The hearing was held at 9:30 a.m. in the Postal Rate Commission's Hearing Room, Third Floor, 1333 H Street, Washington, D.C., Marybeth Peters, Register of Copyrights, presiding.

PRESENT:
MARYBETH PETERS Register of Copyrights
DAVID CARSON General Counsel of Copyrights
CHARLOTTE DOUGLASS Principal Legal Advisor
ROBERT KASUNIC Senior Attorney of Copyrights
STEVEN TEPP Policy Planning Advisor

PANEL I WITNESSES:
FRITZ ATTAWAY
MICHAEL EINHORN, Ph.D.
PHIL GENGLER
STEVAN MITCHELL
ROBERT MOORE
SHIRA PERLMUTTER
RUBIN SAFIR
BRUCE TURNBULL

PANEL II WITNESSES:
JONATHAN BAND
SHAWN HERNAN
KEN KUPFERSCHMID
CHRIS MOHR
JOSEPH V. MONTORO, JR.
EMERY SIMON
JAY SULZBERGER
# I-N-D-E-X

## Morning Session

### Motion Pictures and Audio/Visual Works

<table>
<thead>
<tr>
<th>Speaker</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rubin Safir</td>
<td>6</td>
</tr>
<tr>
<td>Phil Gengler</td>
<td>14</td>
</tr>
<tr>
<td>Robert Moore</td>
<td>16</td>
</tr>
<tr>
<td>Michael Einhorn</td>
<td>32</td>
</tr>
<tr>
<td>Bruce Turnbull</td>
<td>39</td>
</tr>
<tr>
<td>Shira Perlmutter</td>
<td>48</td>
</tr>
<tr>
<td>Fritz Attaway</td>
<td>54</td>
</tr>
<tr>
<td>Stevan Mitchell</td>
<td>58</td>
</tr>
</tbody>
</table>

### Questions and Answers

## Afternoon Session

### Literary Works

<table>
<thead>
<tr>
<th>Speaker</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe Montoro</td>
<td>143</td>
</tr>
<tr>
<td>Shawn Hernan</td>
<td>158</td>
</tr>
<tr>
<td>Jonathan Band</td>
<td>166</td>
</tr>
<tr>
<td>Jay Sulzberger</td>
<td>170</td>
</tr>
<tr>
<td>Chris Mohr</td>
<td>178</td>
</tr>
<tr>
<td>Keith Kupferschmid</td>
<td>181</td>
</tr>
<tr>
<td>Emery Simon</td>
<td>196</td>
</tr>
</tbody>
</table>

### Questions and Answers
CHAIRPERSON PETERS: On the record. Good morning. I'm Marybeth Peters, the Register of Copyrights. I would like to welcome everyone to the third of the four days of hearings in Washington in this Anti-Circumvention Rulemaking.

The purpose of the rulemaking proceeding is to determine whether there are particular classes of works as to which users are or are likely to be adversely affected in their ability to make non-infringing uses if they are prohibited from circumventing technological measures that control access. It's a long sentence.

Today our session will focus on a number of proposed exemptions relating to audio-visual works on DVDs including backing up audio-visual works, tethering an audio-visual work to particular devices and region coding on DVDs. This afternoon's session will focus on proposed exempts for literary works including computer programs.

Let me now take a moment and introduce the Copyright Office panel. To my immediate left is David Carson, General Counsel of the Copyright Office. To my immediate right is Rob Kasunic, Senior Attorney and
Advisor in the Office of the General Counsel also known as "Mr. 1201." To his immediate right is Charlotte Douglass, Principal Legal Advisor in the Office of the General Counsel. And to David Carson's left is Steven Tepp, Policy Planning Advisor in the Office of Policy and International Affairs.

The agenda for the next hearing which will be on May 9th and which will take place here at 9:30 a.m. will be on two different topics but we'll skip that right now and go on to what we're going to be doing. The Office will be posting the transcripts after all hearings approximately one week after the hearing. The posted transcripts will be those as originally transcribed. There will be an opportunity for people to correct the transcripts. The goal is to get the transcripts up as quickly as possible so that people who are preparing for further hearing can have them. Then we'll do the corrections as soon as we get them back.

The reply comments and the hearing testimony will form the basis of evidence in this rulemaking which in consultation with the Assistant Secretary for Communications and Information of the Department of Commerce will result in my recommendation to the Librarian of Congress. The
Librarian will make a determination before October 28, 2003 on whether or not there will be any exemptions to the prohibition which should be instituted for the next three year period.

The format I have in front of me says it's divided in three parts. We've never really totally made it to the third part. The first part is that each of you get to present your statement. There is no official time for that. There are a lot of witnesses this morning so you should make it as brief as you possibly can. Then we get a chance to ask you questions. Hopefully some of them will be tough. And the third part is that you can ask each other questions.

Just for the record, it seems that in our asking the questions you all ask each other questions which is why we never get to the third part. I'm going to stop there. Because there aren't nameplates, maybe we can start with you, Michael, and you could go down, say your name and who you are affiliated with so that all of the people up here know who you all are. Nameplates will appear as this hearing progresses.

DR. EINHORN: My name is Michael Einhorn and I'm speaking here today on behalf of myself.

CHAIRPERSON PETERS: Shira.
MS. PERLMUTTER: I'm Shira Perlmutter with AOL Time Warner.

CHAIRPERSON PETERS: Bruce.

MR. TURNBULL: I'm Bruce Turnbull of the law firm of Weil, Gotshal & Manges here today for DVD Copy Control Association.

MR. ATTAWAY: I'm Fritz Attaway, Motion Picture Association of America.

MR. MITCHELL: Stevan Mitchell on behalf of the Interactive Digital Software Association representing the video game industry.

MR. MOORE: Robert Moore with 321 Studios.

MR. GENGLER: Phil Gengler representing myself.

MR. SAFIR: I'm Rubin Safir. I represent two organizations. One is called New Yorkers for Fair Use which I started in 2000. The other one is NYLXS which is the New York Free Software Linux scene in New York City. It's grassroots.

CHAIRPERSON PETERS: Okay, thank you very much. We'll start at that end and move down. Let's start with you. Bob is telling me we should do proponents so let's start on this end.

MR. SAFIR: So it's the official statement.
CHAIRPERSON PETERS: You make a statement with your case.

MR. SAFIR: All right. The last time these hearings showed up which was 2000 as I recall we were protesting outside at the Library of Congress because a young man in Finland had been arrested for trying to use his DVDs that he had purchased and was his legal property on his computer using a free operating system which in this case was GNU Linux operating system.

It was bizarre because the way he got arrested was he hacked into the encryption that the copyright control people had created in that. But what was really weird about it was that one of the keys somehow magically showed up and was available in one of the commercially available DVD players. Now with all the trouble that the movie industry went through to create this scheme and all the control that they had exerted over the systems, it was rather remarkable that somehow one of these keys just showed up magically just in time when the movie industry wanted to have a test case for the DVD and for the DMCA in order to strengthen their hand. But nevertheless that's what happened.

Unfortunately for them what happened was
it happened in a foreign country. Nevertheless he was arrested not under the DMCA but he was arrested under various things. Then we met him later in New York when there was a court case trying to suppress the reporting of the DeCSS software which hacked into the encryption and allowed for the playing of those DVDs on any choice of operating system that you wanted to play it on.

Since that time I started New Yorkers For Fair Use in response to that gross violation of that individual's rights and gross violation of my rights and my kids' rights. After doing extensive research on the matter of the DMCA and the results of what's happened, we've had been able to come to only one conclusion which is that digital rights management especially as it applies to DVDs is theft.

Originally when I wrote to ask to speak here, I said that I wanted to have an exemption for all cash-and-carry commercial products. The reason for that is because constitutionally "fair use" is defined by Judge Ginsburg and as other judges as your constitutional rights to private property under the Fourth and Fifth Amendments of the Constitution.

When you go out and you purchase something for cash, it's yours. You take it home and it's
yours. If you want to play it on your free operating system, that's good. That's your choice. If you want to play it on your blender, that's your choice. It's yours. If you want to scratch it and you want to rip it apart or throw it out the window or feed it to your dog or use it as a coffee coaster, that's your choice. The information that's on that copy there is also yours and the computer and the system that it runs on. It's your private property.

Now I don't need to tell the lawyers here about what the Constitution says about property but clearly the Fifth Amendment says blah, blah, blah, "...nor shall be deprived life, liberty and property without due process of the law." So let's explain this. Phil is going to help me.

Phil, you're a store owner. Right? Phil, do you have Fats Waller CD or DVD by any chance?

MR. GENGLE: Yes, I do.

MR. SAFIR: Great, how much is it?

MR. GENGLE: Fifty cents.

MR. SAFIR: Okay. Here's fifty cents. Thank you. Now this is my DVD. Wait. I want to use this DVD.

MR. GENGLE: You can't.

MR. SAFIR: Why not? Now that's theft.
That's theft and that's what happens in my computer because I only have in my house free operating systems. There is no legal way despite the fact that they promised us that they were going to allow us on free operating systems using free software to be able to play DVDs. By this time, there still is no legal way of doing it. The way I can play my DVD on my free operating system is to either hack it with something that is a felony or a trafficking program or unless I happen to a genius and able to hack it myself.

Now in the case of the encryption that was used on the DVDs, it was a pretty weak encryption but the reason why it was hacked so quickly was because accidently "somehow" the key in it was made available. I don't understand how that could happen but maybe the good people over there can explain it better.

In addition to that, there's no contract involved. Sure, the DMCA says if you put an encryption on something that you should be able to enforce not copying but actual access to your own property. You have a situation like at New York University in the Dental School where all the textbooks sold are on DVDs. At the end of the semester, the DVD turns itself off and then you have to purchase it again. They graduate from school with
no textbooks.

Now we've been assured by the market that the market is going to take care of this problem. The market can't take of this problem because this is a civil rights issue. The market cannot take care of civil rights issues. A market can only occur when people are guaranteed their civil rights.

What we have right now is an extortion racket. You have to purchase an approved player only to play any DVD or any movie in the continental United States. In Europe, I had the fascinating experience of going to France and they have three DVD players. Each one of them has a $55 license to the extortion racket over there so that they can play English ones and then they can play Japanese ones and then they can play French ones. It's remarkable.

Mind you, in my house, my kids aren't allowed to watch TV. We don't have a TV. I watch everything on my computer. My kids don't know that. I have a television built into my computer.

The bottomline is the first time I went over to a friend's house to see a "Star Trek" movie and he put it in and then the preview started. Then he said "This is boring" and he tried to click it forward. It came up with this big warning which said
"Warning: you do not have access to this part of the DVD." I looked at him like "What?" It was the first time I heard this before. But when you actually see this happen it's astonishing. It's like watching a mugging in Central Park.

I said "How can you let that happen to yourself like that." Sure enough, he couldn't move it back. This was actually Trekkie. It was not a "Star Trek" movie. It was about little snips of comedy or real life Trekkie convention stuff. Once and a while they tried to move around the DVD in order to reseat parts and he accidently flipped back to the previous section which was very easy to do since it was section one, then he was stuck again and there were 14 minutes of previews every time.

This is unacceptable. This is a violation of people's basic and fundamental property rights in which free society is based on. If that's democracy, we need to have ownership of information. It wasn't so long ago, two years ago, that Judith Platt from the Association of American Publishers went over and said that "Librarians are like Waco terrorists because they want everybody to be able to read for free" and this is almost a direct quote. It was such an astonishing thing to read that the light bulb start going up and
you start realizing that something is wrong.

We really have two choices in front of us as a society. We have this huge technological boon which is making information extremely inexpensive. My dear grandfather who just passed away at 89 years old nothing in his lifetime that was produced is not under copyright currently. That means the entire events of his life, the invention of the radio, the invention of the record player, cars, World War II, the airplane, the whole 20th century is under copyright.

You cannot teach children in school anything about the 20th century or any of the technology of the 20th century without being in violation or not violation of somebody's copyright. We can't continue. Now that in itself is not such a bad thing. I would not make the issue that we don't want copyrights.

However the protection of the public as Ginsberg said in the Overage case is that both "free speech" and I will extend it to copyrights "is fair use." Therefore the statute that says "fair use" is defined in Section 102 of Copyright Law that defines "fair use" is not everything about "fair use." "Fair use" as Ginsberg says "is clearly the application of your basic human rights as defined in the Constitution
in regard to the 'exclusive rights' of commerce of copyrighted material." As long as that "fair use" aspect is protected, I couldn't really care if it's 300 years for a copyright but as soon as I can't take my DVD and make a copy of it so I can store it then there's something wrong here.

We've already seen in the last three years multiple changes in information technology platforms from MP4s and MP3s and so on from the CD and it's going to change rapidly again. If we can't be able to move that information around and if I can't give a copy of it to my grandmother so that she can enjoy it, then there's something extremely wrong with the society.

We are at a fork. We can decide that we are going to construct a society that's similar to George Orwell's "1984" or we can decide that we're going to go over and live a free society. There is no reason why at a time period when the cost of information keeps going down, that the cost of education keeps rising. This should indicate that there is something seriously wrong with the way that we are handling information in our society.

One last thing I would like to say, at the end of the last hearings, and I listened to them all
on MP3 as they were going on, or as they were released, they were not on MP3, but on real audio files. The music industry had said the DVDs themselves, or the movie industry had said the DVDs themselves were not copyable. This panel asked them that isn't it possible that if they copied it directly in Taiwan by some device it forbids that you can pirate them anyway which was the point that was made. In fact they said well we'll have to find out for you later. Then later on they wrote in their answer that in fact it's not possible. Even if you copy them bit for bit that you wouldn't get a readable copy. That statement was a flat out lie. I don't know if it's perjury but it was a lie.

Anything coming from that side of the table was tainted by the fact that they had previously lied to this Commission. Two weeks after that you could go Queens and buy hundreds of DVDs, all of them with encryption codes. We checked to see if they had encryption codes in them and they did. They were exact duplicates of the DVDs that the movie industry actually created. Barry Sorkin from AOL Time Warner was one of the ones who contributed to that lie. You have to take that into account when you listen to what the other side of the aisle says. That's my
testimony.

CHAIRPERSON PETERS: Thank you very much.

Mr. Gengler.

MR. GENGLER: All right. I'm here today as a user of one of the alternative systems that Rubin mentioned. I use Linux exclusively on my computers, both a laptop and a desktop. Increasingly, these operating systems like mostly Linux but others like FreeBSD, BOS and even other less common ones are being used as an alternative to Microsoft Windows who people choose not to use for various reasons awaiting to their policies or costs even.

The situation that exists with Linux with regard to movies is that you can't play them. It's not due to a technological impediment. It's perfectly capable of handling DVD play-back if it had access to the keys used to encrypt the movie. These keys are kept private and licensed only to those who pay the licensing fee to the DVD CCA.

Back in the Universal City Studios versus Reimerdes, one of the cases Rubin cited where 2600 Magazine was linking to the DCSS program. The DVD CCA said that they had two licensees for the technology for creating Linux players and that within a few years these players would be available. As of today there
are no licensed DVD players available for Linux or any other of these operating systems. Even if one was released for Linux presumably they would release it in executable form as a binary so that you would not get access of the source and you couldn't see the keys.

In capability in the binary structure between these other operating systems means that a player for Linux works only Linux and wouldn't work on FreeBSD or anything else. So you are still out of luck even though Linux users may have a way to play.

Without being able to decrypt the CSS encryption concerning these DVDs, there's no connecting even personal access to a movie just to watch it. The inability to obtain or use these technologies to get any kind of access to watch it, to make a backup copy of it, to do anything with it is clearly a case where their ability to use a work in a non-infringing way is made impossible by the technological encryption. I'll keep it brief. That's all I have.

CHAIRPERSON PETERS: Okay. Thank you very much. Mr. Moore.

MR. MOORE: Good morning, Madam Register and members of the Copyright Office. My name is Robert Moore and I'm the founder and president of 321
Studios. We're based in St. Louis, Missouri. I began 321 Studios in June 2001 with my son to teach him about the principles of running an Internet business. I am a software engineer by trade. We focused on basically developing a software to address problems that people have with DVDs.

DVDs are a great but fragile technology. Sorry about this but the screen doesn't quite want to synch up with the laptop. Despite the hype that DVDs are indestructible in routine use, they are quite subject to scratching, chipping, warping, delamination, among other things that make DVDs inaccessible.

Our reply comments in this proceeding detail the personal accounts of hundreds of families who have experienced these problems which we've submitted to you. Since our filing in February, we continue to receive messages from hundreds and thousands of other people complaining about the DVD problems and praise for our particular products.

Now to address the real live problems of DVD owners, 321 Studios developed software whose primary purpose is to help people use and protect their DVD collections. While consumers can use 321 software to duplicate and preserve DVDs they have
personally created, the public does not need any special rule to use our software for that purpose.

However because 321 software can restore damaged DVDs to a playable condition and make backup copies before damage occurs, we have been the target of a campaign to shut down our operations. Indeed I learned about how 321 software allegedly violates the DMCA when I read a newspaper article on DVD piracy in March of last year that quoted an MPAA spokesman who was leveling civil and criminal accusations against 321. Since then we have initiated a lawsuit to defend our products and our practices. Thus our participation in this current Copyright Office proceeding takes on urgency.

Without conceding any legal position, 321 has been tainted as a violator of Section 1201 because of the software that it markets. To the extent that the software serves exempt purposes, the bona fides of our operations will be more evident and the public will be able to overcome adverse effects in the making of non-infringing uses of particular classes of works, access to which is effectively protected by technological measures.

I have two purposes for my comments today. First, I want to highlight the problems with DVDs that
lead us to support designation of particular classes of works for exemption and specifically literary and audio-visual works including motion pictures embodied in DVDs that may or may become inaccessible by possessors of lawfully obtained copies due to malfunction or damage. Second, I want to demonstrate how 321 software deals with these problems.

Most DVDs today are released in encrypted form. The DVD's Technological Measure Copyright Scrambling System ("CSS") is well known to the Copyright Office. But let me summarize several things that are relevant to this proceeding. CSS locks DVDs so that they can be played licensed DVD players only. These players are given digital keys to unlock or open the DVD. Secondly, CSS scrambles content so access is further controlled. And thirdly, the Copyright Control Association controls to these encryption keys needed to unscramble the content.

Now according to the MPAA technical expert in our litigation, Robert Schumann, the typical DVD is encrypted in multiple ways and licensed DVD players utilizing player software have four keys to decrypt data. These keys are your disk keys which are used to decrypt the title keys. Your title keys themselves are used to decrypt actual DVD content. Session keys
which are given to unique viewing of a DVD and are deleted when a DVD disk is removed which are temporary keys. Fourth, player keys which are used to decrypt the disk keys.

I would also like to point out at this juncture that these disk keys are stored and can be stored in multiple locations on the DVD and can change from section to section or from chapter to chapter on the DVDs. If an area of the DVD that becomes damaged happens to hold that disk key, it will prevent the access to that particular section of the movie.

Unlike an old LP album which I used to own and I'm sure some of you did as well, if you scratch one song, then you can't hear that particular song or maybe you can hear it and it skips and distorts in that particular section. Unlike the LP or the vinyl records, the DVD once it becomes inaccessible can be completely totally inaccessible or portions of it.

I don't know about you but when I watch a movie it's important to me to see the entire movie from beginning to end. The MPAA may argue that I would only lose access to maybe Chapter three or Chapter four but maybe that's the chapter where I find out the butler did it. If I can't view the entire movie and its content, that's obviously something that
would bother me.

Disk keys and title keys are stored in secured areas of the DVD and themselves are encrypted. Again according to Robert Schumann, a witness in the litigation, he basically says that "321 ZBDX copies circumvents the normal DVD access and copy protections afforded by CSS." As I said, "DVDs are marvelous but also fragile technology." It goes without debate that DVDs are a marvelous technology and that consumers have embraced DVDs as few new technologies, spending huge sums in the process. Typical DVDs can cost anywhere from $10 to $30 each. Players can cost $70 to $1,000 a piece. Box sets of DVDs can range from $70 to $100 a piece.

It's easy to see that consumers spend hundreds and in some cases thousands of dollars on private DVD collections. I am one of those people. I have hundreds of DVDs in my private collection. However this wondrous technology is far from foolproof. It often does not work correctly even on licensed players. They can become scratched very easily. They can become warped due to heat damage. They can become chipped and delaminated.

This is a new thing that I actually learned about within the past six months which is
about DVD rot. There are two layers in most DVDs giving it the ability to hold the voluminous amounts of data on that digital versatile disk. Those two layers due to imperfections in the manufacturing process can actually come apart. When they come apart, again it can make the DVD unplayable or inaccessible in many cases in its entirety.

Since the locks and keys of retailed DVDs are embedded on each disk, corruption can be to content and to the technological measures designed to limit access to content. It is impossible for a user who bought a DVD to know whether the content or the technical measures are corrupted. The only thing the user understands is that the DVD does not work. Corrupted DVDs cannot be viewed or contents skips or is distorted.

While consumers treasure DVDs, we have learned when there is a breakdown they are denied access or their viewing experience is highly distorted. 321 customers explain that scratching can occur innocently and unexpectedly. The biggest demographic of our market for our product is people who have children. A child mishandles a DVD. A family pet claws it. You take it to the beach with you on a portable player and the sand scratches it.
DVDs can easily warp. Warping is a common phenomena experienced when DVDs are left in hot cars or overheated environments. DVDs can chip and crack very easily. Many people find DVDs crack when they try to get them out of the center holding device in the DVD case. What is more manufacturers have provided them no relief. Typically damaged DVDs cannot be returned or exchanged. An investment is therefore completely lost.

At best, one can only buy a replacement at a particular price assuming one is available and this is where it really gets very sensitive. People like myself have bought DVDs that are collector's items. These are special editions that are released for limited periods of time to the public. After that, they are withdrawn. They are no longer available on the store shelf. This has happened to me in several occasions.

I cannot replace the DVD that has become damaged or delaminated through no fault of my own if I wanted to. Some might argue I can go on eBay or I could find another source for a DVD that is no longer available to the public. Does that mean that my only alternative then should be to pay a higher price if I can find a collector's DVD that is no longer
available? Should I be forced to compete in an open market environment for the few DVDs that are left of a particular collector's edition? I do not think so.

321 believes that the harms consumers experience are unfair and are inconsistent with the underlying propositions and purposes of Copyright law. If other kinds of work are damaged, they still may be usable. For example a book can be read even if it's pages are torn. An LP as I stated before can be played even if it's scratched in some cases. A video cassette can be viewed even if the tape has been warped.

But DVDs are different. They are marvelous technology and they have been hyped as a permanency in media. However they are very fragile. If the damage occurs to the access codes, no viewing is possible.

In our reply comments, we submitted hundreds of declarations of problems from consumers. In preparing for this hearing, we received even more. Typical of these is the testimonial of Marcus Zinsberger from Bonita Springs, Florida. Mr. Zinsberger wrote about a DVD of the film "Dragonheart." He explains "It just won't work anymore. I can see no physical damages whatsoever.
I have tried playing it on about four or five different players. It doesn't work on any of them. Since the disk is out of print, it is expensive to replace. Even used copies are hard to get and expensive."

321's premier software product is DVD X Copy and it is designed to create usable back-up copies of DVDs. Importantly DVD X Copy can restore scratched and damaged DVDs to playable condition. Now it can't do it every DVD. Some DVDs are so badly damaged that nothing can bring them back to their original playable condition. But in many cases we have found that DVD X Copy because of the error correction code built into the DVD itself, a DVD-ROM installed on an individual computer can sometimes through hours of retrying to read that data can finally read the data and again restore it back to its original condition.

You should also know that as part of 321's commitment to proper use of copyrighted materials which we have gone to great lengths to try and educate the consumer in this regard, we have incorporated several anti-piracy mechanisms in our software. Now I will highlight these as I explain how our software works.
First before DVD X Copy can be used, you must register with 321. This is an example of our registration or activation screen. Registration or activation is our first line of education and defense. It is important because we actually use digital watermarking technology so that we can track if someone is abusing the software and the copyrights of content owners.

What happens is when a customer of ours activates the software, they do so with a licensed ID and a password that is either in the retail box that they purchase or it's assigned to them when they purchase it on-line. This creates a fingerprint of the user's PC that has to do with the hardware that's inside, the hard drive, the amount of memory and other various hardware configurations specific to their computer.

We tether our application to this personal computer. If they move the software, it will no longer function. That tethering process or that activation process is used so that when our customers avail themselves of the fair use of this product, we create a digital watermark from that activation, from that fingerprint, of their PC and it's embedded thousands of times throughout the video stream.
Our customers must also agree to a stringent use policy. We only authorize use of our software for the making of personal private copies. All users of 321 software told "this program allows you to create an archival or back-up copy of a DVD solely for the private and personal use of the owner of the DVD. Federal Copyright Laws prohibit the unauthorized reproduction, distribution or exhibition of copyrighted materials, if any, contained in this archival back-up copy. The resale, reproduction, distribution or commercial exploitation of this archival back-up copy is strictly forbidden. To use this program, you must agree to respect the rights of the copyright holders."

I believe that most people are honest. I believe that most people desire to see copyright holders rewarded for their efforts and for their investments which is why I think we have steel spikes in front of intersections when the lights turn right. We expect people to obey the law and when they are properly educated with their responsibilities in respect to those laws, I believe that most people respect the law and do so.

Another thing, making backups using 321 software is a slow process. First, DVD X Copy must
recognize the disk. It takes a few minutes to do so. Then we actually ask them if this is a rented or borrowed DVD. Many people have complained that our software would allow the illegitimate backup or copying of rented or borrowed DVDs.

Again what we are doing here is we are attempting to educate the consumer in regards to their specific responsibilities. If they are to answer yes to this question, the program will terminate after displaying a dialogue box showing and demonstrating to the customer that it is not legally permissible to do so. They must own the DVD that they are making a backup copy of.

We also go through the reading process. As you can see here, this particular DVD has gone on for about 32 minutes. The remaining time is about an hour and a half. We do get faster times with some computers. But the point that I'm trying to demonstrate here is that this is not a Xerox machine by any stretch of the imagination. This is a specific one-use process that the user must go through each time they wish to make an archival backup copy.

Now when working with damaged disks as I pointed out before, the process is further complicated because the data on the disk may not be readily
comprehended. I actually thought I had a screen shot of the abort/retry screen shot. What that actually does is when it encounters an error on the DVD disk, the program is using the error correction code built on the DVD.

I'll try to make this as non-technical as possible. There is a data stream that is being read from beginning to end at any particular moment that a player is reading the data off of the DVD. At the end of that data is a check sum. In other words, this is a number so that if you were to apply some algorithms to this data stream to all the numbers and divide it by some number, it would produce this check sum. Once the player has read that data, it produces the check sum, compares it with the check sum at the end of the data stream on the DVD. If they match, then it knows that it read the data correctly.

The error correction code happens when check sums do not match each other. So that the player and the software are actually attempting to artificially reproduce the data stream in such a fashion that it produces the same check sum that it's expecting to see from disk.

Do you follow what I'm saying? That can take a lot of time. We're not actually after many
reads reading the same data over and over again. We are attempting to find the correct balance of data from the read so that we can say "Ah, we finally have it". We have been able to artificially reproduce that data. This can take a lot of time. We have seen cases where in order to turn a DVD back into playable condition, it can take sometimes from six to 12 hours to go through this abort/retry process.

Every DVD backup made with 321 software also contains an indelible disclaimer. That's what this is. When people make a backup copy of their damaged DVDs or DVDs before they are damaged whenever they play that backup in the DVD, this is what they will see at the very beginning. I believe Rubin talked about some previews that he had to sit through for 14 minutes.

MR. SAFIR: Fourteen minutes of previews every time you got stuck.

MR. MOORE: That technology is actually controlled in the IFO files of the DVD. While we don't address that particular issue that Rubin brought up, we use that same technology to force the user to see this disclaimer. So this is an eight second disclaimer that appears on the screen. Our reasoning behind this is that no one is going to make a backup
copy of a DVD and try to pass it off as original. It's going to be quite obvious to the casual observer when they put the backup in, that it's a backup copy indeed.

What's more, DVD X Copy does not store any content on the user's hard drive. The data goes to temporary memory and is erased after the copy is made. Backup copies are programmed to prevent serial copying. In other words, we put bit flags on the backup copies to prevent a copy being made of a copy. We are steadfastly despite what the MPAA or anyone else may believe in favor of the copyright holder's rights and the consumer digital rights.

We are against copyright misuse. We do not want the public to suffer from the limitations of the DVDs they lawfully acquire. At the same time we don't want our software being exploited by copyright pirates. We believe in bona fides of our customers. We do not believe that the average lawful consumer, a consumer who has paid for the purchase of a DVD, intends to make dozens, hundreds or thousands of copies of DVDs using our software. No one has ever shown that to be the case.

And to put our money where our morality is, we go even further. Last winter, we announced a
reward program, announcing that we would pay up to $10,000 to anyone who provided testimony that led to the conviction of any user using our software for copyright abuse. So far, no one has come forward claiming that reward. However I should point out that we have received many tips of DVD piracy that have nothing to do with our software. We have forwarded those tips on to the appropriate authorities.

In conclusion, in the California litigation, we are fighting for our principles and our business life. We asked the Copyright Office to enunciate a clear concise statement that those who lawfully acquire DVDs should be exempt from liability when they repair or make backup copies for their own personal use.

Consumers who are spending billions of dollars buying DVDs and have created this market should be allowed to protect their investment without resorting to the demands by distributors to repurchase the DVD that later goes bad or is no longer available. This market would not exist if it were not for the consumer. Consumers should also be allowed to take the backup copy of a lawfully acquired DVD and purchased DVD and use it where they choose to, in their car, on a boat, upstairs at a home, at a country
retreat, when they are camping, as long as the payments were made and it's a fair use, the Librarian should sanction that process. I look forward to potentially answering any question.

CHAIRPERSON PETERS: Thank you, Mr. Moore. Dr. Einhorn, you're next.

DR. EINHORN: Thank you very much. My name is Michael Einhorn. I'm speaking on behalf of myself. In course of this discussion, I'm primarily speaking as a professional economist. I'm not necessarily a proponent or an opponent of any exemption. I do not dispute legitimacy of regional coding nor any anti-circumvention rules to Section 1201(a).

I've been asked to speak primarily on the topic of regional coding and confine my remarks exclusively to that area. I will try to the best of ability to keep my remarks within the scientific domain of my profession.

I believe first and foremost that the economic reasoning is an essential way of viewing problems. It is appropriately integrated into law to facilitate the policymaking process. Insofar as I know, the most sophisticated use of law in the past 50 years has emerged at least in regard to economic
matters in the anti-trust area where economic insights have affected both the statutory and the common law. That kind of analysis began in the distinguished halls of the University of Chicago Law School which Mr. Attaway is an alum.

What I want to do today is confine myself to the area of consumer benefits and consumer costs and discuss all of these from an economic perspective. I'll leave it up to you to decide where the chips have to fall. I would distinguish that there are three consumer benefits toward facilitating — Before I say that, I should say that all the effects here may be quite small after all Section 1201(a)(2) is in effect. I do not advocate a repeal of that section.

We therefore have a way of controlling any device that can be used to circumvent any technology. Therefore what we are talking about primarily is the ability of certain talented individuals — I am not one — who have the capacity to hack through certain protections on DVDs wherever they buy it. We understand therefore that we're talking about only that limited class use and confine our remarks to that particular area of the market.

Three consumer benefits that can rise from regional coding or the ability to defeat regional
coding, first of all would be new material. A certain consumer may find they are able to get new material in one part of the world that would be much more difficult to get in another part of the world.

For example, an opera lover who lives in Cleveland, Ohio may go to Milan and find her favorite record store. If she does, she may come back with a bunch of DVDs outfitted from all kinds of operatic performances around the world. Some of them may be from the Metropolitan Opera in New York. Those presumably were protected by DVD protection. If she brings them back to Cleveland and she has the ability to hack, she would not be able to do so if this were made illegal.

The second matter is the re-outfitting costs. A person who spends one or two years overseas perhaps in Europe, perhaps on a military base may acquire a substantial DVD collection. If they do come back to U.S., they may have invested thousands of dollars in a DVD collection. They may find themselves in a position where they enjoy some other movies.

They now have to make the decision of what to do next. Should they throw out their old DVDs and buy a whole new set or should they buy a bunch of different regional coding or DVD devices that have
different regional coding practices or if they can, can they hack?

Third is shopping over the border. There are some Americans who have the capacity to shop for DVDs over the border. They will indulge or they will practice what is known as "price arbitrage." They will go to where the prices are cheaper and they will buy DVDs at lower costs.

Each of these practices may do some harm to the content industry. It's after all quite possible for our shopper in Cleveland instead of going to Milan to buy her favorite DVD to contact the Metropolitan Opera and buy stuff through the mail immediately. That certainly is the way she can handle things. Someone who has quite an elaborate DVD collection after two years of being on a military base certainly could come back to the United States and outfit themselves with an entirely different new DVD player. They can bring back a second appliance. That certainly is possible.

In both of those cases, I would say as an economist that there's a bit of a difficulty there. We're putting on some kind of cost on consumers. I'm trying to figure out where would be the opposing gain other than raising some kind of barrier.
In regards to the third element, I'm much more agnostic and much more careful. That is there will be some people who will shop over the border. It is entirely conceivable that people living in Los Angeles or better yet, San Diego, will drive a short distance to go to Tijuana. If they do, they will be able to get their hands on conceivably cheaper DVDs.

As far as I'm concerned, this is where the nub of the problem may be. It may be we have to decide the likelihood for these groups of individuals, these groups of international shoppers, to what degree we are permitted or are going to permit them to do this bearing in mind of course that there may be other consumer gains.

I will point out though that according to what I read regarding your previous rulemaking, you said that you are interested in knowing about the ways of diminishing the ability of individuals to use copyrighted works in ways that are otherwise lawful. Like it or not, these ways are otherwise lawful. It is now legal for example for an American to go over to Mexico and buy a video cassette that may be coded for Mexico and bringing it back to the U.S. and then use it in the U.S. Up to this point, the manner in which people do these things, what I'll call "international
price arbitrage" is in fact lawful. If you want to continue to use that definition of otherwise lawful, you put it in the context that you think is appropriate.

The one point where I also wanted to devote some time to and concluding my remarks is a concept of what is called digital piracy. I'd much rather call this by a scientific name and that name is unauthorized reproduction and distribution of copyrighted content. What I mean here primarily is the ability to put stuff up on the Internet for file sharing systems that facilitate the use by consumers who have not paid for it. I'm entirely aware that certain individuals in this country or for that matter in this world feel it is their moral responsibility to distribute copyright content without the permission of their owner.

To the mind of some, we have what we call life, liberty and pursuit of free content or life, liberty and the right of redistribute free content. I don't believe in that group and I want to distance myself from anything they have to say.

I will make the following comment about their behavior though. It is entirely possible however inappropriate their behavior may be that the
relaxation of rules on regional coding will have nothing to do with it. If they are so determined to put up free material on DVDs and they have the ability to hack it, what they can do is go down to any video store, get a bunch of DVDs and bring them home or they can buy the DVDs. They then given their abilities to hack can hack the DVD protection or the content protection on anything they can bring within the house.

It is unclear to me personally whether regional coding or the ability to defeat regional coding will do much in changing around the behavior of this element. While I don't support what they do, I question whether we'll have much incremental effect on their behavior which is based upon a much wider domain of content than merely DVDs that are brought over the border. Thank you.

CHAIRPERSON PETERS: Thank you. Let's go to Mr. Turnbull.

MR. TURNBULL: Good morning. I'm Bruce Turnbull of the law firm of Weil, Gotshal & Manges. I'm pleased to be here today representing the DVD Copy Control Association ("DVD CCA"). I appreciate the opportunity to present DVD CCA's views at this hearing.
By way of background, DVD CCA is the not-for-profit corporation that is the licensor of the Contents Scramble System ("CSS"). DVD CCA licenses this technology on a royalty-free basis principally to three types of licensees: (1) owners of video content desiring to use CSS to protect their content on prerecorded DVD video disks; (2) to creators of encryption engines and hardware and software decryptors; and (3) to manufacturers of DVD players and DVD-ROM drives.

CSS was developed to protect against unauthorized access to and use of copyrighted motion picture content prerecorded onto DVD disks. CSS accomplishes this by conditioning the license for the technology and information necessary to decrypt the CSS encrypted content on compliance with certain rules for the use of such content. Thus, consumer access to the content is effectively conditioned on the use of products that are designed to protect against misuse of the content once decrypted.

In relation to this proceeding, DVD CCA believes that little has changed since the 2000 proceeding and that the analysis and conclusions from that proceeding continue to be valid in relation to CSS encrypted DVD video content. Accordingly we urge
rejection of all requests for exemption from 1201(a)(1) that relate to CSS encrypted DVD video content.

Specifically the following points from 2000 proceeding should guide the analysis and findings in this proceeding:

(1) Circumvention for a particular purpose including fair use or reverse engineering in order to achieve interoperability are beyond the scope of the rulemaking.

(2) In relation to the argument that CSS as an access control measure frustrates the consumer's ability to circumvent use controls associated with the work, the Register described the allegations of harm in 2000 as a failure to demonstrate actual harm.

(3) Circumvention of copy controls could be distinguished from circumventing access controls. That is the circumvention of copy controls an act not prohibited by the DMCA would not thwarted by the maintenance of a prohibition on circumventing CSS as an access control.

(4) In relation to the argument that an exemption is necessary in order to permit Linux users to play CSS encrypted DVD video disks, the Register stated "There is no unqualified right to access works
on any particular machine or device of the user's choosing." Quoting again, "The reasonable availability of alternative operating systems or dedicated players for television suggest that the problem is one of preference or inconvenience and leads to the conclusion that an exemption is not warranted."

(5) Region coding "serves legitimate purposes and encourages distribution and availability of digital audio-visual works" and any alleged effect of region coding on DVD video disks was de minimis. Those were all from the 2000 proceeding.

Today not only are these same conclusions still valid but the development of the market has only underscored the fact that CSS has enabled the vast expansion of content available to consumers on DVD video disks. In response to consumer's enthusiasm for the format, content owners have released more and more high value content on DVD. This happy situation is directly attributable to CSS and the assurances that its legal and technical regime provide to content owners that their works will be protected from unauthorized access, copying and redistribution.

The continuation of this immensely successful format depends on the continued viability
of this CSS legal and technical regime which must include the rejection of requests for legal permission to circumvent CSS.

Turning to specific requests in this proceeding.

(1) Requests for exemption based on a definition of a class of works that is tied to the proffered use to be made of the work remain beyond the scope of this proceeding. DVD CCA believes the lengthy and careful analysis made in the 2000 proceeding drew the correct conclusion in that regard.

(2) Requests for exemption of CSS encrypted works generally where the class of work is defined either as a CSS encrypted DVD video disk or encrypted works or the equivalent should be rejected fundamentally because they effectively request the elimination of Section 1201(a)(1) entirely.

Clearly Congress did not intend that the value of a technological measure effectively controlling access to a work should be totally wiped out by exempting all works protected by that technological measure. Nor that encryption would be eliminated as an access control technology through a broad-based exemption for all encrypted works. In this case, CSS-enabled products are widely available
at reasonable prices adapted for both traditional CE uses and computer uses. A general exemption is unnecessary in order to provide easy and universal access to the works protected using CSS.

With regard to the request to exempt circumvention of CSS encrypted works for the purpose of enabling the playback of such works using a computer with a Linux operating system, we reiterate what we said in 2000.

(1) There is nothing in the CSS license or requirements that limits its application in relation to Linux and nothing preventing a person desiring to make a Linux enabled CSS application from obtaining a CSS license and adhering to the requirements of that license and the CSS specifications. CSS as I said is licensed from a royalty-free, reasonable and non-discriminatory basis without regard to the operating system to be used in the product on which the CSS implementation is loaded.

(2) There is nothing in the Linux license that prevents a person from complying with both the CSS license and the Linux license as well. In that regard, we note that the founder of the Linux system, Linus Torvald, has in just this past week stated his agreement with this precise point.
MR. SAFIR: No, he didn't. That's a lie. But that's okay. I know that's a lie. You are now perjuring yourself. Why don't you give them the article so they can actually read it?

CHAIRPERSON PETERS: Stop. Let him finish.

MR. TURNBULL: I will be happy to engage on that subject. I do in fact have his posting with me and will happy to engage in that.

CHAIRPERSON PETERS: Thank you.

MR. TURNBULL: Although DVD CCA does not require its licensees to inform us of what operating system they are using for their implementations and indeed we do not gather that information on a regular matter, we are aware of two Linux-based CSS implementations that have been made by licensees. We believe that one of these is still in the market today.

(3) With respect to requests for exemption to permit playback of non-Region I encoded DVD disks on CSS enabled Region I players, we note several points. As found in the 2000 proceeding, the Region code system is a reasonable and proper exercise of the distribution rights of copyright holders.

Accordingly the requester of an exemption
must bear the burden of demonstrating harm beyond the
deminimis level as well as the demonstrating that
there is no reasonable, available alternative cure for
the alleged harm other than the requested exemption.
We believe that no request has demonstrated any actual
harm to any user especially given that there are
alternative means of responding other than granting an
exemption.

Specifically in relationship to the
alternatives available, we note that there are no CSS
license or other prohibitions that we're aware of on
the sale, importation or use in the United States of
a non-Region I playback product. A consumer can
obtain whether in the United States through an
Internet retailer or abroad, a non-Region I playback
device and then use that device in the United States.

For example, a consumer can directly set
the region playback setting for a DVD-ROM drive to
playback whatever region that user wishes including
for example Region II content. Drives that enable
this capability are permitted under the CSS rules and
it is DVD CCA's understanding that many if not all
DVD-ROM drives in fact enable such direct user
selection of the region for the particular drive.

Indeed a quick survey of the retail market
shows that the DVD-ROM drives are available for as little as $19.95, hardly a hardship. Hence the exemption is simply not necessary for the de minimis number of consumers who desire to playback non-Region I content in legitimate compliant CSS playback system.

Finally in relation to region coding, the specific technology that would require circumventing in order to avoid a CSS licensed DVD playback systems region code system is not in fact the CSS encryption itself. While the overall CSS system requires that region code playback be incorporated into the playback system and further imposes certain standards which we call robustness requirements on licensees and implementations of the region code detection and response requirements, the actual technology that would need to be circumvented in order to feed to region code system is not CSS encryption but rather a range of implementations that are based on each licensees own selection of technology. Thus the technology to be circumvented would have to be determined on a producer by producer, product by produce basis.

(4) We believe that two additional requests are not proper subjects for exemption through this proceeding, request for exemption to facilitate
research relating to access control technologies and
requests for exemptions to permit access to public
domain content.

The request for exemption related to
research on access control technologies which are
questionable based on the definition of class of works
as noted earlier should be denied because Congress
provided a specific exemption for research purpose and
did not in that exemption permit the Librarian through
this proceeding or otherwise to modify or extend that
statutory exemption. The requester should properly
address their pleas to Congress.

As to public domain works as we stated in
our written comments, DVD CCA is not aware of any
particular work that is protected using CSS where the
work would be considered public domain. Accordingly
no demonstration had been made that an exemption is
warranted. Even if there were examples however it
would seem that the request would be outside the
request of this proceeding since the authority is
limited to defining a "particular class of copyrighted
works." By definition the public domain works would
fall outside of any class of copyrighted works.

Finally DVD CCA takes no position on the
request to exempt circumvention works where
unskippable advertising was included on the DVD disk
but requests that there would be no recommendation to
permit an exemption of CSS to accomplish this because
CSS has nothing to do whatsoever either
technologically or legally with this aspect of the
playback of DVD video disks. Thank you for this
opportunity. I'll happy to respond to questions.

CHAIRPERSON PETERS: Thank you very much.

Ms. Perlmutter.

MS. PERLMUTTER: Thank you for the
opportunity in order to testify today. I won't take
up the time we have available this morning by
repeating the content of our written reply comments
which go into much more detail. I'll just say a few
words about the context and the potential impact of
this proceeding. Then I hope to be able to discuss
specifc more in the question period.

During the last rulemaking what was then
Time Warner testified on many of these same issues
that are presented here today. We said then that
digital technology creates a need for the use of
technological measures to protect copyrighted works
plus a need for effective legal protection against
circumvention. That of course is what the DMCA gave
us in 1989.
We also said that carve-outs from that protection could jeopardize the ability of copyright owners to provide works to the public in digital formats. We also said at that time that new formats were emerging and already popular, for example, DVDs, which give consumers high quality and richer content choices. Finally we said that there had been no substantial proof brought to the Office's attention that any harm to lawful uses was likely. Rather we were hearing a lot of fear and speculation about negative possibilities, things that might at some point result.

What's happened since the last rulemaking? First of all, 1201(a)(1) has now been enforced for two and a half years. So unlike the last time, we now have some experience with the actual application of the access control part of the statute. We have now had some more definitive judicial interpretation, not only the ElcomSoft case but the Second Circuit's decision in Universal versus Corley.

We have seen an explosive growth in the DVD market and a significant decrease in prices to consumers for purchasing copies of movies as well as for purchasing the players to watch them on. We have seen a myriad of new and exciting offerings to
beginning to emerge for digital content.

We have now emerging on the market legitimate on-line music services which include MusicNet on AOL, a new Apple music service that was just announced this week. These various services give consumers a number of different options for how to enjoy music including streaming, downloading singles and even the burning of CDs.

We have also seen the development of legitimate on-line movie services, MovieLink, and other audio-visual services like Digital Video-on-Demand, both of which have the enormous benefit from my personal perspective of eliminating the trip to the rental store. So you have the opportunity to enjoy a movie for a 24 hour period without having to leave your home.

We have seen still no substantial evidence of harm. Technological protection measures are not beginning to block access. The copyright holders are interested in getting their works out to the public to as many members of the public as possible in as many ways as possible. In fact, technological protection measures are being used to enable more diverse types of access to more works and at different price points.

In a word, there is not only no reason to
reach different conclusions than in the first rulemaking. But in fact we're seeing a success story here. The goal of the DMCA is beginning to be realized already. The trend toward more diverse and more flexible business models shouldn't be endangered by the adoption of far-reaching new exemptions.

Just a few words about the current requests for exemptions, the purpose of this rulemaking of course is as a safety valve to ensure the continued survival of fair use and other public interest exemptions within the framework of the statutory policies that are embodied in Section 1201. We wholeheartedly support that purpose. We rely in fact in all of our businesses every day on a thriving fair use doctrine.

But I think it's important to note that the term "fair use" is often used very loosely to encompass a number of different activities which range on the one hand from creative transformative uses to news reporting to classroom photocopying to home copying. Often we hear the term "fair use" used based on an inaccurate assumption that any personal use by any consumer is necessarily a "fair use."

Our concern is that while many of these current requests for exemptions are couched with
greater specificity than the last rulemaking, when you look at what they ask in reality they are far-reaching indeed. Many of them challenge the fundamental policies that Congress adopted in the DMCA and even some of the basic principles underlying Copyright law neither of which is a proper subject for this particular proceeding.

Copyright owners have always had the ability to decide whether and how their works would be distributed to the public. It would be not only ironic but detrimental to consumers if the new possibilities for methods of distribution that are offered by DRM Technologies were hobbled by unrealistic insistence on an Old World "all or nothing" approach.

In particular, many of the requests boil down to the argument that once a copy of a work has lawfully been purchased, the purchaser must be free to make any desired use of the content whatsoever, short of redistributing copies to others on a commercial scale. These uses could range from the enjoyment of the work on any platform, in any format and in any place or any country to the extraction of portions of the work using the user's preferred technique.

The problem with this argument is first
that it takes away the traditional ability of the copyright owner to control the manner of distribution and with it much of the incentive to develop new formats and new market offerings. But equally important, it destroys the economic feasibility of providing a range of diverse offerings at different prices. Works would only be able to be available at the comparatively high price of a permanent physical copy.

In terms of the factors the Librarian is directed to consider by the statute, what we see now is that the use of technological protection measures protected against circumvention by the DMCA has lead to the increase availability of more works in different formats. There is no substantial evidence those works are still not available for public interest purposes such as both the core transformative types of fair use and other types of fair use as well. The effect of circumvention on the market for copyrighted works and the openness of their owners to make them available in digital formats is great indeed.

So in sum, the worst case scenario envisioned by those seeking cutbacks to the DMCA's protection in 1998 and in 2000 has fortunately not
come to pass. There is no evidence that copyright owners have imposed access controls on entertainment products in unreasonable ways that adversely affect the ability of users who engage in non-infringing uses. Just to conclude the continued effective protection of the DMCA is key to allow the on-going development of new offerings that benefit both consumers and copyright owners. Thank you.

CHAIRPERSON PETERS: Thank you. Mr. Attaway.

MR. ATTAWAY: Thank you, Ms. Peters and distinguished panel. I appreciate the opportunity to appear before you today. I'd also like to thank Mr. Einhorn for being the first speaker this morning not to call into question my honesty, integrity or linage.

I would like to do a little demonstration today. I assume that the written summary that I submitted early will be part of the record so I won't go through all of that. What I would like to do is do a little demonstration on what is fair use. Kelly, are you ahead of me?

The purpose of this proceeding as you pointed out earlier is to determine whether persons who are users of copyrighted works are or are likely to be adversely affected in their ability to make non-
infringing uses. Most non-infringing uses are either licensed authorized uses or fair uses.

Fair uses according to Section 107 of the Copyright Act includes such things as reproduction for purposes such as criticism, comment, news reporting, teaching, scholarship or research. I note that it does not mention backup copies. So far as I know, no court has ever said that fair use encompasses the making of backup copies. Indeed if it did, there would have been no reason to adopt Section 117 of the Copyright Act which specifically allows the making of backup copies under certain circumstances of computer programs.

So with that introduction, I ask my colleague, Kelly O'Connell to pretend she was a student at Fairfax High School making a report on "Spider-Man." In this multi-media report, she needed a short excerpt from "Spider-Man" to make a point that she wanted to make in her report which would probably be a fair use as defined by the Copyright Act.

So I asked her to take her video camera which is not professional equipment. Most people have video cameras like this and I asked her to simply make an excerpt from "Spider-Man" a legitimately acquired copy of "Spider-Man" that is protected by CSS against
copying. I asked her to make an excerpt without
circumventing CSS. First of all, Kelly, you are going
to play the authorized DVD with sound. Then maybe not
with sound. There we go.

(DVD played.)

MR. ATTAWAY: Okay, I don't want to go
beyond our fair use of a small excerpt so let's stop
this and play the fair use excerpt recorded by this
video camera.

MS. O'CONNELL: It crashed.

MR. ATTAWAY: Oh, no.

MR. SAFIR: Gee whiz. I can't imagine.

Maybe you can get your DVD player to work -- Let me
see if there is anyone with a free operating system
here. That's right. There's no DVD with free
operating systems. Sorry. I guess we'll have to wait
for Windows. It will take 20 minutes here.

MR. ATTAWAY: Am I the witness or is he?

CHAIRPERSON PETERS: You're the witness.

MR. ATTAWAY: Thank you. Well, had the
computer not crashed you would have seen not a perfect
copy by any means but certainly a reasonably viewable
copy that would have served the purposes of criticism,
comment, news reporting, teaching, scholarship or
research. I submit to you that virtually any excerpts
of audio-visual work that is capable of being displayed on a computer screen can be copied for fair use purposes and there is no need to have an exception for -- Excuse me.

CHAIRPERSON PETERS: I was going to ask you if we wanted to take the time. Kelly, how much time do you think it would take to reboot it?

MS. O'CONNELL: It's working right now.

CHAIRPERSON PETERS: Because one of the things we could do is stop you here and go to Mr. Mitchell and then come back.

MR. ATTAWAY: All right. You can do that. I'd like to make one other point while I have the stage here.

CHAIRPERSON PETERS: Certainly.

MR. ATTAWAY: It occurred to me during the testimony of the first speaker that there might be an explanation for the total disconnect there seems to be between the people represented by New Yorkers for Fair Use and the Copyright community. That disconnect is illustrated by this statement "Technology is making information extremely inexpensive." That simply is not true.

The type of information we're talking about here today, movies and sound recordings, is
probably more expensive today than it ever has been before. A motion picture made by a major studio costs $70 million to produce and another $20 or $30 million to market. They are extremely expensive. What has become inexpensive is the ability to disseminate those works. That's a great thing for consumers.

But if you cut off the economic foundation for any of these creative industries whether it be movies or textbooks or sound recordings or anything else you cut off creation. That would create a very bleak world indeed when information might be easy to disseminate but no new information would be created.

CHAIRPERSON PETERS: Why don't we go to you, Mr. Mitchell? And, Fritz, we'll come back to you.

MR. MITCHELL: Madam Register and distinguished panel, it is a privilege to testify before you here today. The Interactive Digital Software Association represents publishers of entertainment software who produce works for play on personal computers, dedicated video game consoles, hand-held devices and for play directly on the Internet.

Our member publishers have been pioneers in using the Internet to deliver content and unique
game experiences under a variety of terms that consumers have shown that they are more than eager to accept. We have also been among the leaders in using technology to protect our works from piracy. Virtually all video game consoles employ TPMs in hardware and software to prevent the proliferation of pirated copies. Despite these efforts, the entertainment software industry remains plagued by piracy and indications are that it can be dramatically worse percentage wise in countries that have failed to provide strong legal protections for TPMs.

In short, there is no need for any exemptions to Section 1201(a)(1)(a)'s prohibitions on circumvention of TPMs for any type of entertainment software. We do not believe the proponents of any exemption have met their burden. Even if they had, the exemptions proposed could bring real harm to this industry without significantly increasing the availability of entertainment software to the American public.

Our theme for you here today is that in thinking about potential exemptions of Section 1201(a)(1)(a)'s otherwise clear prohibition, we would ask you to consider not only how such an exemption would be used but also how easily it could be misused.
We've spoken to you on a number of occasions about the most notorious example of this and I know I'm going to get some eye rolling from you on this because we have had a chance to discuss it with you in such depth.

But we're talking here about pirates use of the so-called Section 117 disclaimer. Literally thousands of pirate websites continue to carry elaborate disclaimers purporting to show why downloading software from the site is not infringement but a permissible use of Section 117 to make archival or so-called backup copies.

Habitual misuse of the provision has created considerable confusion even among those not otherwise inclined to break the law. These self-serving interpretations have unfortunately displaced reality for an alarming number of video game enthusiasts.

Recognition of this tendency we think should have a direct bearing on this rulemaking as well. It provides an additional compelling reason for you to continue as you have done to hold proponents strictly to their burden of proof and to create exemptions only for substantial and tangible reasons. It should also follow of course that any resulting exemption should be drafted narrowly, clearly and
carefully to avoid inviting abuse.

There is one more procedural point that I'd like to make. It's one that is made most forcefully on our behalf in the Joint Reply Comments at page 28 of that voluminous document. We would suggest that any exemption you may contemplate for entertainment software should not simply be carried over to entertainment software because of the incidental fact that much of it is published in a DVD format or because of the other incidental fact that entertainment software consoles, some of the leading consoles, can be used to play DVD movies. No exemption for entertainment software whether in the form of computer games, console games, hand-held games or on-line games should be recognized without an independent basis on the record demonstrating why such an exemption is required.

Now as to the specific requests for exemptions that potentially implicate entertainment software products, we do not believe that any of the proponents have satisfied their burdens. One of the very few references specifically to video games in which proponents allege even a potential adverse effect on the availability material concerns, some console publishers reliance on TPMs to enforce
regional coding in video games.

It is suggested that regional coding in such circumstances can prevent a game enthusiast from playing certain games purchased in Europe or Japan on video game consoles sold in the U.S. We suggest that whatever deprivation that may result is isolated, de minimis and easily remedied short of cutting deep into 1201(a)(1)(a).

There is no shortage of computer and video game releases in the United States. More than 1800 new titles have been released just since the end of the last rulemaking cycle, a period which also saw the successful launch of three new console platforms, new handheld platforms and the emergence of an entirely new genre of on-line console games. Many successful titles received release across all regions. Though some others for cultural marketing and legal reasons may only be released in one or two.

Occasionally a U.S. video game collector or an officio nardo may wish to acquire a version of a game produced for the European or the Japanese market. In the case of titles released first in another region, some may not want to wait a few weeks or perhaps a few months for a title's eventual U.S. release. But this we would posit is an inconvenience,
not a harm sufficient to justify an exemption.

With the healthy growth of international Internet commerce, even the most esoteric demands for video games can easily be met. The very same channels through which a collector might legitimately purchase an import game also give him or her the ability to acquire an appropriately coded console on which to play them, a remedy vastly more preferable than allowing someone to take circumvention into their own hands. These options are even more widely available today at lower prices than they were in 2000. Clearly the argument for exemptions to satisfy these needs is weaker now than it was three years ago.

During the 2000 rulemaking cycle when considering regional coding of filmed entertainment on DVD, you were very careful to examine any potential harm along with the positive use facilitating purposes underlying region coding practices. In 2000 for example, you found that region coding served legitimate purposes as an access control and that it encouraged distribution and availability of digital works by preserving market opportunities for U.S. distributors.

Region coding for the video game industry serves the same constructive purposes as well as many
others, ones that we pointed out in greater detail in our IDSA initial reply filing of February 19\textsuperscript{th} at page three in three bullets there. For the video game industry, region coding is used to enhance consumer enjoyment of regionalized language appropriate video game products. It also serves to preserve local distributor marketing opportunities. Ultimately, an undeniably use-facilitating regional coding makes it possible for publishers to offer products that might not otherwise be made available at all.

Publishers are often able to acquire properties subject to licensing restrictions that may allow them, for example, to use content, characters, music or advertising in some regions but not in others. With the ability to use TPMs to respect these limitations, these licensing opportunities and the resulting public distribution of these games might be severely curtailed or become altogether impractical but for the ability of them to be restricted by the publisher using TPMs.

In assessing the need for a given exemption, we would ask that you place considerable weight not only the use facilitating nature of the technology at issue but at also on the potential piratical uses of any resulting exemption. We are
asking that you specifically inquire as a discrete part of your analysis how a given exemption can be misused to facilitate piracy. Whereas the video game industry's region coding technology passes the use facilitating process, we believe that any proposed exemption would fail this piracy facilitation test.

Creating an exemption to permit circumvention of region coding would, we are convinced, affirmatively contribute to piracy. It would make enforcement against circumvention and circumvention devices significantly more difficult. It would also create considerable confusion around the operation of an otherwise relatively clear rule. Confusion and ambiguity we have already seen pirates play to their advantage in these other context.

Any exemption even one clearly restricted to acts of circumvention would undoubtedly be understood by the pirate community as a legalization of mod chips, game enhancers, game copiers and the many other circumvention devices that are commonly used to circumvent TPMs in video game consoles. As counterintuitive as this may seem to those of us who know better, I ask you to reflect for a moment on how much pro-piracy mileage the video game pirates have been able to get out of Section 117.
Finally, I'll mention briefly that Static Control has asked for the creation of three exemption all seemingly aimed at avoiding difficulties it currently faces in producing printer components. We address its proposals in detail in a second reply we filed on March 10, 2003.

To summarize very briefly while we offer no comment on the first proposed class, we do take issue with the second and third classes proposed there. These proposals are totally unnecessary to address any problem that this company believes it is encountering from the operation of the DMCA. But those exemptions if granted risk significant unanticipated impacts on current video game technology as well as other industries who are just beginning to explore the beneficial uses of embedded software.

We truly appreciate the care with which the Copyright Office, the NTIA and the Librarian have administered these proceedings and the proceedings in 2000. To summarize, we believe that no compelling factual case has been made for any exemptions in the entertainment software space. Region coding is use facilitating and any exemption allowing its circumvention would contribute directly to further piracy.
The video game industry has done well to integrate technology into products under conditions that consumers find not only acceptable but so deeply satisfying as to make video and computer games the fastest growing entertainment industry segment in the world and one of America's premier high technology success stories of the last decade. There has been no demonstrated need to create exemptions to these rules now or for in the foreseeable future and certainly not within the next three year cycle. Thank you very much.

CHAIRPERSON PETERS: Thank you. Mr. Attaway, are you ready to resume?

MR. ATTAWAY: We'll find out.

CHAIRPERSON PETERS: We'll test technology.

(DVD copy played.)

MR. ATTAWAY: All right. While you are watching this, I will just point out the obvious that it's not as good as the original DVD. I certainly wouldn't assert that. I do maintain though that it is good enough for the purposes that fair use is intended to serve. It probably could have been better by the use of better equipment but employees of MPAA typically can't afford the latest in video cameras so
this was the best that Kelly could do.

Can you do the final screen shot? The last point I want to make is this quote from the Second Circuit in the Reimerdes case where it said "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 the identical format of the original." Thank you very much. I appreciate this opportunity to testify.

CHAIRPERSON PETERS: Thank you. Because we've been sitting for some time, some people may have certain needs. It could be coffee. We will take a 15 minute break and resume at 11:25 a.m. or shortly thereafter. Off the record.

(Whereupon, the foregoing matter went off the record at 11:12 a.m. and went back on the record at 11:24 a.m.)

CHAIRPERSON PETERS: Back on the record. We do have another panel this afternoon. So we do have limited time. We'll be asking questions of specific witnesses. We beg you to be as concise as possible.

I also want to point out that we're very well aware of the differences of opinion between the members of the panel. This is not an opportunity to
totally debate each other. We're really just looking for the answers to our questions. I'm going to start the questions with David Carson.

MR. CARSON: All right. First of all, if I recall correctly, one of the things we said in 2000 when we were addressing requests that we exempt audio-visual works on DVDs was that the availability of essentially all motion pictures released on DVD also in VHS format was one reason why we saw no problem because whatever people were saying they couldn't do with DVDs, they could certainly do with VHS tapes. That was part of the analysis that we engaged in as I recall. Here is my question. Have things changed in that respect and if they have changed or if they are going to be changing in the next three years, how does that alter the analysis? This one is actually for anyone.

MR. TURNBULL: Perhaps the people who actually put out the content can answer on the question of what's available in each format. I would just say that I think one other point that was made in the 2000 that's directly relevant to this and I commented in my opening statement on it is that the difference between the access control and the use control technologies is such that the use control
which was in the 2000 is the same for both DVD movies and VHS in the use of the Macrovision technology.

In terms of defeating the use control, the same issue arises whether you release the content in VHS or DVD. I think the analysis that was done in 2000 is still valid on that point.

MR. ATTAWAY: I hope that I demonstrated that even if a movie is not available in VHS or any other format that a movie on a DVD one can make fair use of it simply by taking screen shots. You don't need VHS.

MR. CARSON: Can you confirm what I read in the press and what my own personal experience seems to tell me? VHS is essentially a dying format, isn't it? Is that an overstatement?

MR. ATTAWAY: Well, I'm the eternal optimist and I'm still hoping my 8-track will have a use in the future. But I don't know, Mr. Carson. I'm not in the marketing business so I just can't express an opinion on that.

MR. CARSON: Can you add anything, Shira?

MS. PERLMUTTER: Yes, just to say, it may be that in the long term consumers are so much happier with DVDs that it will become the dominant or only format at some point. But that's not true today and
not going to happen in the next couple of years as far as I can see.

So as long as that's still not the case obviously it's very easy to say that there is another format out there that can be used in other ways. Although as Bruce pointed out, you still have copy control measures involved. But as Fritz said, there is still the ability to get access with DVDs and there's still the ability to use fair use. It's just an additional factor in the mix.

MR. CARSON: Mr. Turnbull, you said something that I just wanted to follow up on and get your thoughts on it. If anyone else has any other information on it, I would like to get that as well. If I understand correctly, you said that assuming that there's a legitimate reason to circumvent a region code. We're not talking about circumventing CSS. We're talking about circumventing something else. I wonder if you can just elaborate and explain it to me.

Let's assume for the moment that we are sold that people ought to be able to circumvent whatever they need to circumvent in order to deal with the region code issue. It's your job right now to tell me why we shouldn't say you can circumvent CSS and what it is we should say that you can circumvent.
Not that you're an advocate for that and not that I'm even an advocate for that. I want to know what it is that we're being asked. If we wanted to do that, what would it be that we would actually have to be saying?

MR. TURNBULL: The way the system works is that CSS encrypts the work. Once you have a licensed decryption of the work, the player or the software on the computer then looks for certain pieces of information that are lodged in particular bit setting in the decrypted content. One of these settings is the region code setting. It is not part of the encryption. It is a setting that is in the underlying work or the information accompanying the underlying work.

The requirement to look for that setting and the requirement then to respond to the setting is a license requirement for CSS but it is not part of the encryption that is CSS. But what CSS in licensing says is that the method for looking for the code and responding to the code and then in fact either playing or not depending on the settings and the configuration of the playback system is a matter for the individual implementation but it must be done as we put it robustly. It must be done in a way that is difficult to hack.
So if you have an XYZ playback system, that playback system may use something that is unique to it to both look for the code and also prevent somebody from defeating the region code playback. That's going to be different from the ABC Company's system or from the MNO Company's system. The requirement from the CSS license is simply that it must be done and it must be done in a way that is difficult to hack.

MR. CARSON: Now does one have to get past CSS somehow in order to tinker with those region code settings?

MR. TURNBULL: If you have access to the unencrypted content. All of this is done after the decryption takes place. So the question would be gaining access to that content. Again there are rules that relate to the circumstances of trying to prevent people from gaining access to the unencrypted content. Again those are done on an implementation by implementation basis.

So there are two different things. One is getting access to the content where the prevention of that must be robust. And then the region code detection and response system which again is done individually by the implementation must be done under
the rules in a robust way.

MR. CARSON: So if I understand you correctly and I'm not at all sure I do, if I were sitting at home trying to be able to do whatever I needed to do to play a Region II DVD, CSS would be totally irrelevant. The actual Content Scrambling System wouldn't be anything I'd have to deal with. I'm getting access to the material because I have a compliant player to start with anyway. After that whatever I'm doing may or may not be circumventing some kind of access control but it's not circumventing CSS.

MR. TURNBULL: CSS, the encryption, correct.

MR. CARSON: Okay. Well I have a glimmer of understanding. Thanks. Anyone else have any intelligence on that information.

MR. MOORE: Mr. Carson, actually I disagree with that. You actually must unlock the DVD and decrypt the contents in order to expose the region code. We know that from the backup software that we make. There is no way to get at the region code without first going through CSS.

MR. TURNBULL: I'm sorry. I didn't mean to say anything different from that. You do have to
decrypt the content. But once you have decrypted the content, that is when the region code detection occurs. And if you can gain access to the unencrypted content that has been unencrypted by a licensed legitimate system, then you don't need to hack the encryption system at all.

MR. CARSON: But how am I going to gain access to the unencrypted content?

MR. SAFIR: You can't. Just say you can't, which is the answer.

MR. CARSON: I asked Mr. Turnbull.

MR. TURNBULL: To take the computer system, the player is more complicated because you are opening a player and player manufacturers don't want you to do that. But in a computer where you have access to programming capabilities, there are buses, the interfaces, within the computer that the content travels on once it has been decrypted.

Quite frankly, the CSS license says that the licensed playback system should make it hard to gain access to the content when it's unencrypted and traveling on those buses from the point at which it's been decrypted to the point of which it's displayed. If you can gain access to that, you break through somebody's access control at that point in the system,
then you have the content in unencrypted form and you can do whatever you want to do with the region code setting.

MR. CARSON: Let's assume that the only thing you care about is CSS with that particular organization. Let's just assume that for the moment. For me to do what you just described, would I have to do what you would assert is a circumvention of CSS?

MR. TURNBULL: It's a little complicated because CSS is both the technology and also our license and the conditions on which the license is based.

MR. CARSON: All I care about is the technology.

MR. TURNBULL: Okay. If you are only talking about the technology to do what I just described, you don't have to do anything to CSS. You would be circumventing whatever the individual implementing software company has put in place to make it hard to get at the unencrypted content when it's being passed from the decryption point to the display.

MR. CARSON: Does anyone have a different understanding and want to explain?

MR. MOORE: That's definitely not true.

MR. SAFIR: That's not true.
MR. CARSON: Well right now I have someone giving me one explanation and I have two other people saying that's not true. That makes it real easy for me to decide, doesn't it?

MR. SAFIR: That's right. He's not telling the truth.

MR. CARSON: Explain to me why it's not true. First Mr. Moore. Then Mr. Safir.

MR. MOORE: I think he's trying to explain the underlying technology behind this. The end effect to the end user though is that you must unencrypt the data in order to get at the region code. There is no other way to do so. Period. That would be what they would interpret as a circumvention.

MR. CARSON: Is that true, Mr. Turnbull? You interpret that as circumvention.

MR. TURNBULL: You do have to unencrypt the content. This is the third time to say that. You do have to unencrypt the content in order to find the bit that says what region that particular disk is set for. Once you have unencrypted the content however, CSS, the technology, is no longer relevant to what is going on from that point to the point at which the content is displayed on the computer monitor.

So if you can gain access to the
unencrypted content breaking through whatever system
the individual software company has built, you can
then get at the region code. It may be easier to
defeat the CSS system as encryption technology and
never have to worry about these individual robust
implementations of content after CSS is removed. But
you don't have to.

MR. CARSON: So breaking CSS would be one
way of doing it but it's not the only way. Is that
what you are saying?

MR. TURNBULL: Correct.

MR. CARSON: Do you have something to add,
Mr. Safir?

MR. SAFIR: Yes, you have to break CSS to
get to the access codes in the encoded stuff. You
have an encoded envelope. In the encoded envelope, it
includes region coding. If you don't break the
envelope, then you can't get to the coding. You can't
get to the egg yolk until you break the shell. It's
really that simple.

Anything else he said is just mixing up
the fact of the question that you asked. Yes, you
have to gain access by -- By the way, he already broke
CSS code in order to gain access to the regional
coding scheme. That's a definite. I don't know why
he's using so many words to say otherwise.

This gentleman here who actually wrote a program that does similar things will confirm the actual fact of the science. This reminds me of showing the Shuttle explosion after all these scientists came over and said a lot of gibberish and the guy came over and says this is the problem. He takes liquid nitrogen. He drops the ring in. Then he drops the ring on the floor and it shatters. He says that's what happened to the Challenger. Then everybody said oh.

The answer to your question was a simple yes. You must break through the CSS encryption in order to get to the regional access key.

MR. CARSON: We may follow up in writing to try to get a more detailed explanation. This may not be the best means of getting useful information on the subject. You'll all have an opportunity to explain it to us in plain English.

CHAIRPERSON PETERS: Rob.

MR. KASUNIC: This question is geared to opponents of exemptions. There have been a number of statements that if there is an exemption found whether it's for region coding or for circumventing CSS that this will cause great harm to making works available.
Exactly what would that harm be? How harmful would it be for there to be an exemption to Section 1201(a)(1) in particular given the fact that this is mostly done in private, difficult to find out about, that there are very few people that would be technologically able to affect that circumvention? Also included in that, how many lawsuits or enforcements of circumvention of Section 1201(a)(1) are you aware of?

MR. ATTAWAY: If I may, I'll address the first question. I don't know that I know the answer to the second. To respond to the first question, just let me give you an example of regional coding. To me, regional coding is a marketing decision. A copyright owner decides what regions or what players he or she wants to market the work and makes a decision. Some owners of works will say I don't care. All players can play my content. Others will say no, I only want it to be played on Region I players or Region II players or so forth.

In the case of movie companies, we do it sequentially for marketing reasons. But it's basically a marketing decision just like some works are only available on VCD which is a format that is fairly widespread in Asia. I don't think it exists or anyone has VCD players at all in the United States.
So people who buy VCD audio-visual works if they bring it to the United States, there is nothing to play it on. That's just a fact of life. It's not a violation of any expectation of the buyer when he buys this work.

But getting back to my illustration, if a copyright owner decides not to market works that play on Region I players in the United States and there's demand for those works in the United States and if people in the United States have the ability to hack the region coding system, then there is less demand for the copyright owner to change his mind and decide that he ought to be marketing to Region I players. So the people that don't have the expertise or ability to hack are still out of luck. If there is no exemption that allows hacking and there is demand for that content in the U.S., then there is much greater economic incentive for that copyright owner to market his works on Region I players.

MR. KASUNIC: Mr. Turnbull.

MR. TURNBULL: If I could suggest two particular harms to your granting such an exemption. The first harm is I would reiterate what Mr. Mitchell said which is that you should look at the potential for the misuse of the exemption and the fact that it
will be very hard to keep the information within the confines of somebody's individual garage. So there would be tremendous potential for misuse of such an exemption.

The second is in relationship specifically to DVD CCA licenses, CSS as both a trade secret and a patented technology. Shortly after the DCSS program was created and disseminated, DVD CCA brought a trade secret misappropriation and misuse lawsuit in the California State Court.

One of the bases for maintaining a trade secret is that reverse engineering to obtain the trade secret was done in an improper way. One of the bases for it being improper is that it is a circumvention under the DMCA. If you were to grant an exemption to permit circumvention under the DMCA, we would lose that basis for the maintenance of the trade secrets that are underlied CSS. Now I hasten to add that we have other arguments and I'm not conceding anything in that case. But I do think that you would make it more difficult for us in maintaining the trade secrets.

MR. MITCHELL: For at least some dedicated video game platforms, the harm would come specifically from how such a circumvention is accomplished. In fact, the proponent of this very exemption has
suggested as much in his own submission when he acknowledged that indeed the easiest way to circumvent region coding is to essentially disable the legitimate copy verification process that also enforces other access controls to strip out all of the ability of a video game console to perform the checking between the hardware and the software. So it would result in drastically overbroad circumvention in that instance.

MR. KASUNIC: Well, let me follow up on that point in terms of what the potential misuse for an exemption that may be found. I've heard that both through Mr. Mitchell and Mr. Turnbull. I'm referring now to my handout that I gave you which is a reprint of Section 1201(a)(1). That specifically deals with what the class of works that's published, the effect of that exemption. Is your view of that Section 1201(a)(1)(D) that if we do find an exemption for a particular class of works that the exemption will apply only to non-infringing uses of a work after the circumvention is accomplished? Or would it be something broader that would also allow basically anyone to circumvent for any reason? Or something narrower if you read it that way? That's to anyone.

MR. SAFIR: I'm sorry. Could you repeat the question?
MR. MITCHELL: Is this provision which allows the Librarian to publish a particular class of works and states that non-infringing uses by persons who are users of a copyrighted work who are or are likely to be adversely affected and the prohibition contained in Subparagraph (a) "shall not apply to such users with respect to such class of works for the ensuing three year period"? In terms of misuse of the potential exemption if someone did misuse the exemption, would they still be liable under Section 1201 because they are not using it for non-infringing use?

MR. SAFIR: This is a legal question essentially.

MR. KASUNIC: Essentially yes.

MR. SAFIR: Because I can give you an opinion but it's just an opinion.

MR. GENGLER: I can take a shot at this one. I would say that since Section (D) here says that the use is to be non-infringing that if misuse of it is to be found non-infringing then it's still a violation of the anti-circumvention provision. In that case, it's still illegal and it's not covered by this. Only when the work is a non-infringing use is it exempted from this prohibition.
MR. KASUNIC: Are there any points of view from opponents of exemption?

MR. SAFIR: Can I just add something to that? When Congressman Ashcroft who is now the Attorney General was involved in writing up the DMCA originally, he said that he would not have voted for this or pushed this through Congress which was in his committee if it wasn't for the fair use provision that was later added which is now 1201. It's pretty clear that at least as he said in plain English and also as it seems to be the intent of Congress that use of any access breakage to the works which would then be used for a non-affording copyright infringing purpose would be in itself a violation of the DMCA.

In addition to that let's not forget that there's copyright also. If you violate 107 of the Copyright Law, you are an infringer of copyright. It's not like they don't have any legal protections or recourses at that point.

MR. KASUNIC: I understand that. But I do want to try and focus on this particular point because it does have an impact on what if any potential exemption that we recommend the scope of that exemption is.

MR. TURNBULL: I think looking at the face
of the language the last clause seems to be clear that the exemption would apply to the users who are adversely affected. So you can eliminate everybody else who wasn't a user who was adversely affected using this language.

However, reading the plain language it says with respect to the class of works. It doesn't say to with respect to the non-infringing uses of the class of works. Now it would certainly be what was intended that it would be with respect to the non-infringing uses of the class of works of that class. I haven't looked at the underlying legislative history to see what might be there to expand on that.

What I would say though is that what I was saying and Mr. Mitchell can speak for himself but it is that there is right above the part that you've highlighted this such other factors as the Librarian considers appropriate. What I was saying is that the potential misuse of a exemption is another factor that would be appropriate to consider particularly given in the CSS context the history where there are notwithstanding lawsuits and injunctions.

We continue to see postings of DCSS and other matter which is in violation of our injunction with regard to the trade secrets. Certainly it's
already been found that it was a violation of the DMCA in the *Universal City* case. There is a real reason to be concerned about the misuse of an exemption with regard to CSS.

MR. KASUNIC: Shira.

MS. PERLMUTTER: I agree with Bruce that obviously the intent of this provision is that any exception applies only to the non-infringing users of that particular class of work. So it wouldn't make a lot of sense in the first place.

I only wanted to add in response to your prior question about the harm from an exemption to the circumvention provision in 1201(a)(1) that it has a lot of spillover effect. I just wanted to add that point that if you have a statement by the Office and Librarian that certain acts are legitimate that it can also affect other things not just trade secrecy cases but also how the trafficking in devices provision is interpreted.

You will get a lot of arguments about the extent to which devices are used for legitimate purposes that can spill over. It also may affect the very model of the idea of delivery to consumers on different terms and conditions and just the principle that access means you are buying access to a
particular kind of thing for a particular kind of purpose. You can end up with a situation where individual hacks and individual ability to gain unauthorized access can cause real damage to that delivery model.

MR. KASUNIC: In terms of that damage if there has been damage, has that ever been remedied by Section 1201(a)(1)? Has anyone brought a number of actions under the trafficking provisions? Is 1201(a)(1) being used?

MS. PERLMUTTER: I think the hope is always with one of these statutes that you don't need to use it, that you don't need to go to court and that the prohibitions are there. But I know of only the cases that we've been involved in and I don't know of other cases that might be pending.

MR. TURNBULL: If you have an individual who truly keeps it all to himself or herself in doing their circumvention and therefore doesn't spill over into 1201(a)(2) in trafficking or providing products or whatever, finding out about the individual is going to be rather difficult. So it may well be a reason why I don't know of any cases.

MR. KASUNIC: Mr. Einhorn.

DR. EINHORN: I would urge that if you
have the legal authority to make the distinction you might be very well wise to just limit the exemption to those people who do non-infringing uses if you have the authority to do that. If someone does decide for whatever reason to break regional coding or any kind of access protection and then for the purpose of violating copyright, it may be sensible in addition to having our sanctions under the Copyright Act and under the No Electronic Theft Act to have one more instrument in our toolkit to stopping from this.

I don't know that you have the authority to limit to certain uses. In that particular way, we can address some of the concerns of Mr. Mitchell who feels that people are going to run with this and get the bad idea of what they can or cannot do. By establishing that you can only do this for non-infringing uses and establishing it loud and clear, any prospective pirates who are attracted to regional coding or any kind of circumvention technology for the purpose of unauthorized reproduction and distribution of other people's content can be punished more immediately by the law for their individual actions.

MR. MITCHELL: We should also take into account I believe how such a circumvention might practically be accomplished in this situation. A rule
that would permit region coding circumvention only for authorized uses as I mentioned would likely be construed to actually be much broader than that, to constitute essentially a legalization of circumvention devices that are used for purposes of circumventing regional coding and an additional layer of difficulty particularly for entertainment software publishers in that those particular devices even if it were theoretically and technically possible to only restrict them to circumventing region coding look identical to devices that actually accomplish much more nefarious purposes and that completely circumvent the verification process that is used to distinguish pirate games from non-pirate games.

So what we would have is a rule out there that would allow for a certain class of devices essentially to be used but those devices would not necessarily be region coding only devices. Most of them would allow for the play of pirated games. That has certainly been our experience and those of our member companies.

I would commend you to take a look at the filing by Riley Russell at Sony Computer Entertainment America who actually has produced deposition testimony in support of the proposition that there is no
standalone market for devices that only circumvent region coding. One such gentleman who tried to market the device was out of business within a year. It is because the market that exists for these devices is not one predominantly driven by this region coding circumvention function but rather by the desire to play pirated games.

MR. SAFIR: That's actually a supposition which is not true. The truth of the matter is that the prints that they have in Europe and the reason why they didn't buy that device was because they couldn't find a market. The truth of the matter is that it was hard for this guy to actually his device in the stores especially electronic chains in which these things are available. The only way this was available was basically through the Internet. What you are saying is just flat out not true. In addition to that, you have to also recognize these people already have DVD players.

MR. MITCHELL: Our experience is that --

MR. SAFIR: They have three DVD players.

MR. MITCHELL: Our experience is that whatever devices that may be available only to circumvent region coding, more expensive, much more difficult to find and generally more difficult to use
than the fully functional devices that would allow for
the play of pirated games. It is these fully
functional circumvention devices that account for the
vast majority and the vast demand for this whole range
of circumvention license.

MR. GENGLER: I object to that
interpretation of it because if you say that because
there is a possibility that it could be interpreted as
over broad and potentially be used to try to allow
infringing device, then it invalidates the entire
clause there that would allow for the creation of it
unless it only has non-infringing. Anything that's
non-infringing can also be mostly used in almost all
cases for an infringing purpose. To say that just
because it could be used to do that would be to render
this entire section useless and almost provide for no
exemptions to be possible.

MR. SAFIR: What's your fix on that?

MR. MITCHELL: It is an issue that we
believe goes to the very issue of the availability of
video games. If an exemption were to result from this
proceeding which has the result of putting
circumvention devices into the hands of thousands and
thousands of people that not only circumvent region
coding but also allow for the play of pirated games,
it follows as a matter of course that piracy would thereby increase. If piracy is going to increase as a result of that, then the availability of works could potentially decrease.

MR. SAFIR: But that hasn't happened, right? The DeCSS is already available to anyone who wants it at this particular junction where we are right now. There hasn't really been any more or less pirating on any larger or lesser scale. So here we are sitting and talking about a theoretical loss that can happen. Actually the horse is already out of the barn. The DeCSS code is already out there and there hasn't been any real sizeable impact on the motion picture industry, Time Warner or Universal.

MR. KASUNIC: Mr. Attaway, you had a comment.

MR. ATTAWAY: Just one final comment. As you consider your obligations in this proceeding particularly with regard to regional coding, I would urge you to focus on the words "adversely affected." No one has talked about that today. But when I purchase a DVD, I have no expectation that it will play in my VCR. I don't think I'm being adversely affected by that fact. It's just a fact. It doesn't play.
When I purchase a Region I DVD, I have no reasonable expectation or should have none that it will play in a Region VI DVD player.

MR. SAFIR: That's not true again.

CHAIRPERSON PETERS: Mr. Safir.

MR. SAFIR: When somebody buys a DVD, they have no idea about region coding at all. So they put the DVD in and it doesn't work. So while you might have that expectation --

MR. CARSON: Are you in the middle of a sentence, Fritz?

MR. ATTAWAY: I thought I was.

MR. CARSON: Will you respect Mr. Attaway please and let him testify?

MR. ATTAWAY: I believe that all DVD packaging reveals the equipment where it will play and where it won't play. I don't think there is an expectation that when you purchase a Region I DVD that it will play in other regions. I would submit that there is no adverse impact here.

CHAIRPERSON PETERS: Thank you. Steve.

MR. MOORE: I was wondering if I could add something to that real quick.

MR. MITCHELL: Of course.

CHAIRPERSON PETERS: Sure.
MR. MOORE: 321 Studios doesn't really take any position on region coding. In fact we leave the region coding intact when we make a backup. But Mr. Attaway said that no one has presented any evidence of being adversely affected, I take opposition to that because we have actually submitted here into evidence that several hundred declarations of individuals and families that have been adversely affected by the fact that they bought DVDs that were defected that the store would not accept and return or exchange.

They've bought DVDs that after a period of time delaminated and would no longer play in a player or became scratched due to their children mishandling the DVD and they are unable to gain access to that DVD in order to view what they have paid for. So I do consider that to be an adverse reaction.

CHAIRPERSON PETERS: But you are actually talking about having purchased it and having had access to it later not having access to it.

MR. MOORE: It has happened both ways. It's happened where we've bought DVDs that will not play from the onset where we can't have access to it up front through a normal DVD player. Or through the course of time, it becomes inaccessible.
CHAIRPERSON PETERS: Do you want to comment on the fragility?

MR. ATTAWAY: If I can engage on that point, I don't believe that there is any expectation that when I purchase this DVD it will last forever just like when I bought my 1988 Mazda. There was no expectation that it will last forever or that I should have a right when it wears out to go on to the Mazda lot and get a new one.

People realize when they buy a DVD that if they leave it out in the sun it's going to melt and they are not going to be able to play and they'll have to buy a new one. There's no expectation that this is going to last forever.

CHAIRPERSON PETERS: Is there any expectation how long it lasts for?

MR. SAFIR: Decades.

CHAIRPERSON PETERS: No.

MR. SAFIR: My books do.

CHAIRPERSON PETERS: You're talking about different media.

MR. SAFIR: My CDs have for three decades now.

CHAIRPERSON PETERS: You're fortunate.

MR. TURNBULL: The question of if you
bought a DVD that never played, it seems to me is a different issue and perhaps some other agency of the Government would be worried if the retailer and the producer didn't take it back in that kind of circumstances.

CHAIRPERSON PETERS: Like FTC.

MR. TURNBULL: I think you don't need to have an exemption to the DMCA in order to deal with that problem.

CHAIRPERSON PETERS: For those that never played. Right.

MR. MOORE: Actually I have two copies of DVDs. One is actually quite visibly damaged. It has a split and this will not play at all. This one which is "Dragonheart" which by the way was the declaration I read earlier in my testimony from one of my customers has no visible damage to that back of the DVD. You can't tell that it's been mishandled. Maybe it was. Maybe it wasn't. I don't know if this is part of delamination or what the problem is. I don't even know how old this particular DVD is. But it is inaccessible in a normal DVD player. You cannot access this information.

When this DVD was bought if I owned this DVD, I would expect that I owned the DVD and the data
that's contained on the DVD. I should be able to access it if I choose to.

CHAIRPERSON PETERS: Forever?

MR. MOORE: Well, certainly for some specified period of time. The hype from the DVD industry is that these things are pretty permanent. In fact, that's been an argument from their side against this type of technology. They say DVDs don't break. They are not really all that fragile. They hold up really well. The truth is that through manufacturing imperfections and some mishandling by customers they don't last as long as a enduser expects them to.

MR. GENGLER: Actually on that note of DVDs lasting forever, Jack Valenti of the MPAA in a Congressional hearing to the Committee on the Judiciary on the topic of DVD backups has said something along the lines that DVDs last forever and there's no need to make backups. I don't have the direct quote.

CHAIRPERSON PETERS: You're not going to say anything. Michael.

DR. EINHORN: Without taking a final position on this, I would just urge you when you determine that don't try to determine what the
consumer's expectation may be when they buy something. Rather you in fact may form that expectation by your policy. Let's assume that whatever you decide, you can give out that 100 percent expectation that's correct one way or the other and base the appropriate harms on that assuming that every consumer understand things correctly.

Consumers can be very floppy. They can go back and forth. It's a matter of economic policymaking. The best thing to assumption in the long run is consumer's get the picture and you will have to define for them where we are going.

CHAIRPERSON PETERS: The good news is that consumer expectation doesn't equal fair use. Fair use has its own parameters.

MR. TURNBULL: Could I just ask as a general matter and maybe in relationship to this whether you are going to offer the opportunity for the witnesses to submit post-hearing comments on specific points that may have come up?

CHAIRPERSON PETERS: We haven't decided that yet. We have decided that we may be asking questions.

MR. TURNBULL: It might be valuable again given the time constraints and some of the knowledge
constraints that may exist on some points.

CHAIRPERSON PETERS: We'll think about it.

Thank you. Mr. Lutzker.

MR. LUTZKER: My name is Arne Lutzker. I'm counsel for 321. I'll turn to the expert on 1201 who suggested that I might be able to make some comments. This particular point if this is appropriate I would just like to remark on.

Regarding expectations, the way the DVDs are marketed from a personal experience I was traveling to the West Coast and saw a program on DVDs in which the description of a DVD by proponents of the technology suggested it was indestructible. The guy did bending and that it was designed to last for a relatively indefinite period of time. I think it would be not inappropriate if this is a serious question for the Copyright Office to obtain marketing material from the industry regarding the communication to the public about their expectations on DVDs.

The experience that 321 has had which is evident in the declarations of individuals is that purchases are made and within a relatively short space of time because the DVD marketing as we know has exploded in the last three to five years people in that period of time are experiencing extensive
continuous problems with access to works due to damage that they experience due to things beyond their control which may be at a moment of purchase where a work has delamination or other problems.

Whether one suggests that a work should last indefinitely is not really the issue with this proceeding because you're only dealing with three year period of time. If an exemption applies to a particular class of works as 321 has suggested, damaged purchased DVDs for which full purchase price has been made for those works and if in this three year period more information comes to the forefront, that's fine.

But at the moment, the marketplace has a disconnect. People purchase DVDs. Many of them by virtue of declarations have presented that there is extensive public harm with respect to accessing of works in DVD format where there is damaged experience. This is one of the clear examples of extensive public harm. 321 would be pleased to present more declarations if it's desired. That particular class of works is in need of reform. The expectation of consumers is that these products would last for at least a reasonable period of time and many of them are not experiencing that.
MR. TEPP: Thank you all. I have a number of different questions on a number of different topics. I'm not going to try and ask them all at this point. Since we are talking about this DVD durability issue, I'll focus on that one. I'll direct my first question primarily to Mr. Attaway but others who would like to jump in are welcome to do so.

The Copyright Office in DMCA Section 104 Report to Congress concluded that beyond the backup exception in Section 117 of the Copyright Act there might be a strong case for fair use for backing up other types of works and also in that case I believe the analysis with regard to computers. To what extent do you believe that an argument can be made that backing up a DVD is a fair use? I know you said earlier that there's no case law holding that but how strong do you think the argument is?

MR. ATTAWAY: I think it's very strong. If there are arguments in support of being able to make backup copies of DVDs, that is an issue for Congress to decide. However the Copyright Act in my opinion is quite clear.

As I said earlier in my testimony, if it weren't clear then there would have been no reason to enact Section 117. This is not an issue of
interpretation of the Copyright Act. It may be a legislative issue. We can deal with it in that forum. But I certainly don't think it is a legitimate issue in this particular forum.

Mr. Tepp: I'll give Ms. Perlmutter a chance to come back if you want. Let me rephrase the question a little bit. Mr. Moore has put before us a proposal for an exception to create backups of works to circumvent technology to create backups of DVDs. According to Section 1201, we're supposed to analyze exceptions for non-infringing uses.

That's the reason I'm asking this question. Is creating a backup of a DVD a fair use keeping in mind that Congress may decide to create more certainty for certain acts that are fair use without necessarily saying other acts aren't fair use? In our consideration of the proposed exception, is the underlying activity that they wish to have an exception to circumvent for a non-infringing activity?

Mr. Attaway: No. Well, yes. Wait a minute. You rephrased the question. You asked your question in a way I wasn't expecting it. It is not a fair use.

Mr. Tepp: To create a backup of a DVD.

Mr. Attaway: That is correct.
MR. TEPP: Ms. Perlmutter. Then I'll come to Mr. Safir.

MS. PERLMUTTER: First of all, I agree with Fritz that you wouldn't need the very explicit specific exception in 117 for backup copies if fair use covered it. However the critical thing to focus on is that the purpose of 117, the rationale, for the exception was the vulnerability to damage or loss. So that's a prerequisite to the whole concept of allowing backup copies.

Backup copies shouldn't be just an excuse to have two copies. It should be because there is some particular danger that doesn't exist ordinarily. My reading of the Section 104 report which of course you are the experts on it, it looked as if there was some specific attention being paid to backing up of hard drives because of a potential crash of a computer. That was also focused on the concept that there was a real danger that's not there in the physical work of loss.

Just to point out that we can listen to debates about the extent to which DVDs can be damaged, but the point is no physical property is indestructible. In fact, DVDs are much less vulnerable to destruction than a lot of other types of
material objects on which copyrighted works are embodied like for example, LPs or books on paper. In this world generally, we don't always have the ability to make backup copies of any kind of personal property that might someday be damaged in some way.

MR. TEPP: Mr. Safir, you wanted to speak.

MR. SAFIR: Yes. Let me address two things about this. First of all, clearly the section on fair use in the statute for fair use it says that these are examples of fair use. I can't read the name from here but Mr. Tepp.

MR. TEPP: Yes.

MR. SAFIR: I turned 40 and my eyes fell apart.

MR. TEPP: You did it just right.

MR. SAFIR: Your point is extremely valid. There was fair use before the changes in the Copyright law that included that statute. There would be fair use without that clause. Fair use according to the Supreme Court just a couple of weeks ago clearly says that fair use is your Constitutional protection for property rights and for free speech.

Ginsberg said and you can read it in the Eldredge case yourself that we are not going to discuss in this case the free speech issues because
the free speech issues are covered under fair use. So for years now, we've been going under the premise that fair use is an exception to Copyright. No, Copyright has always been an exception to people's individual property rights under the Constitution which the courts since St. Anne's Act have evolved into an idea or this judicial concept of fair use which then Congress later on went over and codified as examples.

But you can't turn around and say because only these eight things or nine things are the only ones that are in there that are justifiable for fair use, that it's the only fair use you have. Obviously I can use my DVD as a frisbee. Nothing says I can't. It's fair use.

MR. TEPP: Okay. Thank you.

MR. SAFIR: Let me just say one more thing. Time Warner's issue about traditional copyright controls and so on. She has been making a position repeatedly that the DMCA is not some type of radical change in the relationship between individuals and the copies of material that they own and trying to bring things back to some center.

Traditional stuff that you own and everything I own I have additional copies of. I have all my pharmacy textbooks going back to 1984. I have
my grandfather's LPs with Sarah Vaughan on 78 records. I have digital copies of them of MP3s and copies of them on tape and so. I have so many copies it's unbelievable. I have copies of newspapers which I used to scan into my computer, only if there were graphics for cases like when I would testify over here.

All of this has always been part of my fair use rights if not explicitly under there but that's always traditionally what I've been allowed. The DMCA has rapidly changed that so their position is not the traditional position. Their position is radical. It says that the individuals don't have access to things that they paid cash for.

CHAIRPERSON PETERS: Excuse me. You're giving us your interpretation of fair use. We understand that it's your interpretation. There are many different people in this room who probably would disagree with you including a number of courts. We understand where you are coming from.

MR. TEPP: Okay. Let me just make one clarification. I may ask tough questions and loaded questions. I'm not trying to make a point. I'm just asking tough questions. As the Register has said at the beginning of each hearing, nothing has been
decided yet.

Let me move on to my next question which I want to direct to Mr. Moore.

MR. SAFIR: I'm sorry. I didn't mean to imply that you decided anything.

MR. TEPP: Good. Thanks. Mr. Moore, you may have alluded to this already but I want to clarify it. The copies that your customers make using your software, are those copies fully protected by CSS and region coding and all the technological protections that the copyright holders have placed on the original copy or are they somewhat less protected?

MR. MOORE: They don't have the CSS protections in place. The reason for that is because we can't burn the disk key back to the blank media. We actually sought to re-encode the backup with CSS leaving it virtually untouched from the original. We found out that through industry agreements between the DVD drive burner manufacturers and the entertainment industry that they precluded those drives from writing to the specific sectors necessary to make that disk key appear on the media.

We could re-encrypt it with CSS. The algorithms are widely known. But if we did so, they would refuse to play in any player whatsoever. You
couldn't play it in a DVD player and you could not
play in a computer player. So they would be
unplayable.

MR. TEPP: Okay.

MR. MOORE: However I do that any piracy
features that we've incorporated into the backup media
in some ways even reenforce the protection mechanisms
that the entertainment industry sought to include in
the first place.

MR. TEPP: I'll save the rest of my
questions for later. Thank you.

MS. DOUGLASS: I just have a quick couple
of questions. Maybe you have addressed this before,
Mr. Turnbull. Are there DVD licenses for Linux
players now?

MR. TURNBULL: The CSS license -- CSS is
not required for the DVD format. It is an overlay
that has been widely adopted for movies but you can
make DVD without using CSS. The CSS license does not
ask what operating system you are going to use. It
simply says that in your implementation you must take
certain steps including keeping the keys secret and
things like that. So we don't ask people whether they
are making Linus implementations or not.

In conjunction with the hearing three
years ago, we did go out and make an attempt to find out what was available. We discovered and provided to you and it was in the notice that there were two that we were able to find. There could be others we simply don't know about. As we understand it today, one of the two licensees we identified three years ago is still making a Linux-enabled implementation. That is available primarily through OEM deals with computer manufacturers. So it would come loaded with the computer.

MS. DOUGLASS: Thank you. Next question is very hypothetical. I'll back up a bit and talk about yesterday's hearing for purposes of illustrating what I'm talking about here. Yesterday I believe there was an opinion expressed that if there was an exemption for screen readers or TTS, the publishers would interpret that as a mandate and even if the blind and visually impaired which we were talking about yesterday could not implement or could not circumvent, the publishers would make it possible for that particular option to be placed in their eBooks. We were talking about eBooks.

Not speaking about whether anybody has proved a case or whether the criteria have been met or anything and if the Copyright Office recommended that
there were a region coding exemption, what would prevent a region coding just to be turned off? I'm sorry I've given so many words to such a minor point. But what prevents the copyright owners from simply turning off region coding if there were an exemption?

MR. TURNBULL: There's nothing that prevents them from turning it off even today in the absence of an exemption. The region code is not a required feature under CSS or the DVD format licenses. It is something which is available to motion picture companies to use if they wish. It's also usable in combination.

You could have a disk that's coded for three regions and playable in those three regions. I think the answer to your question is there's nothing that prevents it now in your hypothetical and there would be nothing that would prevent it later.

MR. MITCHELL: With respect to entertainment software, it would be a different situation because we again think that there might be some impact on the availability of video games because of the way that region coding is used as a constructive tool to allow games to be made available in certain regions that might not be able to be made available in all regions.
If a video game publisher for example is licensed for the use of certain content or certain music or a certain character only in the U.S. region, they can use region coding currently to make that game available in the U.S. Whereas if they would not use region coding, they would be faced with a very different economic and marketing decision.

Do we make this same game available all throughout the world and incur perhaps additional expenses in doing so? Or if we cannot obtain the licenses to make a particular game available in Europe or in Japan, do we simply forego making this title available in the United States? So it's an exceptionally useful tool to video game publishers for the purposes of being able to make these products available in specific regions and also as I mentioned to increase user enjoyment by ensuring that releases in those countries are released with appropriate content or released with appropriate music or localized to languages that are also compatible with that region.

MS. DOUGLASS: Ye, Mr. Einhorn.

DR. EINHORN: I fully want to endorse what Mr. Mitchell said. I think regional coding is an entirely valid business practice. As a professional
economist, I would strongly not want to associate myself with any other wise. Mr. Attaway points out that a movie costs $80 million to $100 million to produce and distribute.

In so doing, we want to reserve the right for the content owners to make their content available through a bunch of windows that allow them implicitly to price discriminate against different kinds of users depending on where they live and also in their interest in seeing a movie. This is why a movie at a video store costs less than a first run theater.

What the distinction here is though is we're not considering whether or not to disallow regional coding. The system of course we want to encourage. We also have right now a number of ways in which regional coding can be defeated. It can be defeated through PAL converters on video cassettes and it also can be defeated by devices that you can buy and also for limited recoding devices that you can also have on your own computer.

So it's now possible to defeat regional coding. To defeat regional coding in a small number of cases, we're asking ourselves now are we adding any more to the fire here. What is the effect of allowing one more use this time for people who have the
capacity to hack through certain protections and saying you know there are few of you out there but if you have the ability here to hack through a DVD and figure out how to use the DVD without having to buy a second DVD recorder and you can save yourself some money? I guess it was a lawful before and can be a lawful use after. But I don't mean to suggest here that regional coding is something that we want to defeat as a global strategy.

MR. MOORE: I'd like to add that while we talked before about how you must decrypt CSS encrypted data in order to get at the region code, the reverse is not true. In the absence of CSS and in the absence of encrypted data, you can still apply the region code. The two are not dependant on each other.

MR. TURNBULL: Two things. The first is that actually makes the point that I was trying to make before which is region code is in fact independent from the technology of CSS. The second issue is however the reason why CSS as a license matter requires the detection of the region code is that there is no other legal obligation to do that. So you could insert the code in a DVD disk that was created without CSS but there would be absolutely nothing that would require anybody to look at it.
Therefore the system wouldn't work.

MS. DOUGLASS: Thank you.

MR. SAFIR: I'd like to add to that just that from my perspective, I really don't care about regional code either. I don't understand why they really need it. They can just distribute it regionally just like any other products that Nike does or anybody else. But in and of itself, the regional coding is not an issue. The real issue is access to the information.

MS. DOUGLASS: Thank you.

CHAIRPERSON PETERS: Back to you, David.

MR. CARSON: You don't have any questions.

CHAIRPERSON PETERS: No.

MR. CARSON: Let me follow up, Mr. Turnbull, with what you just said. First of all, I gather the region code itself is a technological measure that controls access. Is that understood and agreed to?

(Chorus of yes.)

MR. TURNBULL: Yes, when responded to.

MR. CARSON: Okay, understood. So you don't need CSS to have region coding. On the other hand, I assume CSS might be one obstacle in getting to the region code and doing something with it. Is that
a fair statement?

MR. TURNBULL: Yes, I suppose.

MR. CARSON: I want to spend some time on region coding but first a couple of other questions. I think one of you may have made a passing reference to but they were on the agenda for today and I just want to cover them very briefly. First of all, is there anyone here who would contend that it is a violation of Section 1201(a)(1) to circumvent an access control that is applied on a DVD that contains nothing but public domain material? Is there anyone here who says that if someone put CSS on a DVD that simply had "Birth of A Nation" on it and nothing else and I circumvented that would I be violating Section 1201(a)(1)? Silence. Shira, would I be?

MR. MOORE: I would certainly say no.

MR. CARSON: Okay. I guess I would like to hear from some of the content providers what their position is on it because their response is probably a more interesting one to me.

MS. PERLMUTTER: If it's purely public domain material then the mere act of circumvent, no.

MR. CARSON: No one else disagrees. There might be some interesting questions when it's mixed in with public domain and copyrighted and that's a
different question I understand. We were also
supposedly going to be talking about tethering of DVDs
although no one has talked about it. We had at least
one comment. I just wanted to get some clarification.

At least one of the comments has alleged
that DVDs can be tethered to a single platform
preventing users from playing the same DVD on a
computer and a standalone player. Now I'm not
familiar with that at all. I'm just wondering if
there's anyone here who can tell me if that is or is
not in fact the case. I suppose potentially it can be
done. Are there in fact DVDs out there that can be
only tethered to computers or only to non-computer
players so you can't use them on both?

MR. SAFIR: It's worse than that.

MR. MOORE: Mr. Carson, actually what you
might be thinking about is when I spoke before about
error correction code and how our software actually
works to restore a DVD to a playable condition. It's
because of the different technologies that reside in
a player that sits on top of my television and the DVD
player in my computer.

If a DVD has become damaged, the DVD
player that sits on top of my television doesn't have
the circuitry on the inside of the box to go through
the effort of actually trying to do that error
correction and displaying the DVD. Do you follow what
I'm saying?

MR. CARSON: Yes.

MR. MOORE: So it will not play in set-top
player.

MR. CARSON: But that's a damaged DVD.

MR. MOORE: That's a damaged DVD of some
kind whether it's delaminated or it's been scratched.
However that DVD may very well not necessarily but may
very well play in the player in my computer because my
DVD player in my computer has the necessary circuitry
on the inside to actually go through the effort of
reading the error correction code and trying to make
the adjustment. Does that answer your question?

MR. CARSON: That's not really my question
because the comment which I unfortunately don't have
in front of me but as I understood what the comment
was asserting is that there are some DVDs marketed
that are actually on the market so that once you buy
it off the shelf and assuming it works the way it's
supposed to work, it is restricted to a single
platform. You cannot for example play it on a
computer perhaps or you cannot for example play it on
a DVD player that you hook up to a TV set.
MR. SAFIR: That was actually my comment. It's the Vital Books sting. Vital Books has a product where they sold the entire dental school's textbooks plus other material that students shouldn't have to buy. It forces them to buy them at the university level if you are in the program. Then it only works with the Vital Books player which is only available on a certain pre-installed max by Vital Books. At the end of the semester, the books turn themselves off.

When they marketed this, the infringement on fair use was so clear that they said as a marketing ploy in their website that if publishers should come over and help us do this project because you won't have to compete with your used books anymore in the used book market. Then when I pointed that out to them in a Slashdot thread when I was working at NYU at the time in which I quit over that whole thing, then what happened after that was they removed that stuff from the website because they realized it was so damaging to them.

Now the condition is still like that. Basically most of the DVD at this point is still not printable. Since then, they have been able to print it but it still turns itself off at the end of the semester.
MR. CARSON: My question is really since we're talking about audio-visual works that was really what I was talking about.

MR. SAFIR: But the point is it's tied to one subset of a whole --

MR. CARSON: I understand what you are talking about. I get the point on that. The focus of today's hearing is really audio-visual works.

MR. TURNBULL: Let me maybe comment briefly. CSS was designed explicitly as a multi-industry matter and it was tested and reviewed across platforms and across industries explicitly for the purpose of making sure that in fact CSS was usable and is usable across any platform that anybody wants to build. There is no license limitation and the technology was vetted by many people in the computer industry when it was initially developed.

MR. CARSON: No, I don't think the comment was suggesting this was a function of CSS but rather to be a visual works marketed in DVD format.

MR. MOORE: Mr. Carson, I think I understand your question. As far as I know, there are no DVDs that are currently marketed that way. But I'm certainly aware of the technology inside of the DVD format that certainly could provide for that.
MR. CARSON: Sure.

MR. TURNBULL: I think his backups actually are.

MR. MOORE: Pardon?

MR. TURNBULL: If I understood your presentation before, your backups are tethered to the particular device.

MR. MOORE: That has more to do with the watermarking that we actually put into the video. The backups will still play on a regular DVD player.

MR. CARSON: Okay, let's spend a moment on the backups. We've heard by it's not fair use to make a backup of the DVD. We've heard Mr. Safir's interpretation of the fair use statute. What I don't think I've heard from Mr. Moore or perhaps Mr. Lutzker out of their mouths why it's fair use to make a backup of a DVD. I would think you would want to make that case to us. Here's your chance.

MR. MOORE: Well, it's a fair use or a non-infringing use or both, I'm not a lawyer.

MR. CARSON: You have one.

MR. MOORE: I'm just an average consumer. I'll let Mr. Lutzker answer the legal definition or his legal definition if you would like to hear it. But mine is a non-infringing use. Mine is a use where
I'm not infringing on the copyright holder. I'm not doing anything that would otherwise take any revenue outside of the copyright holders' pockets.

MR. CARSON: Can I just stop you? You are making a copy. Mr. Lutzker, tell me why that's not infringement because we know that's a violation of Section 106 unless you can give me some other provision that gets him out of the bind that he's just put himself in.

MR. LUTZKER: I don't think that there's any question that a backup copy is a copy. I think we'll have uniform agreement on that. There is a separate and more subtle question under 117 which Mr. Attaway has initially addressed in terms of whether a DVD is a computer program as defined under that provision. I don't know that you are going to reach that decision in this proceeding or not. But that's a separate issue in terms of the nature of backups with regard to computer programs.

Making an assumption which I wouldn't conceive about that a DVD for our purposes does not immediately fall in the 117 issue. Therefore, the question is then is it a fair use. The answer is it may be a fair use to make a backup of a program under certain circumstances.
The case that we have presented is really a split case in the sense that it is clear and I would beg to differ with the Register in terms of consumers' expectations. Consumers' expectations are that when you buy a DVD you're going to have it for as I would say a reasonable period of time.

If DVDs are not indestructible but a fragile medium that is subject to material wear and tear such that the access controls can be damaged and therefore deny access to the very product that you have purchased, under what circumstances should you be permitted as a lawful acquirer of that product to make an acquisition of that product and then to make a backup for use purposes? The case that has been presented in the full comments which we do address the backup more specifically and here we've addressed the damaged aspect but the ability to make a backup of a perfectly clean, undamaged DVD in my view may be a concomitant necessity related to the fragility of the medium and combined with the marketing practices of the industry where consumers have indicated we can't get replacement copies, we are basically forced to repurchase the product.

From a fair use point of view, there is no question in my mind that the ability to access a work
that you have lawfully purchased falls within the parameters of fair use. I don't think you would make any finding other than that. If you purchased the product and if it's subject to access controls, you have made a lawful acquisition and you should be entitled to access that work. Whether you can do other things with it falls within the parameters of Section 107 or other exemptions but you should be able to access it.

If you can't access it, then there is a material adverse harm to the consumer. The question then becomes are you allowed on a self-help basis on a private individual basis to make a backup in anticipation of a problem materially occurring. As long as the medium is as fragile as it is, there is a legitimate basis to conclude that fair use under those circumstances is the making of a backup.

What 321 has done in its marketing practices is educate consumers as to what you can do with this by adding indelible disclaimers and warnings that facilitate the proper educational use of that. They have done this on their own initiative. They've added methodologies and digital technologies which can allow the tracing if there is an abuse of the practice. Under the circumstances that have been laid
out in the combined comments and the testimony today, there is support for the conclusion that an individual can make a backup copy of a lawfully acquired, fully paid for work for private personal use only.

MR. CARSON: Okay. Let's turn to region coding. I'm going to focus to the three of you, Ms. Perlmutter, Mr. Turnbull and Mr. Attaway. First of all, the justification for region coding, the one that comes instantly to mind to me and I certainly recall focusing on three years ago is exactly the marketing window. At different times, you don't want people in other parts of the world to be able to play DVDs when you are about to open in the theaters. I'm talking about motion pictures. I'll get to you in a moment, Mr. Mitchell. That's the basic concept I gather. Is that right?

MR. TURNBULL: Yes.

MR. CARSON: Apart from that, is there any other reason why region coding is important in the motion picture industry?

MR. TURNBULL: My understanding is that there are occasions when a particular company will have the distribution rights in one area and not in another.

MR. CARSON: Sure. But that's been true
in all of the copyright industries for ages and most publishers of various kinds of materials haven't really felt that they have to prevent people from reading the book in the region where they weren't permitted to sell it.

MR. TURNBULL: Correct but I think the reason why there was a sense that DVDs might be different is because you can for example have multi-languages and frequently do have multiple languages on the DVD. You can encode different playback formats on the same disk. There might be reasons of efficiency and other reasons to want to do all of that and then say but I want to make sure that this stays in a particular region because I only have the rights in that region. So there may be some differences with other past kinds of technologies.

MR. CARSON: Shira.

MS. PERLMUTTER: And to amplify on that a little bit, our comments are going to this are in somewhat more detail. I think you might want to ask some questions when Dean Marks testifies at hearing in L.A. But certainly just as with the video games, there is some issues about local languages, local censorship, requirements that can make a difference from region to region.
MR. CARSON: But why does that mean that you have to prevent people in those areas from actually be able to view them as opposed to simply not marketing the content in those areas? Aren't you going far beyond what you have to do by coding it so that it can't even be seen on a player in that region?

MR. ATTAWAY: We are only marketing in those regions. People can view them. Anyone can go out and buy a Region VI player if they feel that strongly that they want to want Region VI DVDs in the U.S. Or visa versa, anyone in Singapore can purchase a Region I DVD player in the U.S. and take it to Singapore and play Region I DVDs in Singapore.

MR. CARSON: I understand that. It's not really answering my question though. Why do you have to prevent someone from being able to view a Region II DVD here in the United States?

MR. ATTAWAY: I just said that we are not preventing it.

MR. CARSON: You are making it awful hard though.

MR. ATTAWAY: No harder than if someone chooses to release only on VCD as I said earlier.

MR. CARSON: There is a difference I think.
MR. ATTAWAY: You would have a hard time finding a VCD player in the United States too.

MR. CARSON: Let me try this out on you because I think there is a difference but maybe you'll say it's not a difference. It's one thing to say I have no reasonable expectation that I can play a VCD on my video cassette player or even on my DVD player because it's a different animal. It's a different thing.

Here though you are talking about a DVD. You're talking about a choice that the content provider has made to disable that DVD from playing in a device that otherwise would be able to play it. Now that's very different from the VCD situation where I'm trying to play it on VHS recorder or my DVD player. Do you see the difference? If so, can you explain why I shouldn't care about that difference?

MR. ATTAWAY: I understand the point that you are making but the concept of regional coding was intended to more or less replicate the technology in the analog world when there were different analog VCR technologies, NTSC, PAL and SECAM, which because of those differences it enabled motion picture companies to market motion pictures regionally.

When DVD was being considered, the
decision was made to incorporate regional coding in order to provide the motion picture companies the ability to maintain that regional marketing practice. It was felt that they needed that ability and to induce motion picture companies to release product in DVD format, everyone involved embraced the regional coding concept. I submit to you consumers are better off because of it because it is one of the inducements that allow people to watch movies on DVD format instead of VHS. It was a good thing and not a bad thing.

MR. CARSON: So if you couldn't do region coding, the movies industries would choose not to market DVDs.

MR. ATTAWAY: I believe that was the position of some companies, yes.

MR. CARSON: And just going back to what you said a moment ago, is it your understanding that the reason that in the video cassette world we have different kinds of formats, PAL, SECAM, NTSC, the purpose of that was in fact so that video cassettes marketed in Europe for example couldn't be marketed here?

MR. ATTAWAY: No.

MR. SAFIR: This is false.
MR. CARSON: Mr. Safir, I really don't need you. I really don't. So we are talking about something different here. You may be replicating what happened but the reasons why that happened in the video cassette world were accidental or reasons that because in different areas of world choices were made to adopt different formats.

MR. ATTAWAY: Correct.

MR. CARSON: Here you are making a choice to say people will not be able to play a Region II DVD in Region I. That is a little different, isn't it?

MR. ATTAWAY: It is not different in terms of the marketing practices that are desired to be followed.

MR. CARSON: All right. I understand that. Now we've had a number of comments and one in particular I remember is we have a large Indian community in the United States. We have communities in the United States obviously from all over the world. The Indian one I remember because we had several comments but one in particular pointing out that as I'm sure you know the Indian film industry is the largest film industry in the world.

There are many Indian expatriates over here who would like to be able to watch DVDs. The
assertion is that you can't watch them over here because they have the wrong region code and yet they are not even marketed here. First of all, that's the premise. Is that accurate as far as you know?

MR. ATTAWAY: I'm not a big devotee of Indian movies. I just don't know if they are regionally coded or not. I can't imagine that they would be.

MR. CARSON: You make a good point that you thought the testimony was that the Indians didn't use region coding. Three years ago, that's what I thought I'd heard. That's not what I read in comments in front of us now and that's what I'm trying to get at. Is there anyone here who has any information on that?

MS. PERLMUTTER: I guess the problem we're having is it's the Indian film industry that makes that decision, not any of us. We don't necessarily know what they are doing.

MR. CARSON: Michael.

DR. EINHORN: Can I ask for a point of clarification? Regarding the Indian matter, I would be very surprised if they regional code. I'm sure it's just coded for India.

MR. CARSON: But that's regional code,
isn't it?

DR. EINHORN: Only for one region.

MR. CARSON: Right.

DR. EINHORN: Would that be covered by the DMCA since it's a foreign copyright? It's a work that is not --

MR. CARSON: Yes. Don't worry about that, Michael. It's not an issue. Let's assume for the moment and hopefully we'll get the real fact because apparently none of us here have the real facts. Fritz.

MR. ATTAWAY: I was just advised that in the reply comments of IIPA the statement is made based on information given to them by the Indian film industry that they do not regionally code.

MR. CARSON: So that's not an issue. Okay.

MS. PERLMUTTER: But only to follow up on that, essentially it's the choice of the film maker not to encode so that Indians all over the world can watch it in that format.

MR. CARSON: Which is great.

MS. PERLMUTTER: That's always possible. There's no requirement that anything be region coded.

MR. CARSON: Right. But let's assume and
this may be a false assumption now. You certainly have given me information that suggests that what was in that one comment was false. Let's assume that there are a more than trivial number of cases where people who acquire abroad DVDs of motion pictures that are not available for sale in the United States want to view them in the United States. What's the justification for preventing someone who wants to do that from doing it?

MR. ATTAWAY: The justification is to maintain the regional distribution system of motion pictures. There are a lot of people not so much in the United States but in Asia who would like to view motion pictures on DVD before they reach theaters in Asia. Regional coding was developed to allow motion picture companies to engage in sequential marketing.

MR. CARSON: Let me make my question clearer. This may obviate the need for you to reply because this is not necessarily an attack on regional coding. In fact nothing I've said should be considered an attack on regional coding.

MR. ATTAWAY: I feel like I'm being attacked.

(Laughter.)

MR. CARSON: You're supposed to, Fritz,
but that's just for the fun of it for me. The point
is I may ask tough questions because I'm trying to get
things out of you. That doesn't necessarily mean I
have a opposing point of view.

MR. ATTAWAY: I understand.

MR. CARSON: But in any event, the premise
I'm getting at really is why shouldn't someone here in
the United States who purchased a DVD in Japan or
India, brought it home and wants to see it if they can
figure out how to do it be able to circumvent the
region coding in the privacy of his or her own home so
he or she could watch it. That's the question.

Shira.

MS. PERLMUTTER: Two points. The first is
it's just important to recognize that what you are
talking about is affecting the rights of foreign
copyright owners and how they decide where their work
is going to be viewed. This exception would be one
that would say that you can circumvent to get access
to a foreign right holder's work that they intended to
be seen somewhere else. I just think that's important
to keep in mind.

MR. CARSON: So you think the Copyright
has the right to determine where a copyright owner's
work is going to be viewed.
MR. SAFIR: Isn't that nice.

MS. PERLMUTTER: I think we have the rights that are set up in the Copyright Act. But I think if something is encoded in a certain way, it's meant to be sold in only one place.

MR. CARSON: Sold. My person bought in India and brought it back here.

MS. PERLMUTTER: But my point is only that you are dealing with issues that have to do with foreign copyright owners' interests and rights and that's just something to take into account as you look this.

MR. CARSON: Sure.

MS. PERLMUTTER: My second point was going to be that overall what you are looking at is the extent to which there have been adverse impacts. The point is that there are many ways that in those relatively small percentage of cases where someone buys a foreign film that happens to be regional coded and wants to watch it here - and we have no idea on this panel at the moment what level of problem we're talking about - that there are many other ways to do it. Bruce has talked about some of them. So it's important to look at the whole picture. Is access for doing that kind of thing actually being unduly
impaired rather than the specifics of the particular exemption in 1201(a)(1).

MR. CARSON: Okay. Let's turn to the video game industry. We heard articulated that the primary basis for region coding in the motion picture industry which is one that this office certainly three years ago not only understood but more than understood said that's legitimate and that's part of the reason why we don't really see an issue with respect to region coding. That's what we said at that time.

Now with video games, I don't think you have the same issue that we just talked about with the motion picture industry about timed release. First of all, video games don't play in motion picture theaters obviously. So that's not an issue, correct?

You've given us a handful of reasons why region coding is there. One is that it helps you comply with your licensing agreements. Another is that it allows a game publisher to match content to cultural sensibilities and so on to basically target a particular addition as it were of a video game to the local market. The third one sounds like the same thing. I'm not distinguishing very well because it's marketability and user enjoyment.

One is maybe you want to comply with local
laws and the other is you want to target it to your market and what your users expect. Why do you need region coding for that? Why can't you just sell a particular country's edition in that particular country? If someone wants to bring the Japanese video game here and play it, let them play it. Why are you preventing them from doing it and why should we care that you should be able to?

MR. MITCHELL: There is another rationale too that I believe you had recognized during the 2000 rulemaking as a legitimate purpose for regional coding. It is enhancing local distributor marketing opportunities for regionally appropriate content. We would suggest that this too for the video game industry is an important consideration in that it does foster the growth of local distributorships, local retailerships for appropriately region coded product and discourages the world market in one region product that might otherwise interfere with that development in what is basically a nascent industry in making key markets around the world.

As to your question about why those purposes couldn't also be accomplished through just simply marketing a particular content, I suppose you are correct that those purposes could initially be
accomplished. However it wouldn't necessarily
guarantee that those products couldn't be resold in
other markets en masse and would not necessarily
facilitate those purposes in the secondary markets to
which it is sold.

MR. CARSON: Okay. That's it.

CHAIRPERSON PETERS: Since it is 1:00
p.m., what we will do is conclude now. One more?

MR. TEPP: I promise to be short. I just
want to follow up on something. Thank you for your
indulgence. Mr. Carson earlier asked "Is a region
code an access control?" Mr. Turnbull's reply I
thought was an interesting one, "When it's responded
to." That triggered in my mind a different part of
Section 1201 that says affirmative responses are not
required from devices. Are devices which fail to
respond to region controls, multi-zone players, more
like devices that avoid or bypass the region control
or are they simply failing to affirmatively respond to
region controls?

MR. TURNBULL: Because the manufacturers
under the CSS license are obligated to interpose some
form of technology that makes it difficult to avoid or
bypass simply or to ignore the region code and to hack
into the system that responds to the region code,
there is technology as I said earlier which would have
to examined on a product-by-product, producer-by-
producer basis which protects that capability in a way
that likely would considered to be an effective
technological measure under the DMCA.

MR. TEPP: Aside from licensing issues
though, you have a player out there that's a multi-
zone player. It may be violating your license. It
may be violating at patent but it exists. For
purposes of 1201, is it a circumvention device?

MR. TURNBULL: Let me try it again. The
XYZ manufacturing company has made a DVD player
including a robustly implemented region code playback
system. In order for the XYZ manufacturer's device to
become a multi-zone player, someone has to defeat the
region code system that they have built into their
player.

MR. TEPP: What if it was never built into
the player is what I'm asking.

MR. TURNBULL: They are. The multi-zone
players that I'm aware of that are on the market what
has happened is that manufacturers' implementations
have been defeated and their parts have been
substituted in an after-market process that's done
either by the user or more likely by a service center.
CHAIRPERSON PETERS: David has one.

MR. CARSON: I just want to follow up on that. By whatever means I get myself a multi-zone player, as far as you're concerned I bought it. I got it. Now I'm going to watch a DVD from Region III. Have I just violated Section 1201(a)(1)?

MR. TEPP: That's where I was going.

MR. CARSON: Yes.

MR. TURNBULL: I don't see how you have actually defeated anything that was in that product because it was not in that product when you bought it.

MR. CARSON: Well the region coding was in the DVD and I have a product which doesn't exactly ignore the region coding. It just accommodates the coding for all regions. While I'm doing that and actually using that, am I circumventing any access controls?

MR. TURNBULL: I don't think so.

MR. CARSON: Any other views?

MR. ATTAWAY: I think that is analogous to when you purchase a DVD drive for a computer as I understand it. You can set it for any region that you want to. As a matter of fact, you can go back and forth several times. So you're clearly not violating 1201(a). Could I make one more point? Mr. Carson,
you were so tough on me and I was flustered. I neglected to make this point.

Actually I tried to make the point earlier and I didn't make it very well. The point is that you should not permit circumvention of regional coding because it removes the incentive to market those works in the U.S.

If you allow circumvention of just for the sake of this example Indian films to be viewed in the U.S. which are encoded regionally, you eliminate the incentive of Indian producers to release those films in Region I. So all of the people who do not have the ability to circumvent that would like to view those films will not be able to. That's why you shouldn't do it.

MR. LUTZKER: If I could add just one thing also along the lines of what Fritz said and supplementing in response to the questions about the backup because we do deal with specifically in our written comments at pages nine, ten and eleven, you could look at that and also it addresses the very first question you asked about is VHS a soon-to-be eliminated technology. What we did in these comments is and I realize representatives here may not be aware of it but quote members of the studios who are
suggesting that in fact VHS is a technology of the past. Many of them are eliminating products so that you can only get it in DVD format.

CHAIRPERSON PETERS: With that, we will conclude this morning's hearing and for those who may be testifying this afternoon, we'll be back in an hour. Off the record.

(Whereupon, at 1:07 p.m., the above-entitled matter recessed to reconvene at 2:08 p.m. the same day.)

CHAIRPERSON PETERS: On the record. We will resume the hearing this afternoon. Almost everybody was here this morning so I won't go through the formal opening. Just to make it clear that there are no time constraints but you should be concise in your remarks. Then after you finish your testimony and everybody has finished then the panel will ask questions and we will have the transcript up within one week. But you still have an opportunity to correct it and then the corrections will be up online.

This afternoon we're going to basically here from Mr. Montoro, Mr. Hernan, Mr. Band, Mr. Sulzberger, Mr. Mohr, Mr. Simon and Mr. Kupferschmid. Let's start with you, Mr. Montoro.
MR. MONTORO: Good afternoon, Ms. Peters and members of the Board and thank you for inviting me to speak before you today. I welcome Mr. Tepp. It's nice to have you on the Board with us.

Since time is limited, I may not address every issue but that in no way means that I either agree with disagree with it. It does not seem like it was only three years ago that I was here last. During the 2000 rulemaking, I sat before you and explained the problems consumers faced with using dongled software when those mechanisms failed to permit access because they either have malfunctioned, been damaged or have become obsolete.

For those that were not present during the previous hearings, what I have here in my hand is called a dongle and while one of these devices may seem innocent enough, quite often consumers are forced to use multiples of these devices to run software programs on their computer. This is also a cause of failure. This is what we've been asked at times to run on top of a laptop. Can you see that?

My testimony at that time, along with others on the subject, was in some way responsible for the second exemption that arose from the first rulemaking. As a father, I have derived great
pleasure in watching my daughter grow up over the past 10 years. As parents, we try to teach and lay down certain guidelines, but we don't always get to see how well we did. In my testimony today, I hope to show you that the guidelines this Office laid out regarding the second class of exemptions in 2000 were not only correct but have done much good as well and that a renewal of that exemption is warranted.

In October 2001, I received an inquiry from a potential client. This was a large organization with amazing people resources that did an extensive analysis report. Apparently they had heard of my company through my comments and testimony during the previous rulemaking. I learned they had two programs which used a dongle that ran on the same machine at the same time. One set of these access control devices had failed in the past. The manufacturers were no longer in business and there was no way to replace these devices that were starting to act up.

I also learned that due to budget constraints and the amount of time it would take to train people on new programs, it was not feasible to find and use an equivalent piece of software. Further, incredibly enough, no one in their vast
organization had the technical expertise to replace these control mechanisms.

That potential client was the United States Department of Justice. The agency involved was the Immigration and Naturalization Service, the INS. This software was used for the travel document production system which as you might know produces passports and visas.

In the words of the INS, "If those dongles had failed again, there would have been an indefinite halt in travel document production." In a post 911 world, I think you can all imagine the implications of a catastrophe like that.

I am proud to say that this potential client became a customer of mine, and this is in large part due to the decision made by the 2000 panel and the Register of Copyrights. Thank you, Ms. Peters. We were able to solve the access control problems the INS was having and once we completed the project, I received a very nice thank you letter from the INS that is attached. All of you should share in that praise.

I have read the papers of some of my opponents that claim a renewal of this exemption is not justified simply because a number of the comments
and reply comments only included one or two examples as evidence that a real problem exists. I would like to point out that nowhere in the notice of inquiry does it state that the submissions from the previous rulemaking are to be ignored. And in those comments and reply comments there is a substantial amount of material presented by my company, the National Library of Medicine, the National Agricultural Library and others to justify a renewal of this exemption.

I would not want anyone to think that the problem of access control devices is a trivial one. Therefore I would like to submit along with my testimony today an additional 87 pages of examples that have to do with malfunctioning, obsolete or damaged devices. Ms. Peters stated in the Final Ruling of October 27, 2000, "that no evidence had been presented that the marketplace is likely to correct this problem in the next three years." And three years later, we see how right she was. Please take note that of the papers I am submitting with my testimony, none were previously presented, and in fact, all of the problems submitted today have occurred over the past three years.

It seems that others are aware of the problems users face and I would like to applaud the
Software & Information Industry Association ("SIIA") and its president, Mr. Ken Wasch, for their forward thinking. The SIIA represents over 600 high-tech companies that develop and market software and electronic content. In their reply comments on page 10 paragraph 2, Mr. Wasch says that "even with only a few examples submitted, the SIIA still recognizes the need for an exemption and is willing to give those commentators the benefit of the doubt."

He goes on to say that they do not oppose the codification of an exemption if one meets certain criteria, "Subject to threshold conditions, literary works including computer programs and databases that the circumventor has legal access to, but are protected by access control mechanisms that fail to permit such access because of malfunction, damage or obsolescence which results, or in the immediate future will result, in damage to such works."

I do take issue with some of those threshold conditions that he mentions. I also wonder if they are outside of the scope of this rulemaking procedure, which is to determine a class of works. As Ms. Peters suggested in the final rulemaking, "Congress should consider amending section 1201 to provide a statutory exemption for all works,"
regardless of what class of work is involved, that are protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence." It would seem that this would be the proper place for those conditions to be incorporated. However just in case, I have to go over it anyway.

The first condition is "a person or organization should have legal access to the work at the time of circumvention." I certainly agree on this but wouldn't it be assumed that the person must have legal access anyway because I don't think we'd be making exemptions for infringing users. As long as the user has legal access to the work, then the copyright owner will already have been compensated.

In the course of good business practices, my company has required a copy of an invoice or some other proof of purchase from a customer. There are however occasions where the person or company cannot locate a copy of their invoice because the software had been purchased too long ago. For instance, the Department of Justice was not able to locate an invoice for their software because it was purchased more than eight years ago. Since companies do not need to maintain tax records for that long, it would be an undue burden to ask them to provide an invoice
or not receive relief. Therefore I would suggest when some other proof of purchase is not available, there must be an alternative such as a declaration under penalty of perjury. My company has used both of these methods for many years now.

The second condition given "any person or organization seeking to qualify for an exemption must notify the copyright owner and give the copyright owner the opportunity to cure the problem, for instance, by providing a copy of the work in a form not protected by access control technologies or fixing the problem with the access control measure."

On this I disagree. In the final rulemaking as well as in the papers I submitted today, it is clearly stated that "vendors of the software may be non-responsive to requests to replace or repair the dongle or may require the user to purchase either a new dongle or an entirely new software package, usually at a substantial cost." One of these companies is called ERDAS. They produce Department of Defense software which includes Target Mapping programs. The company only warrants the device for 30 days. After that a new dongle must be purchased. If the software package is out of date then no warranty is even offered.
Certainly the vendor's website should be the first place the enduser should start looking for a solution. A number of the examples I have submitted have come directly from the manufacturers' websites, however, sometimes they are already aware of the problem or there is not always a solution provided.

Ornis software notes, "The manufacturers of hardware locks have informed us that the new breed of parallel port devices are likely to damage the dongles due to the method used for high speed data transfer. These devices include parallel port SCSI adapters, scanners, Ethernet adapters, tape drives, video cameras, floppy disk drives, CD-ROMs and CD writers. This list is not inclusive." In another paper from Ornis, they acknowledge, "that an ongoing project for Rainbow Technologies, a device maker, has been to greatly reduce the failure rate of their dongles."

We must remember the software manufacturer does not act alone. They are also dependent on and their products must interact with the dongle vendor that makes the hardware device and software drivers, as well as the operating system vendor, such as Microsoft, Apple or Red Hat and Linux. It can be weeks or months before a problem is reported, then...
identified, tracked down and finally resolved.

So what would be a reasonable time to wait for the company to cure a problem? How long could the INS have waited to print passports and travel documents? I submit that the very event itself is too much.

One of my clients is a worldwide company called Stratus Technologies. They are headquartered in Massachusetts. They manufacture servers to run mission critical applications. Among their clients are the United States Federal Agencies. Stratus servers are currently being used for defense, financial intelligence and aviation mission critical systems. With these systems, access control device failure is not even an option. Therefore the company with the full knowledge and approval of the software vendor has used my software to replace the hardware dongle which has allowed their customers to enjoy a 99.999 percent uptime of their servers.

This is clearly one example of how the availability for copyrighted works has increased since the passage of the exemption and that the market of copyrighted works has gone up as well. I would love to live in a world where companies were responsive to their customers' needs and trusted them. But to hope
that a company would provide a copy of the work in a form not protected by an access control device is a little much to hope for. After all, if they trusted their users then why would they have used the access control device in the first place.

The third requirement they mentioned suggests "that there must be a non-infringing work available in unprotected form that is equivalent to, or would serve as an adequate substitute for a specific digital work that is protected by an access control measure and would otherwise be subject to an exemption." I don't believe the SIIA is specifically referring to the hardware lock/dongle access control problems I'm speaking about. I think we all know that there is a tremendous amount of time that is required to learn a new software program, even if it is in the same field. Trying to determine what would be an equivalent program would be a nightmare, not to mention the costs involved in buying new software and training people to use it.

I have a letter from a lady named Janice Lourie who has authored books, articles and is the holder of several software patents as well as a graphic artist. She spent over two years mastering a program called "Elastic Reality" which was bought by
Avid. Avid later disconnected the product and incorporated some of the features into other products but not all the features. Asking someone to invest another two years to train in another program rather than remove a problem device is not a practical solution.

The last point I would like to raise in regard to the SIIA reply comment is the same comment they made three years ago. Mr. Wasch says that there are easy real-life solutions to the concerns alleged in some of the comments. He states that "there are numerous third party companies that offer to escrow software code in confidence. If users are concerned about having access to code due to malfunction or irreparable damage to the access control technology or due to the demise of the copyright owner's business, they can use these trusted third parties to escrow the software to ensure future access to the content if such an event was to occur."

The flaw in this thinking is the same as it was three years ago. Software code is only possessed by a developer not an enduser, so it is up to the developer to escrow the code. Since it is not mandatory for developers to do so, no matter how concerned a user may be they still are not going to
have access to the code and they will get no relief.

But I'll just pursue this for one more second. Let's suppose there the manufacturer had escrowed the code and a few years later went out of business. We've happen to get very lucky because when one of us calls up a year or so later the phone is still connected and we hear a phone message saying "Sorry we've gone out of business but you can check with XYZ escrow company where our code is located if you are having a problem." I'm sure we all in this room have some computer experience as an enduser. I wonder how many would be able to read that source code in the language it was written in, perhaps C, C++, Paseal or maybe Assembly language. Then find the programming tools needed and have a few thousand dollars laying around that we don't need to purchase those tools to compile the programs to build the software to debug the program of errors. Did I mention the time it takes to actually do all that. As you can, the very notion is humorous.

On the BSA, in the joint reply comments submitted by the firm of Smith & Metalitz and others, the author's only argument to the renewal of the exemption is that there is not enough evidence on record at the time of his writing. So hopefully I've
been able to build the record to their satisfaction. They have also expressed the same concern as the SIIA of a requirement to seek the assistance of the copyright holder which I've already addressed.

There has been no harm to the industry. So many of the opponents have in words the lawyers like summarily dismissed the comments of others in this proceeding claiming that the commentator did not provide enough examples. Allow me to turn the tables for just a moment. It should be noted that nowhere in these proceedings has an commentator presented real evidence that there have been any negative impacts as a result of these exemptions going into effect. In the reply comments of Mr. Metalitz, he states that there are no reported nor unreported cases that he is aware of that would show that the provisions have had a substantial adverse impact.

The industry has continued to grow with the exemptions in place and this with an economy that has not been its strongest over the past three years. Companies such as Aladdin Knowledge Systems, makers of some of the access control devices along with Rainbow Technologies have continued to grow. Documents I have included show in the case of Aladdin, through the years 2000-2002, a steady increase in sales and a
record fourth quarter for the year ended 2002.

In the case of Rainbow Technologies, in Quarter 4 2001, they report a strong finish with increased revenue and operational profitability. In Quarter 4, 2002, the company reports a 19 percent quarterly revenue growth and significant improvement in operating income. In Quarter 1 2003, they announced strong results and a fivefold improvement in net income quarter over quarter.

Technology is changing again. I've included several articles that show that three and a half inch floppy drives are following the path of the five and a quarter inch drives, vinyl records and eight track tapes. Some disks are protected with access control software making it impossible for the Library and educational institutions to make archival copies. Misters Carless and Kahle of the Internet Archive have already listed programs that they are unable to back up because of the dongles. Next will be software programs on floppy disk protected by access control software that they will be unable to transfer to other media.

As I said earlier, it has been three years since I sat before you and presented testimony which was very similar to today's. Unfortunately the
problems that we discussed back then have not gone away or have been cured or are likely to be cured again in the next three years.

We can look back over the last three years at the results of the first rulemaking. The availability of copyrighted works has increased as in the Stratus example. Libraries and educational institutions can now archive access control protected applications onto other media.

The value of copyrighted works has increased as in the Department of Justice/INS example. Relief is now available to legal users, after the copyright holder has already been compensated to continue to have trouble free use and access of their software as in the case of Ms. Lourie and the many other examples included. No evidence has been presented to show any type of adverse effect to the industry.

Since Congress has not yet acted, it is once again up to this panel to provide the consumer with relief in granting a renewal on the exemption of the second class of works, those protected by access control mechanisms that fail to permit such access because of malfunction, damage or obsoleteness. Thank you.
CHAIRPERSON PETERS: Thank you, Mr. Hernan.

MR. HERNAN: Good afternoon and thank you for the opportunity to testify here today. My name is Shawn Hernan and I'm the Vulnerability Team Leader at the CERT Coordination Center at Carnegie Mellon University. The CERT Coordination Center is part of the Software Engineering Institute which is a Federally funded research and development center dedicated to helping others make measured improvements in their software engineering capabilities.

The CERT Coordination Center was established in 1988 by DARPA to provide coordination and leadership in response to Internet security emergencies. Today we continue that mission with funding from the Department of Defense, the Department of Homeland Security, the Secret Service and other law enforcement and intelligence agencies. Among other functions the CERT Coordination Center is a leading provider of information about Internet security vulnerabilities.

Intruders cause billions of dollars in damage each year by compromising and disturbing the information systems upon which the U.S. economy is dependent. Many estimates of the damage caused by
computer intrusions and viruses exceed $14 billion which is the approximate annual revenue of the U.S. recording industry.

Poor information security is a large and growing threat to the economic vitality and national security of the United States. Furthermore none of the incidents seen in the last few years have even approached the level of damage that is possible. Despite the billions in dollars of damage so far, I believe we've been lucky.

At the heart of this problem are the vulnerabilities in computer software. Publicly disclosed vulnerabilities in computer software have skyrocketed from 262 in 1998 to more than 4100 in 2002. Unless vulnerabilities in software are dramatically reduced, system operators will be unable to evaluate and remediate even the most serious vulnerabilities. More research is urgently needed into the ways to reduce software vulnerabilities. However the DMCA is having a chilling effect on that research at the CERT Coordination Center.

Often when a researcher discovers a flaw and the software vendor disputes the finding, CERT is called upon to act as an arbitrator of technical facts. We've recently encountered exactly that
situation while investigating vulnerabilities in software from Adobe and ScriptLogic.

DMCA and other copyright issues were raised in the course of both investigations. In each case we were able to establish the facts with a minimum of disagreement. However, less scrupulous vendors could use unfounded threats of DMCA prosecution to stall or halt our investigation. Our concern has not arisen in a vacuum but is based in part on the actions others have taken in response to DMCA.

In August 2001, Niels Ferguson, a highly respected cryptographer, self centered his own work describing flaws in a video encryption scheme developed by Intel. He did this because in his words "I would go bankrupt just paying for my lawyers."

In September 2001, Dog Song, a well known and respected programmer and author, replaced the contents of his website with a single sentence, "Censored by the Digital Millennium Copyright Act."

In April 2002, the IEEE for a brief period of time required authors to certify that their work did not violate the DMCA. In July 2002, Hewlett Packard Corporation threatened SNOSoft with action under DMCA for publishing information in tools designed to
demonstrate weaknesses in HP software. The threat came after CERT had already been in contact with both HP and SNOSoft regarding the flaws.

In October 2002, Red Hat refused to disclose details about a security flaw in their operating system for fear of violating the DMCA. According to the site that had the details, the information could only be shared with non U.S. citizens. And there are the well publicized cases involving Ed Felton of Princeton and Dmitry Sklyarov of ElcomSoft.

For those of us with computer security expertise, the result of these cases has been to instill fear in law abiding and responsible researchers. At the same time, I know from my experience in the CERT Coordination Center that the activities of those who would use knowledge about computer security to compromise computer systems continues unabated. It is a classic case of the law of unintended consequences. Quoting Richard Clark, former Director of the U.S. Office of Cybersecurity at the White House, "I think a lot of people didn't realize that it (DMCA) would have this potential chilling effect on vulnerability research."

I'm here today to ask the Librarian of
Congress to take those steps within his power to remove the fear, uncertainty and doubt that the DMCA has caused for me and for others in the security community. The exemptions in section 1201 for security testing and encryption research suggest to me that it was not the intent of Congress to hamper security research.

Unfortunately the exemptions are imprecise. The exception for encryption research does not provide any protection for other kinds of security research including vulnerability research. The security testing exemption requires the testing to be done for the purpose of protecting one's own system or sharing the information directly with the developer of that system.

In addition the very definition of security testing requires that the owner or operator of a computer system consent to such testing without clearing defining the meaning of ownership in a world in which software is routinely licensed. While these requirements may sound like good public policy on the surface, they rest on the assumption that the software developers are operating in good faith. Unfortunately in practice, the DMCA provides unscrupulous software vendors a means to suppress vital research and
criticism.

For one example of how the seemingly sensitive rules of DMCA fail to work in practice, consider that many legitimate licensees of software are unable to submit reports to a software manufacturer without purchasing expensive support contracts. This leaves a researcher in a quandary. Shut up, pay for support or risk prosecution.

In cases where the developer has gone out of business, there is literally no one who can receive the information. In other cases the developer has stopped making updates to a product that is still widely used and vendors will not often acknowledge or correct flaws in unsupported software.

A faulty assumption underlying section 1201(j) is that any given vulnerability is confined to a single vendor. Software is often derived from a common source or written according to a common standard. This results in software flaws which are shared across many vendors, sometimes numbering into the hundreds.

The time and effort required to notify a large community of software vendors securely often exceeds the resources available to average researcher. This leads the researcher in another quandary. Shut
up, assume the full burden of handling the problem through to the end or risk prosecution. A researcher may choose to report such flaws to the CERT Coordination Center or another coordinating body, though section 1201(j)(3) suggests that the security testing information must be shared directly with the manufacturer of the software.

We see vulnerabilities every day in our work and reducing them will not be easy. It will require investment in new research. But in its attempt to provide intellectual property protection, the DMCA in effect stifles fair, open and responsible criticism. It may appear to consumers as though all software is equally poor and vendors feel no pressure to change. Instead we should be doing all we can to create market incentives for software manufacturers to focus on product quality and to invest in research to ensure that quality. Public attention on existing vulnerabilities is the best way to create these incentives so that the long standing flaws we see again and again in software products can finally be eliminated.

I believe these examples and arguments have shown that the DMCA is having a chilling effect on computer security in general and scholarship and
criticism in particular. That is in no one's interest but better security is. As security increases, software manufacturers will have higher quality, more secure products to offer. Users will benefit from greater assurances that their information is safe and secure and content providers can have greater faith that their product remains in the hands of licensees.

I do not believe the intent of Congress was to diminish computer security research or divert talented individuals to other fields. The protections included in DMCA for encryption research, security testing and privacy lead me to believe that these were valued activities that were specifically intended to be protected. But the protections are vague and the environment litigious resulting in precisely those effects.

We hope that Congress will address the shortcomings in DMCA to clearly and unambiguously provide a safe haven for security research but we recognize that this is not the forum for such requests. In absence of more comprehensive Congressional action, we respectively ask the Librarian of Congress to adopt the exemptions proposed by the CERT Coordination Center. Thank you.

CHAIRPERSON PETERS: Thank you. Mr. Band.
We missed you this morning. You have been at every one of our hearings.

MR. BAND: This is my swan song, I guess. I'll try to make it good. Thank you very much. Last week, the "Washington Post" published a startling photograph of rooms stacked from floor to ceiling with books that had been saved from looters at the National Library in Baghdad. Apparently a Shiite cleric pictured in the photo feared that these precious books and manuscripts would be looted so he arranged for them to be moved to an empty room at a nearby mosque where he could watch over them.

One of the great ironies of the technological innovations in storage media is that those ancient books from the National Library in Baghdad have a better chance of being accessible to future generations than much of the content produced in this country over the past 100 years. This is because the innovative forms of storage media rapidly become obsolete as they are superseded by seemingly better storage media.

As you well know for sound recordings, there have been metal disks with small notches, paper rolls for player pianos, wax cylinders. Remember the 45 RPM singles, the 33 RPM LPs, reel to reel tapes,
cassettes, 8-track tapes, digital audio tapes and now
the CD. It is very difficult if not impossible to
purchase players for all of these media except for
cassettes and CDs. And even cassette players are
becoming scarce. A similar progression has occurred
with computer media. For years, PCs have not been
able to read 5-inch floppies and many PCs today cannot
even accept a 3.5-inch diskette.

In addition to being prone to
obsolescence, innovative technology is exceeding
complicated and therefore prone to malfunction. A
modern PC operating system has as many components as
a Boeing 747. Just about anyone who has purchased a
PC has had the happy experience of dealing with tech
support as he has attempted to install new software or
get the PC to perform as it should.

Our collective personal experience with
the obsolescence and malfunction of technology make
the necessity of this exemption intuitively obvious.
Just as we know that the sun will rise tomorrow, so
too we know that access control mechanisms will fail
to permit access because they will malfunction or
because they will become obsolete. We all know this
to be true so we really don't have to debate the need
for this exemption. Yet some commenters have argued
that the proponents of this exemption have not provided sufficient evidence of the need for this exemption.

In addition to all the evidence that Mr. Montoro is offering today, the Internet Archive has provided at least half a dozen separate concrete examples of obsolete access control mechanisms that must be circumvented to enable lawful uses. But for these commenters, I fear that no amount of proof will be sufficient. I suspect that they're opposed on principle to any exemptions.

Now other commenters recognize the obvious need for this exemption but seek to limit it by requiring that the lawful possessor of the copy first request assist of the copyright holder. To mandate this approach in all cases would be extremely inefficient and burdensome to the user. He will have to find the current corporate incarnation of the copyright holder. He then will have to contact the copyright holder and wait for a response that may never come. If a response does come, it may direct the user to send the copy at the user's expense to the copyright holder. The user may then have to wait weeks or even months until the copy is returned. To prevent these abuses, the Copyright Office would have
to develop a highly regulatory exemption with deadlines, depute resolution mechanisms and so forth.

The current market-based approach makes much more sense. In the vast majority of cases, the user will first turn to readily identifiable copyright holder because the user will possess the technical expertise to circumvent or because the circumvention will be inexpensive and the user will hope that the copyright holder will stand behind its product.

There will only be a handful of cases where the copyright holder will still be in business but the user will have the sophistication to circumvent and it will be cheaper or faster for the user to do that than request assistance from the copyright holder. These few instances will not measurably harm the copyright holder. The Copyright Office need not worry about them.

In sum, the Librarian got it right the first time and should renew this exemption. Thank you very much.

CHAIRPERSON PETERS: Thank you. Mr. Sulzberger.

MR. SULZBERGER: Thank you. I'm Jay Sulzberger and I'm here representing New Yorkers for Fair Use. I was a little bit puzzled as to what to
say on this panel because seemingly this particular panel is about very specific harms or very specific parts of a big complex law. But as a matter of fact, I've been provided by the first three panels with a parade of horribles.

Mr. Montoro seems to have an 86 page parade of horribles. Of course, CERT has the most extraordinary parade of horribles, things that one would not have thought could happen in America, things that one would have expected from the old Russian Communist Empire. Of course, Mr. Band has just brought up the problems of the spontaneous or planned looting of ancient libraries of Earth's heritage.

I was going to try to make what I thought was a difficult argument that we should not be discussing particular exemptions to particular anti-circumvention clauses of the DMCA. But I think that with the three panelists before me that the pattern is clear. There is no excuse for any anti-circumvention law in the United States of America because in each and every case it is not that we have a parade of particular offenses against good sense, offenses against our freedom, attacks on free markets, attacks on scientific research, attacks of artists' rights, attacks upon our rights of free speech and the most
important, a fundamental general and effective attack
upon our present right of private ownership of
computers.

Computers today are printing presses and
it's shocking. I have certain conservative
tendencies. I'm also sympathetic to the Socialists
but the idea that everybody who is a member of the
middle classes can pick up a computer for $300 and pay
their $20 a month and get Internet access and set up
a webpage, it's shocking. Democracy is one thing but
mob rule is another. Yes, there's nothing that
America can do about this. I hope there isn't but it
looks like there is.

The DMCA's anti-circumvention clauses in
combination with the loose association, alliance of
cartels, oligopolies, monopolies, which I term the
"Englobulators" is in the process of placing spy
machinery and remote control machinery at this very
moment into every single Intel motherboard that's
going to be sold in the new year. When Microsoft
completes the software part of its system of DRM
called Palladium, this will end completely your right
of ownership, your right of private use of your
Palliated computer.

Now a question arises. It can't be true
what I'm saying. I'm a nut. I'm an extremist. I'm
strident. Yes. But I'm not nearly as much of a nut,
I'm not nearly as much of an extremist and I'm not
nearly as crazy, vicious, strident as the
Englobulators.

The question arises. Why hasn't the press
picked up on the fact that I'm the less extreme of the
extremists? I believe in the Constitution even though
I didn't sign it. That's my anarchist side. I think
there is something to the first 10 amendments and we
should take the Fourth Amendment very seriously. I
think also the Fifth has something to say about
takings.

Why doesn't the press get it? A very
simple reason. I'm talking about rights and power.
I'm talking about fundamental rights of ownership,
fundamental rights of free speech, fundamental rights
of free association using our Internet and our
computers. Because in practice today, most people run
a damaged, malfunctioning and obsolete operating
system usually called Microsoft Windows or several
versions. Copyright law has already been dreadfully
misapplied in the past 20 years to prevent people from
gaining control of their property and their house.
It's pretty important property.
We know that Microsoft and as a matter of fact, all other vendors and makers of source-secret operating systems, it's almost impossible not to given into the temptation to spy somewhat when you are ether connected to the Internet. Sun has done it. Other companies have done it. It's mainly Microsoft because it was only after 1990 that the Internet became widely spread although some of us had email in 1970. But now, most people have a computer. It's their means of personal communication. It's also their means of authorship. It's their means of publication.

Let me deal with the accusation of copyright infringement. Yes, sure. There can be a heck of a lot more very serious copyright, the most dreadful sort because there are computers in the Internet. I don't give a good God darn about it. The invention of writing was dreadful to the ancient honorable profession of the singing poets. The invention of the printing press did terrible things to the Catholic Church's position in Europe particularly once the Bible was translated and then printed.

Things change. The cries of a small unimportant industry, I mean the whole of the "content providers." I, of course, refuse to admit that there are any more content providers. I reread my own stuff
and enjoy it much more than Disney has made since about 1935. I stand equal to them by the way. New Yorkers for Fair Use, one of our favorite tropes is "Nonsense, we're not consumers. We're owners and we're makers."

Let me try and outline what anti-circumvention laws do and what they're about to do. This is one of our standard pieces of propaganda. We've been handing it out since last summer. "We are the stakeholders." Why do we say "We are the Stakeholders"? It's an old joke. Everybody knows this. I'm sure this is not the first person to say.

In Washington parlance, what is a stakeholder? It's some organized group that can afford a full time lobbyist. That's all.

The bizarre spectacle of course of seeing small private interest, when I say small, I mean small. The cotton subsidies last year in the United States were about 40 percent the gross of Hollywood. You don't see huge articles about particular laws and the deep struggle and the basic principles over how much of a subsidy they should get.

I'm not sure I'm actually going to read this whole thing but Freedom one, you may buy a copy of a movie recorded on DVD. You may watch this movie
whenever you please. You may make copies of this movie, some which may be exact copies and others may be variant copies.

We all know that the legal underpinning of DRM is anti-circumvention. In the future, you won't be able to do that. Now this is an assault of private ownership of computers. This is absurd. Let me just say and you all know this, Ernest Miller and Joan Feigenbaum both of Yale have suggested that this is just a mistake and it will soon be corrected.

Copyright law shouldn't say anything about private copy. In the first place, technically it's going to be very hard. You're going to have endless of the most difficult subtle things. For example, there's something on a news spool. Is that a copy or is it something in transmission?

The nature point which will defend us against the dreadful assault on private property which is the all the anti-circumvention clauses of the DMCA is to draw a nature line inside your house. You have a copy of something. If you have lawfully obtained it -- By the way, we're not copyright extremists. I myself am a big supporter of the GPL which is a somewhat strict copyright license. I consider it to be part of the one main foundations of the success of
free software. If you don't draw the line and you seek for exemptions, you'll have to make hundreds of exemptions. Even if you enforce them and you could enforce them, the principle would remain. You don't have control of your machine. You have to get lobbyists or grassroots organizations to come to Washington to appear before every three years and beg on bended knee for a particular exemption.

We don't have to do that. You are allowed to turn to Congress and say "We've seen the parades of horribles and there's not just one parade." All of the people here arguing for exemptions, the principle is the same. These people can't reach into your house and tell you what to do. It's absurd.

I'm going to try to avoid discussing the other side of the bundle of rights that these people want to take away from us, the rights of free publication, the rights of free dissemination which are of course restricted by copyright which I support strongly. I don't think it right that I should go down and steal a movie without paying for it and set up a movie house and charge admission for it.

I'm sorry. I lose my track on one of my sentences before. You know the Xerox machine. It's always the same structure you all know this year. The
people who have the old methods of publication think
their methods have to go on forever. Always the word
"business model" is used. We're not worried about
their "business models." We're worried about our
computers and our rights.

I believe it is within your commission to
turn and say we've had it. What are we going to do?
Do we have to have these hearings every six months?
We're going to have to have ten of you up there and a
hundred of us here explaining the absolute terrible
things that anti-circumvention laws in the United
States do to markets, do to freedom of speech, do to
development of better computer, etc., etc. I think
you can turn and say "We've heard enough."

We would suggest that Congress reconsider
the entire bundle of anti-circumvention clauses of the
DMCA. If I'm asked specific questions, I would be
happy to try and connect by at most three half steps
any particular anti-circumvention measure to truly
horrible and very large scale things. Thank you.

CHAIRPERSON PETERS: Thank you. Mr. Mohr.

MR. MOHR: Hi, my name is Chris Mohr with
Meyer & Clipper on behalf of the Reed Elsevier. Thank
you for the opportunity to testify and offer our
perspectives over the last three years. I represent
Reed Elsevier, a leading publisher of a variety of products including trade publications, educational works and electronic databases. We invest millions in the creation and distribution of copyrightable content.

Our position in this proceeding is simple and that is no exemptions should apply to databases of any stripe. The reasons for this are laid out in our comment and I'm only going to summarize a few key points here.

This is a very different proceeding from what happened three years ago. In 2000, we had no record in front of us. Any judgment that was made by the Copyright Office at that point in time was by definition predictive because the Statute had not yet gone into effect. Now we are benefitted by three years' worth of a rearview mirror in which we can gaze.

The Office had made the rule surrounding this proceeding clear. The burden is on the proponents of an exemption to offer evidence, not theoretical critiques, not policy reasons, as to why the Statute never should have been enacted or suggestions on how to revise existing defenses that might be in the Statute.
The Notice of Inquiry asked for "concrete examples or cases of specific instances in which the prohibition on circumvention of technological measures controlling access has or likely to have an adverse effect on non-infringing uses. It would also be useful for the commentor to quantify the adverse effects in order to explain the scope of the problem, e.g. evidence of widespread or substantial impact through data or supplementary material."

This puts the burden on the proponents in two significant ways. The first is to identify verifiable, non-infringing uses that they've engaged in under the existing exemption. The second is to identify causation, that these are in fact due to the existence of the prohibition. Then at the end of the day, there is still a balancing requirement that has to be done on the benefit of these access controls on non-infringing uses.

Now Mr. Montoro has submitted what we think is -- and frankly I have no way to draw any opinion on what might be or might not be attached to his written comments because I haven't seen them. So to the extent that he has attachments, I don't know what they are. I can tell you that to the extent that he's offered actual instances of government agencies
and his relationships with government agencies, that
isn't relevant evidence for the simple reason that
circumvention done pursuant to contracts with
government entities is exempted under 1201(e).

Thus far our position is as it was in the
initial going. Now again if he has other things that
relates specifically to hardware dongles and computer
programs subject to hardware dongles that may be a
record. I don't know. I haven't seen it. But as to
what I've heard so far, we don't think that there's
any exemption here.

As a side matter, we would also point out
that one of the things that ought to be considered is
the risk of what happens when stuff gets out of its
wrapper as of Friday has gone up. The Grockster
decision said that it's okay if you have basically you
know infringement is going to be widespread. You know
that's the primary reason that people are going to use
their service. You are not liable for anything that
might happen. It might be a rather bizarre
application of the knowledge standard.

If that is in fact legal, the risk to any
copyright owner of any circumvention of protection
measures is greater than it is now and it's already
pretty large. With that, I still have remarks about
the evening session. I looked at literally. So I'll shut up.

CHAIRPERSON PETERS: Thank you. Mr. Simon.

DR. EINHORN: Are you going to go out of order?

CHAIRPERSON PETERS: No, Mr. Kupferschmid.

MR. KUPFERSCHMID: Good afternoon. I'm Keith Kupferschmid. I have to say I've been called many things in my lifetime, some good and some bad. I've never been called an Englobulator. Is that what's it called?

MR. SULZBERGER: Englobulator. I think that's useful term of art.

MR. KUPFERSCHMID: So in actuality, I'm Vice President of Intellectual Property Policy and Enforcement at the Software Information & Industry Association. I want to first off express my appreciation for this opportunity to testify here today. I would like to thank the Copyright Office and the panelists in particular for conducting these hearings.

By way of background, SIIA is the principal trade association of the software and information industry. We represent over 600 high-tech
companies that develop and market software and
electronic content for business, education, consumers,
the Internet and entertainment. Our membership is
quite diverse. We have information companies like
Reed Elsevier, West, McGraw-Hill, New York Stock
Exchange. We have software companies like Corel,
Oracle, Veritas. We have DRM companies like
Macrovision, Protexis and Aladdin. We have others
that probably not so easily definable like AOL Time
Warner and Sun and a whole bunch of others.

So SIIA members represent a very wide
range of business and consumer interests. Our members
create and develop new and valuable access control
technologies for use by others seeking to protect
their copyrighted software and content with such
technologies. They use access control technologies to
protect their proprietary software and content. They
purchase or license software and information products
in other content and services that utilize these
access control technologies. So as you might imagine,
SIIA and our members are extremely interested in the
issues that arise in the context of this hearing.

Unlike many of the other companies and
individuals you may have heard from either today or
yesterday or in the future, we're really not on this
side or that side. We are really smack dab in the middle because of where our members are. Although our interests extend to many of the exemptions that are proposed, I will endeavor to limit my comments to three exemptions specifically talking very briefly about tethered works and thin copyrighted works and then also the existing exemption for malfunctioning access control measures.

As noted in our comments, SIIA believes that none of the comment submitted relating to tethered or thin copyrighted works either individually or taken as a whole provides sufficient factual evidence or legal argument to justify the creation of an exemption to section 1201(a)(1). With regard to the existing exemption for malfunctioning access control measures, we likewise believe that none of the comments submitted individually or taken as a whole provide sufficient factual evidence or legal argument to justify renewal of the exemption in its present form.

I will visit this issue since this is a topic of the hearing but first, we'd like to say just a few words very briefly about the other two proposed exemptions. First off, tethering, an exemption for tethering or access control measures that is for post
sale use is unwarranted and very much unwise. Many of the alleged problems and concerns with tethering and post sale transfers are presently being addressed by those software companies that do use tethering.

Alleged problems for those who upgrade their computers, change operating systems or transfer software to another person are based on incorrect or incomplete information. For example, users who purchase new computer or hard disk can contact the software company's technical support agent to get assistance in either reinstalling or reactivating the program that's protected by a product activation code at no additional cost.

In addition if the user reformats his hard disk or replaces his current operating system in most cases, reactivation will take place without that person even needing to contact the software company at all. I won't go into any more detail because our written comments do go into detail here and do provide a more detailed explanation of this.

To the extent that there is any basis to the concerns raised, the benefits of being able to curtail piracy and to improve customer access to these software products greatly outweighs any temporary glitches or inconveniences that might be occasioned by
some users. Once again we describe in detail these type of business models and they're adversely affected by these proposed exemptions. I won't go into detail here.

With regard to thin copyrighted works, there's a proposed exemption for thin copyrighted works, fair use works, pro se educational thin copyrighted works, pro se educational fair use, they should all be soundly rejected. First off, these exemptions were rejected in the first rulemaking. Secondly absolutely no new facts or legal arguments have been proffered that would alter the analysis or the decision rendered by the Library of Congress in the first rulemaking. Absolutely nothing new has been added to the record.

In addition because of the recently enacted TEACH Act, it creates an exemption that directly affects at least certain educational uses of copyrighted works protected by access control measures. At the very least, it would be unwise to create any pro se educational use exemption.

In the event that the Library of Congress disagrees with our views on either tethered works or thin copyrighted works or the existing exemption for malfunctioning access control measures, SIIA strongly
urges the Library of Congress to adopt a certain thresholds requirement that must be met before any organization or individual can qualify for an exemption. As I will discuss shortly, this is especially important for any exemption for malfunctioning access control measures.

These three threshold requirements should at the very least include the following:

(1) Any person or organization seeking to qualify for an exemption must have legal access to the work at the time of the circumvention. Mere possession of a work should not be sufficient for an exemption to apply. The person or organization seeking to avail itself of the exemption must have legal access to the work at the time of the circumvention. To allow otherwise would harm numerous business models used by copyright owners today and in the future to get their products into the hands of the consumers and would open the door to widespread what I'll call "legitimate piracy."

For instances, many software and information companies make their product widely available to users but access to the works is limited to those users who have a key. Password or product activation code are examples. To obtain this key, the
user must first license the product from the copyright owner. Allowing those who merely possess a copyrighted work to circumvent the access control attached to that work would adversely affect these business models to the disadvantage of many legitimate users.

Examples of business models adversely affected include the software as a service model, pay-per-views, and of course try-before-you-buy software. All these would likely not exist if anyone was allowed to circumvent the access control measures that prevent non-licensees from accessing the software.

2) The second threshold condition and this is the most important of the list that I have here is any person or organization seeking to qualify for an exemption must notify the copyright owner and give the copyright owner an opportunity to cure the alleged problem. When the user cannot access content that she has legal access to, it is usually more efficient for that user to contact the copyright owner to remedy the problem rather than taking it upon herself to circumvent the access control measure. I haven't heard anyone disagree with that.

In many cases the copyright owner will be willing and able to adequately address the user's
concerns. Frequently the only time users are unable
to obtain the assistance necessary to access a
protected work are only when the company is going out
of business or is not able to support the access
control used on their products. In those two
circumstances, a user can easily meet this threshold
requirement.

Also requiring that users contact the
copyright owner and give the owner time to cure the
problem will ensure that the copyright owner is aware
of the problem and can take steps to fix the problem
in the future. For example, Aladdin Knowledge Systems
is a software company, an SIIA member, who is affected
by this malfunctioning, damage or obsolescence
exemption. They will replace a damaged dongle for
free if they are contacted. If the customer contacts
Aladdin first, there will be no need for them to
contact a service like Spectrum Software.

It will also give the copyright owner the
opportunity to notify other users of the problem and
provide them with an appropriate technical solution.
But of course if they don’t know about it and if they
are never contacted, this never happens.

3) The third threshold is that there must
not be a non-infringing work available in an
unprotected form that is equivalent to or would serve as an adequate substitute for a specific digital work that is protected by an access control measure and would otherwise be subject to this exemption. I won't go into detail on that threshold condition because you have that in my written comment.

To touch upon the subject at hand which is malfunctioning access control measures, the reminder of my comments will be about that. None of the comments submitted provide a factual basis or any substantive legal arguments in support of the malfunction, damage or obsolescence exemption as it exists today. These comments merely recommend that this class exemption be renewed absent as evidence to the contrary.

In direct conflict with the requirements established by the Library of Congress, these comments fail to provide any justification for the Library of Congress to renew this exemption for another three years. Several of the comments suggest the burden should fall on the opponents of the exemption to prove that the exemption should not be renewed.

Placing the burden of proof on opponents of an exemption would have the effect of creating a perpetual exemption. Under this scenario, the
opponents of an exemption would have to prove something they are not in a position to know. While the opponents of an exemption may have a general idea of who is taking advantage of an exemption or how many people are taking advantage of an exemption or even what type of activity they are engaged in, often times they do not know this information at all and can only make rough estimates.

There can be no doubt that the burden of proving the need for a new exemption or a renewal of an exemption should fall squarely on those who are in the best position to provide evidence of the value and need for the exemption and the adverse effects that are likely to occur without one. For example, there is no way for a particular dongle company to know precisely how many of their customers or more significantly their non-customers contacted or use software Spectrum or similar companies to circumvent their dongles and whether the need for an exemption still exists for those companies. In fact, one SIIA member who produces dongles tried to get a list of Spectrum Software’s customers from them to ensure that only authorized users who are using their service but Spectrum Software would not divulge this list.

If there’s an explicit requirement in the
exemption that the copyright owner or dongle provider first be contacted by the circumventor, then copyright owners like Aladdin would perhaps have a better idea of the number of people wishing to take advantage of the exemption and perhaps be able to provide more information to the Copyright Office. Because the existing exemption includes no explicit requirement that the copyright owner be contacted first, there is no way for the copyright owner to know with any certainty whether anyone is availing themselves of this exemption.

Therefore the burden of proving that an existing exemption should be renewed must be placed on those who are engaged in the activity for which an exemption is requested. Since the only comments that were filed merely make perfunctory requests that the malfunctioning, damage or obsolescence exemption be renewed without providing evidentiary or legal support whatsoever, the Library of Congress must reject the request for this exemption.

Now although there is no evidentiary legal support for renewal of the existing exemption, there does appear to be some evidence that a subset of this class exemption could possibly be renewed. We do not believe that the level of evidence provided in the
written comments today has met the burden of proof required. But if sufficient evidence were to be provided at these hearings, we would not oppose the codification of a more narrowly tailored exemption for malfunctioning access control measures which causes or in the immediate future will cause damage to the protected work as noted in more detail in our written comment provided the exemption is subject to the threshold conditions that I mentioned.

Although SIIA would not oppose a sufficiently narrow exemption for malfunctioning access control measures provided sufficient evidence is provided to establish a need for such an exemption, we are certainly concerned about its abuse. A mere belief that the works may be susceptible to damage should not be enough to qualify for an exemption. The circumventor must have tangible, creditable evidence that supports a good faith belief that immanent damage to the protected work will occur. Otherwise this exemption could be misused by pirates and hackers merely by claiming that circumvention was necessary because they thought the protected works are or will be damaged. In addition, it is essential that the threshold conditions outlined by SIIA be incorporated in this exemption especially the second threshold
condition.

Before closing, I want to just mention a couple additional things. I heard from Mr. Montoro earlier where he quoted us in his comments. His quote if I have this correct is that we apparently said "Even with only a few examples submitted, the SIIA still recognizes a need for an exemption and is willing to give these commentators the benefit of the doubt."

Our comments don't say that. It's not in here. I give Mr. Montoro the benefit of the doubt also that he just made an honest mistake. But I encourage you to go to page 10 paragraph 2 of our comments which I will not reread and read the quote for yourself or read the whole paragraph.

In addition, let me just mention one other thing. I have a little show and tell for myself. Mr. Montoro, if you could actually pick up your link of dongles there, I want to make a comparison here. You see that and you see this. Companies are switching to what is called a USB lock. They are getting away from these dongles.

This is because quite honestly of some of the issues and problems that have been occurring with dongles. This is a lot smaller than that. It's a lot
more secure. It's a lot more effective. It doesn't have quite the same issues that arise with dongles. It's less likely to cause conflicts.

For instance, many dongles are one-sided so you cannot plug the printer into it. Or many dongles are also plugged into the SCSI port which also causes some printer problems. This is not true for USB locks like this one. This is made by Rainbow Technologies. After the hearing, I can give you some material to read up on that and give you a copy of this if you are interested. But it's just simply not true for USB locks which plug into the USB port itself or if you have many USB locks, you can plug it into a USB hub. It's easily bought at something like Circuit City or Best Buy.

The real conundrum we have here is that on one hand we are asked to address the problems of old technologies, problems people are having with dongles. Then on the other hand when we go ahead and address them, we hear complaints that "you're not servicing our old technologies." So we're really damned if we do and damned if we don't in many instances. This is just one example of that.

The last thing I'll mention is some responses and comments that Mr. Band had about the
Internet Archives. He referenced the fact that it's about the amount of information. If you look at the Internet Archives, you look at the amount of information that is supplied. Although I do have some issues with the so-called "amount" which I don't think is very significant, I'm not even going to focus on that.

I want to direct your attention to the quality and accuracy of their information because quite honestly it's just not true. This is not information from me. This is information if you go on their website itself you can find. We copied, cut and pasted and put it right into our comments. That was with minimal research. I'm sure you could find more inconsistencies.

Also with regard to something Mr. Band said, "we would oppose all exemptions on principles" or something of that nature, I think you heard me say the exact opposite here. It's just not the case. We want an exemption that is narrowly tailored to the specific, distinct, verifiable problems that are complained up provided there's sufficient evidence.

With that, I will close. I want to thank the Copyright Office and the panel for giving me this opportunity to testify here today. I'll pleased to
answer any questions especially follow-up questions since I have not seen this 87 page document. I'm very interested in seeing that and being able to provide you with a response. Thank you very much.

CHAIRPERSON PETERS: Thank you, Mr. Kipferschmid. Mr. Simon.

MR. SIMON: Thank you. Sure I'm working right? Thank you for giving me the opportunity to appear before you today on behalf of the Business Software Alliance ("BSA"). BSA members are the residual of the technology industry that doesn't belong to SIIA. As you proceed in this rulemaking, I would urge you to keep in mind a couple of what I believe to be important kind of facts in this process.

One fact is that access controls have now become a key tool in both anti-piracy and security technologies. That's important. Product activation is being utilized by a broad range of software companies, Adome, Intuit, Microsoft, Semantech. Security technologies especially important in today's world depend on access control to make firewalls, filters, intrusion controls and antivirus products work. Many think that the solution to fungus that is SPAM and that is invading our e-mail inboxes also lies with technologies like filters that depend on access
controls for their efficacy and effectiveness.

Second, the Statute creates a burden of a showing of harm in order for an exception to be promulgated by the Librarian. But I think that the way the Statute works is it's not enough to show that harm is evident or is potential but it requires a balancing test. It requires a showing that that harm outweighs the harm that would be created by the exception.

I believe that to be true because otherwise the whole Statute wouldn't work. The Statute was created because the Congress perceived that threats of piracy, theft and other crimes were sufficiently acute to create this universe of statutory rules. That was a Congressional determination. If you are to deviate from that determination and create an exception to their judgment, I believe that the burden is not only to find harm but to determine that that harm outweighs the original Congressional purpose.

The third thing that is important to keep in mind is the goal of this rulemaking is to correct problems not to rewrite the law. So many of the submissions that have been sent to you would you like you to rewrite the Act. I don't think that is within
the ambit of what this rulemaking was intended to do nor frankly with due respect that it's in the ambit of the Librarians's authority. It's important to keep that in mind as well.

So the DMCA struck a balance between copyright owners and users with the goal of fostering new markets so that broad segments of the public could access copyrighted materials in digital form. I believe that it has occurred. The tribunal rulemaking proceeding was intended to renew this balance and if demonstrably needed for limited classes of works to modestly recalibrate it for the ensuing three years. Just those three years, the Statute requires that they do an overall review every three years.

So just because you made an exception last time around for malfunction, damage and obsolete, the situation doesn't mean that the cases has to be made or presumed for the next three years. BSA members strongly supported the inclusion of this rulemaking in the DMCA because we believed that it provides the needed safety valve to ensure that the DMCA stays current and relevant as a marketplace evolves and develops. This rulemaking is in place to ensure the Statute functions well, not to rewrite the law, not to rethink it, not to undo it.
With that said, that throat-clearing out of the way, let me talk specifically about five issues. Since this is the only opportunity that BSA will have to testify before you, they include a couple of issues that are necessarily in the title of this evening's session. Those five issues are malfunction, damage and obsolete access controls; security research issue which was raised by the witness from CERT; contractual terms as a precondition for access; embedded software; and circumvention for the purpose of non-infringing uses.

With due respect to works protected by malfunctioning, damaged or obsolete controls, I would like to note that this exception as promulgated by the Librarian last time around is most probably inconsistent with the provisions of the Act. The Act permits the Librarian to promulgate exceptions in respect of classes of works, a subset of the category in Section 102 because this exception applies to all literary works, computer programs, etc. We believe that it fails to meet that statutory directive.

We also think that it suffers from a second flaw which is that the terms malfunction, damage and obsoleteness are never defined. What may be in Mr. Montoro's mind, a malfunction, may be in the
mind of the designer of the product, performance exactly as intended. What some folks view as an obnoxious access control may well be obnoxious. Don't buy the product. It may well be exactly what was designed and intended. So if you were to proceed down the path of trying to rethink this particular type of exception, I would strongly urge you to think through trying to define those terms rather than leave them as pregnant imperatives.

In this rulemaking, several groups have submitted statements in support for this exemption. By simply stating that the existing exemption be continued, ignoring the procedures of the Copyright Office that require each exemption to be reviewed de novo. I'll give you an example. Comment 18 from the Center for Electronic Law is typical. It notes that the problems at the Three Rivers Community Technical College faced when their contract employee left the college. Apparently he had the only password to a particular system. The college was unable to access the system when the contract employee was effectively fired because he wasn't doing his job.

Simply put this example does not demonstrate any failure or obsoleteness of the DRM. What this example demonstrates is that the people in
management failed in allowing only one person to know
the password to a critical system, never mind that
person being a contract employee. The factual
difficulties faced by this college are real. It's a
real problem but they have nothing to do with this
rulemaking. They have nothing to do with an exception
of the anti-circumvent rules.

Let me move on to a point that was raised
by Jonathan on the obsolescence issue which we'll come
back to in a second. But in effect, Jonathan argued
that technology moves along very quickly. We went
from 5-inch floppies to 3.5-inch floppies to who knows
what. Every time one of those things stops being
widely available, it creates a problem.

There is a perfect solution to that. Stop
technological progress. Stop moving from one format
to another. You'll never have anything that's
obsolete because you'll have a single standard for all
time. It will always be supported and it will be
perfect. I don't think that's how the world works.
Things move along. Things change.

Moving on, works protected by access
controls and circumventions needed to carry out
security research. This is a big deal issue for BSA
and its members. Many of BSA's members are in the
business of producing, developing, deploying security
products. This issue was specifically addressed by
the Congress in the law, not in the rulemaking, in the
law in section 1201(j).

I would suggest, urge to you that in those
circumstances where the Congress has already enacted
specific exceptions, the Librarian must proceed with
extreme caution in changing or expanding that
determination because you run very close to rewriting
the law. If the Congress thinks this exception as it
has drafted is inadequate, it has the prerogative to
do so.

BSA members include the leading security
companies and none of them support an exception. BSA
members have significant concerns that may propose
exceptions which would have a negative impact on the
security by creating an opportunity for the widespread
distribution of cracking tools. We are not in any way
suggesting that the kind of testing that CERT does and
the kind of testing that legitimate entities do and
the monitoring and disclosure that they do is anything
but indispensable. It is indispensable quality of
security that we provide through our products.

We are saying this is something very
simple which is we do not believe that the provisions
of the DMCA stand in the way of the good work that CERT is doing or in the way of the development and deployment and testing of better security products.

The second exception that the Librarian promulgated last time was kind of into space. It was with respect of what I will colloquially call "censorware" so various filtering products. The way that this exception was formulated in our opinion is again both imprecise and substantially over broad. I'll give you an example.

The way antivirus products work is you have a database of virus definitions which are generally protected by some kind of technological protection measure. What you do is you run those definitions to figure out whether or not the particular virus exists. You want those definitions protected because otherwise the bad guys get access to it and can work off those definitions to create viruses that you can't control. The way that your exception read last time "the compilations consisting of lists of websites blocked by filtering software applications" is probably broad enough to encompass web-based definition sets for whether it's an antivirus product or security products or filtering for SPAM products or a variety of other databases
which are used for security and integrity reasons.

I am not speaking to the issue which I think is what the Librarian was getting at which is being able to test the integrity of filters to make sure they were not over broad when filtering for things like pornography or other similar social issues. What I'm suggesting to you is if that's your intent, do it narrowly and don't inadvertently cast a shadow over important security technologies that are now an integral part of what we all depend on.

I'll say just two words about some of the submission which have urged you to create an exception for contractual provisions that may be associated with the -- I simply put to you that contract law is an important body of law and it is of right now not Federal law and as of right now not within the ambit of the Copyright Office or the Librarian of Congress.

The embedded software issue has become germane in your deliberations because of the Lexmark v. Static Control case. BSA has not and does not have a position on that case and its relevance to this proceeding for the following reasons: the fact is that this case is still under way; and that the principal causes of action asserted in that case have nothing to do with access control and 1201. They have
something to do with copy control. They have something to do with copyright infringement. Neither of those issues is the subject of this rulemaking.

The second and related point is that the Copyright Office has not traditionally treated embedded versus nonembedded software in any way differently from the other. Such distinctions should be avoided now and going forward. So the case before the courts is where it belongs. The legal issues before the court are not anti-circumvention of access controls. You should let the courts play out whatever they are going to play out.

The final point is circumvention for non-infringing uses. This is an issue that keeps on popping up again and again. I would simply like to share with you something that I learned at a conference at Berkeley which I attended some three or four weeks ago.

The issue that was being debated was whether or not you should permit circumvention for purposes of fair use. The question was asked of a rather distinguished panel of computer scientists. Ed Felton was among them. A computer scientist from MIT was among them. There were two or three others.

The question that was asked of them was
this. With today's technology, would you, some of the best computer scientists in the country maybe the world, know how to design a DRM that would permit fair use but would not swallow up the entire purpose of the Statute? As a pure engineering technological matter, can you do that? The answer came back the same from all of them. It was just two letters, one word. No.

I submit to you that these notions that somehow you can calibrate -- It's unfortunate. The current status of engineering technology does not permit us to calibrate based upon individual's activities quite that way. Maybe someday it will. Until such time, I would urge you to think very carefully and very long about exceptions for non-infringing purposes. I'll stop right there. Thank you very much.

CHAIRPERSON PETERS: Thank you. Are you ready? We'll start with David.

MR. CARSON: Keith, I have questions for you, having to do with what's been most simply stated at page two of your reply comments, the threshold requirements that you think should be required before one came up with an exemption along the lines of or a subset of the exemption that we currently have for malfunctioning, damaged or obsolete access controls.
You have three requirements. One is that
the person who is seeking to qualify with the
exemption must have legal access to the work. Another
you have to basically notify the copyright owner to
give them a chance to work it out and finally there
must not be a non-infringing work available in an
unprotected form that could do the job basically. The
first question, I assume your answer is going to be
yes. Do we have the power under 1201(a)(1)(a) to so
limit a class of works and if so, can you tell me how
you construe that statute in a way that gives us the
power to put those conditions on the class of works
that we exempt?

MR. KUPFERSCHMID: That's why I suggested
them as threshold conditions rather than incorporating
these straight into the class of works themselves
because even in your rulemaking last time in the
discussion pieces you mentioned quite of few of these
if not all of them as criteria that affected your
decision making process. So I think most certainly
you could include them as threshold conditions in
order to be eligible for any of the classes and then
define the classes in terms of characteristics of the
class of works.

MR. CARSON: But how is for example
whether Mr. Montoro goes to the software company to see if they can fix it first how can that be considered part of the definition of that class of works? It has nothing to do with the works. It has to do with what the particular person wanting to circumvent has or has not done.

   MR. KUPFERSCHMID: Like I said, by making them threshold conditions rather than incorporating this language into the specific classes, you're not defining the class itself by the use or the users. Do you see where I'm going?

   MR. CARSON: I see what you are saying but it's not helping me because I guess that leads me to the next question. Where do you find in 1201(a)(1) that we or the Librarian has the power to impose threshold conditions on who can use and take advantage of an exempted class?

   MR. KUPFERSCHMID: I don't see that it's not in there either. I certainly think you have the leeway to do that. I don't see any place where you would be prohibited from doing that.

   MR. CARSON: We can do it because it doesn't say we can't do it.

   MR. KUPFERSCHMID: There's definitely a process here where you are able to decide really what
should be exempted and what should not. These threshold conditions are one way of doing it. Like I said, I don't see any prohibition against you being able to do that.

MR. CARSON: The second question is still primarily for you, Keith. Sorry. To repackage a question that Mr. Kasunic gave to the panel this morning because maybe it will or maybe it won't help you out with respect to at least the first of those threshold conditions you would like to have imposed, 1201(a)(1)(d) says that "the Librarian shall publish any class of copyrighted works for which he has determined that non-infringing uses by persons who are users of a copyrighted work are or likely to be adversely affected" and the prohibition contained in subparagraph (a) in 1201 "shall not apply to such users with respect to such class of works for the ensuing three year period." How do you interpret 1201(a)(1)(d) and in particular, do you interpret it as allowing only people who are engaging in non-infringing uses to circumvent with respect to a designated class or do you interpret it as permitting anyone to circumvent with respect to a designated class once that class has been designated?

MR. KUPFERSCHMID: Certainly not anyone.
I've been part of the last two panel discussions and people have answered this question in depth. I don't want to repeat what they said that much but it certainly is not anyone. The end result has to be a non-infringing use.

The reason I put this in the threshold conditions is because the problem is if you don't see it there, people think "Oh, gee, it does apply to anyone and I don't have to be a legitimate user."

I've seen this on user groups, discussion, chat rooms. If it's not there in the words, in the "Here's the criteria", they are going to think it's not part of it and it will apply to anybody.

MR. CARSON: But I gather then -- I shouldn't gather anything until you tell me whether I should. Let me ask you. Based upon your interpretation of 1201(a)(1)(d) in terms of legal analysis not in terms of how people perceive it, doesn't 1201(a)(1)(d) really take care of that first condition that "the person or organization seeking to qualify for the exemption must have legal access to the work at the time of circumvention"? Is there leakage there?

MR. KUPFERSCHMID: I think from a legal perspective, I think you are correct. I don't think
there is leakage from my standpoint. But I can't separate myself and just put on my blinders and see what's happening in the rest of the world. That's why I'm suggesting this. It's because if it's not spelled out, the rest of the world is going to go "We have an exception for access control measures" without delving into what are the further criteria. So it goes beyond a legal criteria.

MR. CARSON: I follow. Thanks.

CHAIRPERSON PETERS: That's it? How about Steve?

MR. TEPP: Okay. Thank you. Mr. Carson wants that side so I'll come to this side. Mr. Band, I'll start with you. You are here as I understand it representing a number of organizations, libraries, law libraries and similar CERT organizations, a significant segment of which are part of institutions that are part of or state institutions. So my question to you deals specifically with that segment of the groups you are representing. The Supreme Court as you are probably aware has held that the state institutions and states generally have sovereign immunity from many Federal laws including Trademark Act and the Patent Act directly and through the Fifth Circuit's ruling it appears that it extends to the
Copyright Act as well. I think it's reasonable to assume to Section 1201 of Title 17. Given that general sovereign immunity from enforcement of Section 1201, what is the need for that segment of the people you are representing today for any exemption at all for any purpose under 1201?

MR. BAND: I guess there are several levels of answers to that. First of all, as you noted, that's only a subset of the people I'm representing and not the other people that I'm representing or our organization is representing. Secondly, there are various statutes pending in Congress that would - actually I don't know if they've been reintroduced this year but they've been there in the past and I'm sure they will be reintroduced - that would find various mechanisms to address that issue. So we're looking at this in the long term. Whether it's this Congress or the next Congress, I think eventually that issue will be addressed.

Another part of this puzzle is that it's conceivable that the institution might have sovereign immunity but it is far from clear that the individual librarian who actually engages in the activity would not be able to be sued under some legal theory either under the Copyright Act or some other legal doctrine.
As a result, it could be that the library itself, that institution has sovereign immunity, but the employee might not and might be subject to suit or could be sued in his individual capacity and so forth. So there is still some potential for liability and exposure to those individuals. I think also simply as a practical matter the institutions have been operating under the assumption that the copyright laws still apply to them, including Section 1201.

MR. TEPP: Let me follow up on that real quick on a couple of points just to get your response. The legislation that was out there last year as you noted has not been reintroduced. Do we have to consider whether there is a likelihood that it will be enacted in the next three years as part of any evaluation of exemptions with regard to those institutions? The second part, I'll just get them both out and then you can answer both. To what extent the remedies against the individuals in these institutions that you've referenced would be limited to injunctive relief and the extent to which injunctive relief after the fact is really a prohibition on the act of circumvention?

MR. BAND: With respect to the second question, the answer is I don't know. I haven't
studied it carefully enough and I could get back to
you on that. With respect to the first question, I
guess what I find curious about the question and
actually the whole line of questioning of course is
that these exemptions do not apply to individual users
or to classes of users.

The exemptions are applies to classes of
works. That was a position that the Copyright Office
took in the last rulemaking and I assume it's sticking
to that position that the exemptions are applying to
classes of works and not classes of users. If you are
willing to start entertaining exemptions with respect
to classes of users, then we're willing to talk about
that.

MR. TEPP: Okay. Thanks. Just to clarify
why I'm asking, obviously the scope of our authority
is something we've been asking about. I think there
clearly was some decision made last time but there is
still questions being asked. The statute -- I'll just
leave it at that. Thank you.

MR. BAND: But I would just as a final
note add that notwithstanding the sovereign immunity
issue there's still large segments of the library
community who would not be able to benefit from
sovereign immunity regardless of how it's construed
and its future.

MR. TEPP: Thank you.

MR. MONTORO: May I comment on that?

MR. TEPP: Sure.

MR. MONTORO: Thank you, sir. I had a comment to make which is also along this. Mr. Mohr also raised up that comment about the government already being exempt which I think is what we are talking about here that the Libraries Association or educational facilities for backup might be already exempt. But it doesn't really discount the examples any. These are still tangible examples of problems that can happen.

MR. TEPP: That's a different kind. I'm talking about the sovereign immunity issue. What Mr. Mohr was referring to was the statutory exception for government agencies within 1201(e). As long as you've raised that, let me ask you a question. Do you agree with Mr. Mohr that the activities you've cited where you're a contractor for a government agency do fall within the scope of statutory exception in 1201(e)?

MR. MONTORO: I'm not an attorney to comment legally on that. Even if it was true, I would simply say that again it does not discount the examples any of these problems happening in the
marketplace. If they can happen to a government facility or a government agency, they certainly could happen to other people as well.

MR. TEPP: Okay. Thanks.

MR. BAND: But also let me just add that it doesn't seem to apply to all activities of government authorities. It applies to lawfully authorized investigative, protective, information security, or intelligence activity, not everything else. So it may apply to some aspects of the INS but I'm not sure that even passport control would necessarily fall within that list of activities.

MR. HERNAN: May I follow up as well?

MR. TEPP: Sure.

MR. HERNAN: One of the particular issues we face at CERT being part of a federally funded research and development center is that the work we do is directly in support of the United States Government but we are encouraged and do receive private funding as well. We sit as a bridge between private industry and government organizations. That's one of our roles.

So it has been particularly of concern to us to what extent are we required to show that any particular activity we engage in is being funded by
the Government or being funded by private money. Although let me thank Mr. Simon for his nice comments about his work we think it's pretty good too. We don't know without any particular case law to back this up if our particular activities have to be documented as being funded pursuant to some Government contract or through private funding sources.

MR. SIMON: Can we ask questions too or not?

MR. TEPP: We've never gotten there but fire away.

MR. SIMON: I was just curious if CERT had ever been sued or if anybody had ever sent you a letter alleging that what you were doing was a 1201 violation.

MR. HERNAN: It has been intimated to us by some of our contacts not necessarily the legal or management contacts at software vendors but certainly our technical contacts have from time to time intimated that the research we would need to do in order to produce an advisory or another document may in fact be a violation of 1201.

MR. SIMON: Okay, but you've never gotten a letter or a suit filed against you or anything like that.
MR. HERNAN: That's correct but I think that has more to do with the fact that we are recognized as a fair and impartial organization than anyone's recognition that we aren't necessarily immune from that.

MR. TEPP: Mr. Hernan, let me follow up with what you just said because it's interesting to me. The statute 112(e) says "person acting pursuant to a contract with the United States". It doesn't appear to be interested in who's paying.

MR. HERNAN: I don't know. That is an open question to us and a subject of some considerable debate at least among the technical staff. Without any case law that anybody can point to and certainly with the concerns of individual prosecution, we don't know if we are acting pursuant and what are the requirements to show that the work we are undertaking is pursuant to a government contract.

MR. TEPP: Should I take it though that if you knew that you were acting pursuant to a contract that Section 112(e) would take care of all your troubles with regard to Section 1201?

MR. HERNAN: With a certain minor exception. As part of our FFRDC contract, we are legally limited in the size of the organization. We
can only employ 250 member in the technical staff
about 20 of which form the CERT Coordination Center.
Our mission as an FFRDC is to engage private industry
and bring best practices to bear in private industry.
To the extent that we cannot teach others who are not
acting pursuant to a government contract to do what we
do. It directly interferes with the core mission of
an FFRDC.

MR. TEPP: So then it sounds like your
primary concern is about trafficking in the
circumvention measures, talking to other people about
how --

MR. HERNAN: No, sir. My primary concern
is doing the research that is necessary to produce the
document which may itself be subject to the anti-
trafficking concerns. I know we have some concerns
there. But merely the act of doing the research
required to produce the document is of some concern to
us as well. So if we are in a lab testing a product
if we can't get past the anti-circumvention clause of
1201(a) to even be subject to the risk of 1201(b),
that concerns us.

MR. TEPP: I'm taking a long time. I
apologize. Let me try and wrap it up. If you got an
exception for 1201(a)(1) that allowed you to do the
research that you are interested in doing, you could do the research and create the document you're talking about, would you then though be unable to do anything with that document because of 1201(a)(2) or 1201(b)?

MR. HERNAN: 1201(b) I think we would be protected largely because the document is not designed primarily as a circumvention device although that's again lacking case law. Refresh my memory please again regarding 1201(a)(2).

MR. TEPP: That they are advertised primarily as a circumvention measure and whether they have substantial other commercial uses.

MR. HERNAN: Again not being a lawyer, I don't know how 1201(a)(2) would apply to that work or not. Being a non-profit organization, it's unclear to me how one goes about talking about the commercial value of our work.

MR. TEPP: Let me wrap this by just throwing it back to Mr. Mohr since you are the one who started us on 1201(e) to let you if you would like respond to any of the issues that have been raised and whether or not you think for example the notion of the INS being able to print passports which is something that 1201(e) would allow circumvention of the malfunctioning access control.
MR. MOHR: Frankly I think that's a protective activity even assuming that you read the statute that way and depending on how you construe the second clause. In other words, if you say that "this section does not prohibit any lawful authorized investigative", etc., then it goes down and says "or a person." So it's unclear as to whether the "or" stands by itself or a person acting pursuant to a contract or whether that's a subset of the investigative activity. But even if frankly the idea of the passport control isn't a protective activity, it doesn't really pass the laugh test.

MR. SIMON: Actually there's a more fundamental issue there because I thought passports were issued by the State Department. So what's Justice doing issuing passports?

MR. TEPP: That's definitely beyond the scope of the meeting. Thank you for your indulgence.

MR. MOHR: I'm sorry. Could I just add a few points to what you said about the threshold conditions? If you find that you have no authority to issue conduct based conditions such as a waiver or such as seeking lawful usage in fact that is not already in the statute, it would seem to me that the obverse is true that the record necessary to support
an exemption would have to be ratcheted up. In other
dwords, does that make sense?

MR. CARSON: If you explain it, it might.

MR. MOHR: Okay, fair enough. I'm
assuming that the language that you mentioned in
1201(a)(1)(d) I believe. I've been going back and
forth over that and I think Keith's reading is
probably right that it's built in. But at the same
time it talks about usage and determining is separate
from the class. So if that's the right reading of the
statute and you're going to exempt a class then what
is necessary to support the class is going to be much
higher than what it would be if the lawful use
requirement was already built in. Am I making myself
clear?

MR. CARSON: I think I follow it.

MR. MOHR: In other words, if (d) doesn't
build in the lawful use requirement, then we are
talking about a totally different level of record that
we need. That's the obverse of what we're talking
about.

CHAIRPERSON PETERS: Got it. Rob.

MR. KASUNIC: I just have a couple of
questions. The first relates to the balancing that
Mr. Simon raised that we have to look at in this
rulemaking. Assuming that there is an ample showing of harm that would support the exemption that we had the last time dealing with damaged, malfunctioning and obsolete, what harm has come to past in the past three years since we've had an exemption in place? How could you specify and quantify what harm has resulted to copyright owners as a result of that exemption?

MR. SIMON: I think that's the wrong question to ask.

(Laughter.)

MR. KASUNIC: But that's the one that's before you.

CHAIRPERSON PETERS: But he asked it.

MR. SIMON: But I'll try to answer it anyway. I just tell it the way I see it. You can have dongles which Mr. Montoro argues to us are needed to support obsolete situations where there is malfunctioning. But there's a high risk that these very same devices are going to be distributed for illicit purposes, for purposes of making unauthorized copies.

For example a question I would like to hear Mr. Montoro answer is what precautions does he take to make sure that his dongle-beating devices don't end up in the wrong hands. There is a specific
reason. Some years ago there were a couple of products called RivalLock and IceLock which were dongle-defeating software products using as one of BSA's members, CNC Mastercam. CNC Mastercam sued a company called ImagineThat which was then distributing those products.

A District Court judge in Connecticut held the court is not persuaded by the claim "non-infringing uses" offered for ImagineThat's products and finds that the products are not widely used for legitimate non-objectionable non-infringing purposes. The defendants have offered no creditable evidence that the products are widely used for legitimate non-objectionable purposes.

That company, ImagineThat, is a precursor of Mr. Montoro's Spectrum Software Company and in fact Mr. Montoro owned that company and was enjoying from distributing those products based on that ruling. So there is harm. There's a District Court that found the exactly identical tools in that instance with respect to CNC software products for causing real harm.

MR. KASUNIC: Before Mr. Montoro answers your question, I'd like to see if anyone else can answer mine. But is that then the result of this
exemption during the last three years?

   MR. SIMON: No, but this exemption would
create a further level of defense and a further level
of argument to argue in cases like this where while
there's very little evidence being presented that the
product is being distributed for a good purpose in
fact would be almost a justification.

   We have this problem right now in the
software industry in a different place in the law but
the same concept which is Section 117. Pirates
distribute pirated copies all the time. They say,
"No, this is permitted under backup and archival
copying under Section 117 so it's perfectly legal for
you to do this."

   I think I did last time during your
proceeding point you to literally dozens and some
thousands of websites where this is posted explicitly.
What we fear is that if this exemption were
promulgated in a very broad way, that it could be used
as a justification for piracy.

   MR. KASUNIC: One thing in that respond is
you used the word "could" and you used the word
"fear." We've already commented on those in our
circumstances being speculative. What I'm really
looking at is --
MR. SIMON: That's exactly the reason I suggested to you that the question you should be asking is the burden is on those to show that there's harm being caused by the current statute, not by the statute to defend itself.

MR. KASUNIC: I understand that and that's why I assumed in this question that we had evidence of the harm. We have had this exemption for three years. Is there any other specific idea?

MR. KUPFERSCHMID: Yes, if I can add. First of all, I want to say I agree with everything that Emery just said. But I want to go back and stress that second threshold requirement that I had about contacting the copyright owner, the dongle manufacturer because without that, we have absolutely no way of knowing.

We tried. We had one member company who tried contacting Spectrum Software who was using their services or using their devices and couldn't find out. Really there's just no way for us to know. Let's not forget who the burden of proof is on in this instance in this rulemaking.

So as it stands certainly if this threshold requirement is not included in some manner, we're going to be coming back here in three years and
three years and saying we have absolutely no idea. At least with that threshold requirement, we might have some idea of what's going on because then we'll have the people who are supposedly using this actually coming to us, the copyright owners, and letting us know. So we'll have an idea of what the harm is. But until something like that happens, we'll have absolutely no idea and it will be speculative.

MR. SULZBERGER: I'd like to address the question of harms due to the DMCA and actually earlier what I consider misguided laws about copyright and software. I would like to specifically address some of the supposed harms that would come to writers of anti-virus software.

You know real operating systems simply don't have viruses. For example, none of the Unisys have viruses despite the claims of the Microsoft apologists. There is no cause for any anti-virus software so there is no cause for any discussion now.

How come you can't go into a store and just buy an already loaded cheap IBM-style PC loaded with a free operating system? The BSA is of course partly at least a creature of Microsoft and they go around they terrify small companies and medium sized companies and government agencies and school districts
and demand that their licenses be shown to them.

At the same time, Microsoft's copyright license with the endusers guarantees the enduser the right to refuse the license and get a refund. The BSA stands with Microsoft in refusing to grant endusers relief from ever having to worry about anti-virus software.

Now I'm going to connect this with dongles too. Dongles are old and nowadays often limited piece of hardware and software which is indeed a form of DRM or copy protection. Microsoft in collusion with unfortunately Intel and other large manufacturers of CPUs and motherboards is in the process of creating a single dongle which is deeply embedded into the motherboard and the CPU. There will be no dongle business and there'll be no getting around dongle business when this happens. This is happening now.

The harm to consumers is simple. No matter what Microsoft says and no matter what the BSA says they intend to never allow any free operating system, one that doesn't have viruses, the ones that run the `Net, the ones that send your email, the ones that run most of your websites that you go to. They don't want to let those into people's houses.

The foundation, the legal underpinnings by
which they intend to prevent this is misuse of copyright law. I just wanted to address where the real harms are. We're not talking about small to small companies or dongle go-arounds or dongle helper companies or dongle companies. We're talking about the entire home operating system business.

The reason you have viruses and the reason your stuff doesn't work so well is because misapplication of copyright law and the failure to enforce the Anti-Trust Law. Every single anti-circumvention provision acts to increase the power of the present cartels, oligopolies and monopolies here. Thank you.

MR. KASUNIC: Mr. Montoro, I do want to give you the other side of question and how has this exemption specifically benefitted what you have been able to do in the last three years? How have you used this exemption?

MR. MONTORO: Thank you, sir. In the testimony that I've already given I gave substantial examples of the good that has actually occurred not only through the Department of Justice INS examples but through many others as well. These are real examples. They are all documentable. These are not fictitious. The people's names are right there. But
there are issues that were raised by Mr. Simon that I have to address and also some issues that I need to address as well that Keith brought up.

Mr. Simon, I just need to make a correction. It's Mr. Montoro. M-O-N-T-O-R-O.

MR. SIMON: I apologize for that.

MR. MONTORO: Thank you, sir. Now I don't know how much I want to get into the previous litigation that was going on back then. I only want to say that this was only a preliminary injunction. There was never any information that was submitted by the plaintiff which was done in a Connecticut court by a Connecticut plaintiff. If the issue would have been pushed further, I think the outcome would have been quite different.

One of the examples that was raised by Shawn and some other papers on our first day of hearings was Mr. Finkelstein I believe is the cost of litigation is so prohibitive against a small defendant that quite simply a lot of times a small guy can't afford to litigate these matters. At the time, that was the case. We just don't have the resources that companies with those kind of $500 million or $1 billion companies can actually come at us with. That's all I want to say about that at the moment.
I would also like to note that I don't think Mr. Simon ever did give Mr. Kasunic an actual answer to his question as to what harm actually ever occurred over the past three years that this exemption was in effect. I do have comments to make on Keith's comments as well.

I do agree with the SIIA on their try-it-before-you-buy software. Certainly that should not be exempt because the person does not have legal access to the full use of the software at that time. So there's no question there.

He brought up a company called Aladdin and said that "Aladdin will replace -- I'm sorry. Let me back up one more thing. Keith mentioned that in my testimony -- I have to go to the little glasses now. I'm not used to that. That's really different for me. That has changed in the past three years which is that I can't see anymore. It's terrible.

(Laughter.)

Anyway, the comments that I said was that Mr. Wasch says that even with only a few examples submitted, the SIIA still recognized the need for an exemption and is willing to give those commentators the benefit of the doubt. It goes to credibility which is why I want to bring this up. The actual
quote was "We are willing to give these commentators the benefit of the doubt therefore the SIIA does not oppose the codification of an exemption." If that sounds like I turned something around, I do apologize, Keith but I believe the point was still there and it's pretty accurate as I said it.

Also going to credibility, Aladdin Systems does make dongles. Keith mentioned that the company will replace a dongle for free. There's no need to contact either the manufacturer or my company or anyone else that might make a similar product. What I have to say is I respectfully suggest that it's just plain wrong. It's not even close to being accurate.

A lot of places these dongles are supplied and as I said I have the whole string set up here, these are blank devices that are supplied by the manufacturers of the device. Rainbow Technologies makes one. Aladdin makes one and other companies make them. It's very clear they supply the developer with a key. The developer then puts whatever information they want to put in there that's unique to that company. That's exactly the reason why Aladdin for example would never be able to replace a manufacturer's key because they would have no knowledge as to what's inside the key.
I don't want you to take my word for it. This is one of the papers that I brought in today.

CHAIRPERSON PETERS: Mr. Kupferschmid, you will have an opportunity.

MR. MONTORO: That paper is one by Rainbow Technologies. I'll be happy to supply one. Keith, I'm looking for that page that shows the technical problems with Aladdin and then right after that is the one by Rainbow Technologies. It's the page right after this one.

MR. KUPFERSCHMID: I have to jump in here for a second.

MR. MONTORO: Let me just point it out to you.

MR. KUPFERSCHMID: I have never seen this document and never heard about it until about an hour ago.

MR. CARSON: You can keep it, Keith.

MR. KUPFERSCHMID: This is 80 some odd pages and I'm expected to go through this and give an opinion right now. That's not going to happen.

MR. MONTORO: No, that's not necessary for this one issue that I do want to go over. I don't think that you would disagree that Aladdin and Rainbow basically made dongles and that these products
although they have their own benefits basically are the same.

What I do want to read is on problems that Rainbow documents. They have a question and answer, an FAQ section right there on that second paper, Mr. Tepp. The question is "Why do I have to contact my developer? Can't you replace my key?" The answer by Rainbow Technology is "A hardware key represents a physical license to an application. Rainbow has no legal ability to sell someone's software. Rainbow merely is a vendor supplying blank keys to our customers and not even we know the content of the key once it is programmed by our customers, the software developers. We know nothing of their application or how they implemented our product into theirs, nor are we licensed or contracted to support their customers..." I'll stop there but I think I've made the point.

One further thing regarding Kupferschmid's testimony is that Keith mentioned about USB keys. He asked me to hold these up so that everyone can see how big these things are and they are pretty impressive. He did show the new USB keys. Could you hold that up for me, Keith, so everyone can see that? Thank you.

Now I've also brought in some papers and
I showed you about the financials that I talk about that no one in the industry has been hurt. What I wanted to go over briefly just so everyone can see was that in 1998 only Aladdin, and not Rainbow but there are other companies that make access control pieces, 36,139 of these devices; in 1999, 44,691 devices; the year 2002 44,345; the year 2001 46,613; the year 2002 49,520. Obviously they are doing well. That's almost a quarter million devices. To say that an exemption is not needed for over a quarter of million people from this one company that have the devices of this size because now we're introducing a new device is completely wrong.

MR. SIMON: Mr. Montoro, since you are answering questions and I hope I'm pronouncing your name correctly this time.

MR. MONTORO: Thank you, Mr. Simon.

MR. SIMON: Could you help me out and give me some idea of what steps you take to make sure that the people who acquire your products are actual legitimate licensees of software?

MR. MONTORO: Yes, sir. You asked that question. I did address that actually in my testimony earlier but I will go over it again for you. What my company does first of all is that we have an order
form that the customer must fill out. That order form also includes a declaration basically that says they are the owner of the software and that they have tried to contact the developer and have not been able to obtain any relief.

The second thing that we do is we require the customer to then go ahead and send in a copy of a proof of purchase. In other words like I said earlier, a copy of an invoice, a packing slip, something that shows that actually that company is licensed.

The third thing that we would require if that's not available would be a declaration under penalty of perjury as in the example of the Department of Justice where they were not able to find an actual invoice because it was done so long ago. That's the first part of the question. I'm not finished.

The second part of the question is what happens when someone would get my software. How do we make sure that the software is not going and being distributed worldwide and not contributing to any kind of a piracy problem which really is an outstanding question?

I'd like to give you a great answer too. I will. I've been a developer for over 13 years. One
of the things that I've tried to do is make sure that
my software cannot have been installed, or if it is
copied, it gets copied, I'm sorry, not copied, it gets
transferred, it gets -- I know it's hard, isn't it?

MR. KASUNIC: It sounds like a DRM.

MR. MONTORO: Indeed.

MR. KUPFERSCHMID: It sounds like an
access control measure.

MR. MONTORO: It is.

MR. KUPFERSCHMID: Maybe it can be
circumvented on this exemption.

MR. MONTORO: And maybe I could make my
own software. Actually yes, it might be. But what we
try to do then is protect the client's software.
Let's say in your BSA case for MasterCam for example,
the software that I would distribute is Spectrum
software. It would read the lock device. Once it
reads the lock device it creates the software
equivalent to the dongle. We're not even bypassing
the security measure. This is actually a replacement
of the security key but it's being done in software.
That software piece is then actually tied to that
computer.

Could you please sit back a little bit,
Keith? It's nice to talk to you. Thank you. That
software is then tied directly to the computer by
certain things down in the registry and also by some
other things as well that I'd rather not talk about.
So that software then cannot be copied off of that
computer. We try to be responsible.

MR. SIMON: That's great stuff. And I
think that if the Copyright Office were to go forward
with some kind of exception in this area if it were to
implement safeguards like the ones that you described
which you have to authenticate the guy is a legitimate
licensee. You have to ask them hard questions. You
have to make sure that the software you're providing
them is not just spread all over the world. Those are
good safeguards.

MR. MONTORO: Thank you.

MR. SIMON: Our objection is not to your
helping out people who have a problem with technology
that's not working or some vendor has gone out of
business.

MR. MONTORO: And you and Keith made that
point.

MR. SIMON: Our concern is making that
when you are helping the guy who has a legitimate
problem you don't inadvertently end up helping out a
whole bunch of other people too who don't deserve your
help.

MR. MONTORO: I understand that point and my company has tried to be responsible in that way. Even when Keith in his paper brought up the three conditions essentially, we're not completely opposed to every condition as long there are safeguards that permit the use of that product or a use of a service to bypass that device or replace that device in the event that some things can't be done.

MR. SIMON: Fair enough. Thank you.

MR. BAND: If I may just jump in, the important point is that Mr. Montoro has a market based incentive to prevent his product from being distributed too far because then he's losing business. My point is that I think market-based solutions take care of a lot of these issues rather than trying to over regulate, even assuming that the Copyright Office had the authority to put all these conditions, which I'm not sure it does have. But assuming that it did have it, it's really not necessary given that in most cases the people doing the circumventing are people with highly specialized skills. He has a market reason not to want it to be overly distributed so he's going to take care of it himself.

MR. SIMON: I like his answer.
MR. KUPFERSCHMID: Let me just add also something Mr. Montoro raised early on in his comments which is he mentioned about how many of the dongles and these USB locks as well have been distributed and that Aladdin is distributing a lot more of these days. Yes, that's true. The reason it's true is because there's a lot more piracy these days. That's why there's a lot more demand for the dongles and for the USB locks. There are lot more software companies these days that feel the need for them. That's why their business has increased.

CHAIRPERSON PETERS: I noticed that your hand is up. However actually this is a formal hearing and the only people who can ask the questions are us and the people who are the witnesses. They have an opportunity to present their views but there's no way in this process that we can take anything else.

AUDIENCE MEMBER: I understand that, Madam Chair. I've heard so much fear, uncertainty and doubt --

CHAIRPERSON PETERS: I'm sorry. We're not going to put this in the record. Charlotte.

MS. DOUGLASS: I just have some quick one-shot questions. One of them goes to Mr. Sulzberger. I understand I think that we're not here to really
talk about fair use in general so whether or not the DMCA shafts fair use or not. I just wanted to ask about Palladium. What are the alternatives to Palladium? Why would you say "the end of the world we're not going to be able to do anything after"?

MR. SULZBERGER: I can think of many business models as they are called or fanciful projections, businesses. But if I had the same persuasive power not saying anything corrupt here in any simple way that the Congress of the United States as the MPAA and the RIAA, the American Association of Publishers has, I can think of many business models that could make me billions of dollars very quickly if I could get special laws by which the United States, police forces and the courts would protect my new businesses.

Here's a new business. I project porn on the side of buildings and I then debt people's accounts if they look at it. Now I could claim as a matter of fact under Copyright law that I need these special protections. After all, I own the porn in the sense of copyright because I hold the copyright. My answer is very simple. Things really do change. We don't build pyramids anymore. Faberge eggs haven't been made in some time. Actually stuff like Petrarch
wrote isn't being produced as much anymore. There are extraordinarily complex and actually heavy interactions between law, polity, custom, economics and human techniques of building things.

So today the music industry cartel of the most absurd sort is able to charge $15 or $20 for a CD of a few songs. I don't know. I've never bought one in my life. Now that the Internet has come and computers have come surely there is dreadful copyright infringement just as there is every single day when one uses the Xerox machine.

The answer is that Congress shouldn't pass laws to defend the special interests which are themselves gross violators of anti-trust law in the crudest possible sense and of course real copyright infringers as everyone knows. In a matter of fact if there were a symmetry in these laws, I would demand – Here's my answer to Palladium partly – that I be given permission to seize control of all the RIAA companies' computers so I could make sure they are not violating my copyrights.

After all, their company is somebody that's been convicted and have paid hundreds of millions of dollars for copyright violations. I have never violated a copyright in my life on any piece of
popular music. So it seems to me quite reasonable that I should be able to go to the Congress and say and I should be able to go to Microsoft and say "Give me control over their machines." The answer is things change. If it's no longer they can't make money by selling CDs or they can't make money by selling things over the 'Net if the trade-off is I give up my right to private ownership of my computer, I give up my right to privately e-mail, encrypt what I want to my friends, then I say "Good, there is no more such business." There aren't any buggy-whip companies today and that's because things change.

Once you get a sense that what we're talking about is a small industry, there'll be music. I make music for myself. There'll be music. There'll be performances of music. With the free Internet, we'll make movies and we'll make more music. We'll make it collaboratively. Already people have put together which is not as finished a product as the "Star Trek" movies but amateurs have thrown together a short "Star Trek" movie. Probably they would consider perhaps a copyright violation, the copyright of the only idea of the "Star Trek" universe. We don't need to give up private ownership of computers just to protect a few cartels.
By the way, one of the monopolies we'll be protecting is Microsoft because no matter what they say since they violate the law today daily in the most gross manner possible, they certainly -- They violate by the way copyright licensing as I pointed out. Why are they pushing so hard for Palladium? Because without Palladium, we're going to break through. You'll be able to really control your own machine and a free operating system on it and they don't want that. Let them die. That's progress.

MS. DOUGLASS: Okay, Mr. Hernan has an answer to that, too.

MR. HERNAN: I just wanted to be on record a little bit regarding Palladium. Palladium and its related technology, TCPA and now TCG, is a useful and powerful security technology that has legitimate uses. It is a tool like lots of security tools. With all due respects, Mr. Sulzberger, I don't think the scenarios of Microsoft trying to take over the world through Palladium and TCG are really within the scope of this hearing. It is a useful and powerful technology that can be used for good and bad purposes.

MR. SULZBERGER: May I briefly respond?

MR. CARSON: Is it pertinent to what this hearing is about?
MR. SULZBERGER: Yes. I said I would demonstrate it and I will demonstrate right now. What does Palladium do? It enables a person who is not the owner of the machine to run a Trojan which is heavily protected by effective technological measures as envisioned under the DMCA and makes it illegal for you to try and look and see what they are doing with your machine in your living room. It is directly connected.

Now I wish to address Shawn Hernan. Of course I agree absolutely that there are some uses and it's conceivable I could want to allow you, sir, to run a shrouded Trojan operating system on my machine. It's conceivable. Let's be realistic. The same arguments would show that the first ten amendments of the United States Constitution are useless. This power should not be granted. It will be effectively granted to a small group of monopolists, convicted monopolists in one case, oligopolists and cartels who have displayed the most brutal contempt for the rule of law and to think that now they will evince the most delicate concern for free markets when by changing one bit of the mask they would none but keys assigned by Microsoft to be placed in the TCPA is a fantasy so fantastic that I do not believe that anyone, Mr.
Hernan, if he would consider the history would actually defend this. Thanks. That's all I'm going to say.

MS. DOUGLASS: Thank you very much. I have one question of Keith. Just for clarification, your second threshold condition was that the would-be circumventor would have to notify the copyright owner. But if the copyright owner is no place around or if the copyright owner has gone out of business, I would presume that would not be necessary. All he would have to do seek to contact the copyright owner. Is that what you are saying?

MR. KUPFERSCHMID: Yes, he would have to seek and provide evidence of the fact that he tried to contact the copyright owner and the copyright owner is no longer in business.

MS. DOUGLASS: Thanks.

CHAIRPERSON PETERS: Do any of you have any questions that you would like to raise for the record of any of the members of the panel to answer?

MR. HERNAN: This morning we saw a wonderful example of one of the dilemmas that faces CERT on a regular basis. Mr. Carson asked a number of questions regarding the actual behavior of the region encoding scheme on DVDs and got two equally credible
answers but obviously conflicting answer though. If Mr. Carson were not an attorney for the Copyright Office but were rather an attorney for a large corporation, how could he engage a private corporation to settle that question without that private corporation risking prosecution under DMCA for circumventing the very work about which he is curious?

CHAIRPERSON PETERS: And who do you want to answer that?

MR. HERNAN: Anyone.

CHAIRPERSON PETERS: Not us.

MR. CARSON: I think you need to bring back someone from the last panel to answer this.


MR. BAND: I just have one quick comment. Mr. Simon before was suggesting that I was asking for progress to stop and that it would be the solution to this problem. But of course I'm not asking for progress to stop. No one here is. I think we're just recognizing that it's a fact of life that progress is occurring. On the whole, it's a good thing. But the point is that the progress that is occurring has certain side effects and what we need to do here is try to minimize some of those harmful side effects. That's the point of the exemption we're seeking.
CHAIRPERSON PETERS: Okay. If nobody else has any questions, then the hearing is closed. Thank you. Off the record.

(Whereupon, the above-entitled matter was concluded at 4:32 p.m.)