Spectrum Software, Inc.
5272 Timucua Circle
St. Augustine, FL. 32086

904.797.6600 Phone
904.797.3246 Fax

May 2, 2000

Opening Remarks

Thank you for inviting me to come before you today. As a software developer and a U.S. Citizen it is a great honor for me to take part in our legislative process and I deeply appreciate the opportunity.

While I do not officially represent any trade groups or organizations, I do represent the views of numerous individuals, businesses and Universities that have experienced first hand, problems with various technological measures. I will also echo the opinions of several well-known authors such as Ed Foster of InfoWorld magazine, who has written about computer and technological issues for over 20 years, as well as Jim Seymour of PC Magazine.

Reading the Digital Millennium Copyright Act 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." [1]

My understanding of congress's intent in establishing the prohibition on circumvention of access control technologies is to prevent cable and satellite theft and to control illegal access to software, primarily over the internet. An example would be downloading a trial program such as Norton's Anti-Virus that requires a password or serial number to make it a registered version. Once the program has been purchased or registered, the access control technology is no longer in effect. The consumer is no longer burdened by the protection measure and can run and make a backup of the program. Someone selling or distributing a serial number that would create an illegally authorized version of that trial program would violate this act. With section 1201a implemented in this manner, I have no objection whatsoever.

What does concern me however is when one purchases a software program or DVD, becomes an authorized user and the access control measure remains in effect. In a case such as this, will the lawful user be able to make a fair use of this work?

The issue before us is whether persons who are users of a copyrighted work are or are "likely to be" adversely affected in their ability to make non-infringing uses of a copyrighted access controlled work. The answer to that question is yes.

Introduction

In the world of computer software there exists something called a hardware lock or dongle. 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, these fall under category two and it is not a violation to circumvent these devices under this act.

It is important to distinguish and make clear, that the large majority of these devices are used simply to prevent unauthorized copying or distribution. We are starting to see however, some devices that control the number of times you can use a program. Here a user has paid upfront for a specific number of uses. A good example might be the software that this very Copyright Office used to scan our 364 letters in response to this hearing. The software Adobe **Acrobat Capture is** priced from $699 and includes the ability to scan 20,000 pages. It comes with a dongle or hardware lock. Under ideal conditions, when 20,000 pages have been scanned the device no longer functions and you may purchase additional pages or buy an unlimited page version for $7000.

A typical user has received authorization to access this work but this device also prevents one from making unauthorized copies or distribution of the software. As implemented it prevents the authorized user from making a functional archival copy of the program because of the usage control device. This would be a fair use under previous copyright law but not under section 1201a.

The intent of congress and the courts was clear before 1201a, 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. If the lock were damaged and could not be replaced, then the user would not be able to use the remaining pages they had already paid for.

The same problem exists with DVD's, unfortunately because of the Content Scrambling System. A consumer that lawfully acquired a DVD is not able to make a backup of that media. Media and hardware can be damaged. I would ask who has not come across a bad floppy disk, a chewed up videotape, a scratched record or damaged Compact disk?

I am not suggesting that the rights of 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 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.

The reasons an exemption for fair use is needed

On October 12, 1998 in a STATEMENT BY THE PRESIDENT,[2] Mr. Clinton said of the DMCA **"This bill will extend intellectual protection into the digital era while preserving fair use."** Fair use policies are intended to protect the public interest and I hope that during my testimony I can show you why they are needed in this case.

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. This could be devastating to a small business, library or educational facility.

Hardware locked software programs can be very expensive, a program called 3D Studio Max by AutoDesk™ for example, costs $3000, another called Mastercam™ 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. 10 setup manual)***[3] **and Cadlink Technology Corporation;** ***If the security device is lost, stolen or damaged by whatever means, a replacement must be obtained from Cadlink before the software will function properly. Cadlink can charge the full current list price of the original software to replace this security device.***" [4] 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 in units 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. The numbers are even higher for 1999. http://www.safeware.com/safeware/pressreleases.htm. [5] http://www.safeware.com/safeware/99pressreleases.htm. [6] In a library or university setting, there are many people that have access to these devices and it is these institutions that are the least likely to be able to afford purchasing another software program.

Changes

Technology changes very fast. What is current today may be old technology tomorrow. It wasn't too long ago that we all used 5 ¼" floppy disks. Even Time Warner concedes, "many technical protections are still in their infancy." It is reasonable then, to believe that just as in the past, today's media and technical protections will become obsolete. Examples of this include: vinyl records, 8 track tapes, laser disks, DIVX (which was Circuit City's failed attempt at pay per use DVD's) and 5 1/4"' floppies. High Definition Television is also on the way. The current DVD's are not of HDTV quality. Is there any guarantee that future DVD players will be able to play today's movies? Considering that just two weeks ago, the FCC began proceedings to resolve compatibility and copy protection issues involving digital television receivers and cable systems, it is not very likely.
http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/2000/nrmc0022.html [7]

The National Library of Medicine has experienced problems where they have computer programs on obsolete disk formats that incorporate technological measures that do not permit the information to be restored or archived to other platforms. They are forced to maintain obsolete operating systems and equipment to access these materials.[8] This is not a cost effective way to enter the 21st century.

All of the concern regarding the year 2000 and its effect on computer systems and software was brought about because of the real possibilities of network and computer shutdowns and errors in software. Jason Mahler, Vice president & General Counsel of the Computer & Communications Industry Association whose members include AT&T, Bell Atlantic, Intuit, Oracle, Verisign and Yahoo said ***"the year 2000 problem demonstrated software programs of all types can require error correction...Once one has lawfully obtained a copy of a software program, he or she should certainly have the opportunity to repair that program so that it functions properly."*** [9]

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.

Technology companies 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 and needs to be replaced. Here, a perfectly good software program becomes worthless without the hardware lock and the consumer suffers. Steve Jacobs, president of Individuals with Disabilities at NCR Corporation used dongled software from Microsystems Software. Every member at that division works on a volunteer basis and the software evaluates the abilities of children with disabilities. Microsystems was sold to the Learning Company who no longer supports those products and **"one of our dongles is broken" leaving us out in the cold"**[10] Another letter says ***(We are a manufacturer that has 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.)*** [11]

In another example, once a company has been acquired, their software program is generally phased out. After a period of time, the program and lock device is no longer supported because companies either 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 technological 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. ***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" Our PADS system has now been down over 30 days."***[12]

Some, such as the Software & Information Industry Association ("SIIA") have suggested, "at first blush ... these examples appear to justify the creation of an exception to section 1201(a)(1)." The SIIA goes on to say that other options make this exception unnecessary. The first option they list is "If "consumers" are concerned about having access to code due to irreparable damage to the access control technology or the demise of the copyright owners business, they can use trusted 3rd parties to escrow software code in confidence to ensure future access to the content if such events occur. (reply comments #59) ***The mistake made here is simple and obvious; consumers do not have access to the source code written by a developer!*** Further, developers are **not** required to escrow their materials with

any 3rd party and even if they were it does not overcome the issues of fair use, interoperability, theft, security testing and research! The second solution the SIIA offers is "to get the copyright owner or the manufacturer of the access-control technology to "fix" the technology". The problem with this logic is twofold, first the question was -what do we do when the copyright holder **is out of business or the product is no longer being supported?** Second, because of the secure nature of the technological measure, only the developer of the software, not the manufacturer of the hardware lock, can program the dongle or fix the application. The reason is because these hardware lock devices have unique information embedded in them from the developer and there are also unique codes that are embedded in the software program that only the developer would know.[13]

Jim Seymour in PC Week Magazine wrote about another reason we cannot depend on the manufacturers to fix a problem. PC Week Labs does product evaluations and AutoDesk sent in their software 3D Studio, an animation program to be evaluated. The techs couldn't get the program to run with the security device, so AutoDesk sent another one, it wouldn't run either. They tried another computer with the same results. When they contacted AutoDesk again they were told,**** "**buy another computer**". Reminiscent of earlier testimony here today, Mr. Seymour goes on to say that "**dongle makers and the software vendors that support them, argue that dongles are essentially trouble free, no burden at all to honest users. Ahh, if only that were so...dongles cause a world of trouble for those unlucky enough to buy applications using them.**"[14]

When AutoDesk's customer satisfaction director said to Ed Foster of InfoWorld magazine, AutoDesk has found dongle type hardware locks more annoying than authorization code schemes, Mr. Foster received a wave of dongle hell letters from readers that had similar experiences. One reader from an academic institution reports that out of 16 computers the school had recently upgraded from AutoCAD version 13 to version 14, 5 were put out of action when the dongles failed. Many readers report having to put up with multiple dongles, a situation that can lead to trouble. Another reader wrote in "**Some vendors always say, "If you have multiple dongles be sure to put ours on first or else the computer might hang or crash.**"[15]

The availability for use of copyrighted works

The availability of dongle-protected works for use by libraries, companies and Universities is also diminishing. Some 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. 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, in order to prepare them for entry into the job market. ***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."*** [16] **The University of Virginia, *"ITC will lobby actively with software vendors not to require dongles. This is already happening at the state level..."***[17] 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."***[18] http://www.micro.cc.utah.edu/hoisve/csoft.html

Incompatibility problems

While the manufacturers of these devices claim that they are troublefree and transparent to the user, they are anything but. On the companies web sites are many examples of incompatibilities and conflicts. Often months will go by before a solution is found, in some cases there is no solution. 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, http://www.rainbow.com/tech/help/technotes.html. [19] 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) [20] One fear many people have is that not only expensive high end applications will use these technological measures but every day software and even kids games will come with these devices. Unfortunately these people are correct. In a document by Hewlett Packard, "My Interactive Pooh" comes with a dongle. This device causes "incompatibilities with HP DeskJet printers" http://www.hp.com/cposupport/printers/support_doc/bpd06343.html [21] I don't think I am exaggerating when I say that we are inviting a technological nightmare and soon will see a protection device on every piece of software we use. In another HP document two-way communication cannot be established with a printer using a dongle, their solution is to remove the dongle, now you can print but cannot run your program. [21a] Sometimes a Hardware lock driver will be updated by a new application, causing the older application not to work. http://www3.autodesk.com/adsk/support/techdoc/0,,160075,00.html. [22]

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. One of the lock companies commissioned a study to use the findings as a sales tool against a competitor, the results: Rainbow's 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. [23]

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. (*letter from R.J. Austin, Tx.*) [24] 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.

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)

These same statements are true for DVD as well. Being able to view or operate a DVD on other platforms such as Linux, is also at issue. The justice department has spent a considerable amount of time and money investigating Microsoft and one of the reasons given by the assistant attorney general of the United States for splitting up Microsoft was that they would not make their Office software available on a competing platform like Linux.

Physical problems

For a University, Library or other facility that must run some of its software on a server there is a physical problem as well. When a business such as the Durham Electric Company in Durham, NC has 6 dongles hanging off the back off a computer, imagine the number that a University or Library has or will have in making works available to the Public. ***("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)*** [25]

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 5-10 inches of hardware locks sticking out your laptop?

Does the act of access circumvention affect the value or price of copyrighted works?

Not paying for software you obtained illegally 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 or individual if they were not able to use what they paid for. The effect of circumvention for authorized users will increase the sales of DVD and Software, where previously unsupported platforms are now available and those institutions that have policies against using dongled software will once again become users.

No one wants to see computer software pirated, however there are other ways to protect software besides hardware lock devices such as pass codes, 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. Perhaps we should follow the lead of a company called Unisoft of Milford Connecticut. Unisoft is a software developer that used dongles on their software from day one. When the manufacturer of the dongles discontinued the model, they considered other brands. Their conclusion – *"**A determined pirate can make an unauthorized copy of software and make it run, regardless of dongles. To a legitimate user, however, a dongle is an inconvenience at best, and at worst makes completely legal software completely useless."... We are more interested in satisfying our legitimate customers than foiling pirates.... we will aggressively investigate and prosecute any and all illegal copying of our software, but will not do it at the expense of our honest customers". They now use a simple license file and pay a referral fee to their customers if a customer gives a copy of the software to someone and they end up purchasing. "We think that our software is very reasonably priced, especially the prices for adding additional users. We think that the Software Support Program (SSP), our annual support subscription, adds significant value to the software and is also reasonably priced. We think customers will find that it is most cost effective to be legitimate and to keep up-to-date. But most of all, we don't think that our customers would try to***

cheat us. We trust our customers to buy additional licenses when they realize that they need extra workstations." [26]

In my conversation yesterday with Mr. Lareau, Vice President of sales at Unisoft, he confirmed that customer satisfaction has increased and there are less headaches for the company and was not able to identify any decrease in sales by using this policy.

An independent study done in Canada bears this out. Of those polled 48% had an unfavorable opinion of hardware locked software [27] and 52% felt that there was a need for a replacement device. [28]

Solutions

I'd like to stress again that most these devices are primarily used to control unauthorized copying or distribution, [29] however the rights of the consumer to use and enjoy 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 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."

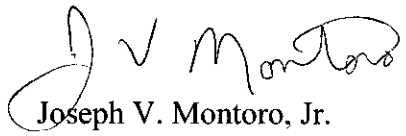
To date we have only looked at this issue in terms of black and white, either access control technology is circumvented or it is not. I submit we should look at it a third way. We should let the industry develop legitimate ways to replace troublesome access control and/or copy prevention technologies if one can do so and preserve the rights of the copyright holder.

Through my software development, I have been able to create a one for one hardware lock replacement done in software that has all the functionality of the original device yet cannot be copied unless you are authorized. Through this product, I have been able to overcome every objection raised regarding software including interoperability, compatibility and fair use while still protecting the rights of the copyright holder.

I would respectfully submit that an exemption be made so that once a person has lawfully acquired access to a work, subsequent uses of that work will be exempt under fair use. At the very least, this should be applied to computer software and DVD's where media can be damaged and there will always be issues of compatibility and interoperability. Lastly, it would be a waste of resources for any institution, agency or user that may qualify under current or future exemptions to bypass or replace a technological measure themselves when that is not their field of expertise, therefore companies should be permitted to advertise and provide these services providing certain criteria that you decide is met.

Once again, thank you for the opportunity to appear before you and I look forward to answering any questions you may have.

Respectfully,



Joseph V. Montoro, Jr.
President