine what is effective and what is not. As Mr. Leahy stated in the Conference report on the DMCA dated October 8, 1998, this legislation should not "establish or be interpreted as establishing a a precedent for Congress to legislate specific standards or specific technologies to be used as technological protection measures, particularly with respect to computers and software. Generally…technology develops best and most rapidly in response to marketplace forces." We should let the industry develop legitimate ways to circumvent or replace access control and/or copy prevention technologies if one can do so and preserve the rights of the copyright holder.

I would respectfully submit, that no software program, DVD or any electronic medium be distributed unless the end user has the ability to have a working backup of that media, further circumvention measures of copyright protection systems should be permitted and made available for any type of software where interoperability, compatibility and fair use are an issue.

Although it may be out of the scope of these proceedings, I would suggest that the copyright law address the issue of licensing agreements as put forth in the Uniform Computer Information Transactions Act (UCITA) so that our rights as consumers cannot be simply clicked away and publishers can not write their own intellectual property law and circumvent well established intellectual property principles and statutes such as those in the copyright act. (Caterpillar Inc. http://www.4cite.org/catopp.html)

I have available the materials, documentation and witnesses I have referenced to and I would be willing to testify at a hearing regarding this matter.

Respecfully,

Joseph V. Montoro
President
good2@fdn.com

**COPYRIGHT OFFICE NOTE**: Appended this comment were two articles: "Dongles foil pirates-but drive users crazy," by Jim Seymour (from *PC Week,* November 21, 1994, vol. 11 no. 46, p. 44), and "Autodesk fights dongles, but should users have to put up with anti-piracy issues?" by Ed Foster (from *InfoWorld,* June 8, 1998; see http://www.infoworld.com/cgi-bin/displayNew.pl?/foster/980608ef.htm). Because these articles are copyrighted works of third parties, the Office considers it inappropriate to post them on its website.