UNITED STATES OF AMERICA

LIBRARY OF CONGRESS

COPYRIGHT OFFICE

RULEMAKING HEARING

FRIDAY,
APRIL 11, 2003

The hearing was held at 9:30 a.m. in the Mumford Room (LM-649) of the Library of Congress' James Madison Building, 101 Independence Avenue, SE, Washington, DC, Marybeth Peters, Register of Copyrights, presiding.

PRESENT:

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

WITNESSES:

JONATHAN BAND
DAVID BURT
STEVE ENGLUND
SETH FINKELSTEIN
SETH GREENSTEIN
THOMAS LEAVENS
PANEL I - Compilations of lists of websites blocked by censorware ("filtering software") applications

Seth Finkelstein, supporting the exemption . . . 6

Jonathan Band, American Association of Law . . . 15

David Burt, N2H2, Inc., opposing the exemption . 18

Question-and-Answer Period ................. 25

PANEL II - Copy-protected Red Book Audio Format compact discs

Seth Greenstein, Digital Media Association . . 108

Thomas Leavens, Full Audio Corporation . . . 124

Steve Englund, Recording Industry Association . 134

of America

Question-and-Answer Period ................. 142
MS. PETERS: Good morning. I'm Marybeth Peters, the Register of Copyrights. I would like to welcome everyone to the first of our four days of hearings in Washington in the second anticircumvention rulemaking.

The agenda for the next three hearings, which will take place at the Postal Commission in early May are May 1st, May 2nd, May 9th. Then there's two days in Los Angeles. That's being finalized, and all of the information will be on our website next week.

Before going further, I would like to introduce the people from the Copyright Office who are here with me. To my immediate left is David Carson, the General Counsel of the Copyright Office. To my immediate right is Rob Kasunic. We call him "Mr. 1201." He's kind of been our ongoing person from the beginning. So he's probably the one who has been contacting the various witnesses.

To David's left is Steve Tepp, who is a Policy Planning Advisor in the Office of Policy and International Affairs. To Rob's right is Charlotte Douglass, who is a Principal Legal Advisor to the
General Counsel.

This hearing is part of the ongoing rulemaking process that, as most of you know, was mandated by Congress under Section 1201 of the Digital Millennium Copyright Act. Section 1201 provides that the Librarian of Congress, not the Register, thank you, may exempt certain classes of works from the prohibition against circumvention of technological measures that control access to copyrighted works.

The purpose of the rulemaking proceeding is to determine whether or not there are any particular classes of works as to which uses are, or are likely to be, adversely affected in their ability to make non-infringing uses if they are prohibited from circumventing the technological access control measures.

Pursuit to the Copyright Office's Notice of Inquiry which was published in The Federal Register on February 15th of 2002, we received 51 initial comments proposing exemptions to the prohibition, 138 reply comments. All of these are available for viewing and downloading on our website.

We intend to post the transcripts of all hearings approximately one week after each hearing. These transcripts will be posted on the websites as
originally transcribed, but, of course, the Office will give persons testifying an opportunity to correct any errors in these transcripts.

The comments, the reply comments, the hearing testimony will form the basis of the 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 by October 28th, hopefully, this time a little bit earlier than October 27th, on whether or not exemptions to the prohibition should be instituted during the following three-year period, from October 2003 to October 27th, 2006.

The format of each hearing will be divided into three parts. First, each of the witnesses will present their testimony. This is your chance to tell us why we should believe you, and especially I'll look at you, Mr. Finkelstein, because you're the one who is the proponent of the exemption on this particular exemption.

The statements of the witnesses will be followed by questions from us, the Panel. I hope that we ask tough questions that you will have to think about, and all the questions are going to be the same
for everybody. We hope that everybody gets tough questions.

This is an ongoing proceedings. I want you know that no decisions have been made about anything. I put in my notes "about critical issues." I can tell you it's not only the critical ones, it's no issues.

The purpose of the hearings is to further refine the issues and evidence presented by both sides in an effort to fully obtain the relevant information. The Copyright Office does reserve the right to ask questions of any of the participants after the close of the hearings. Any such questions asked and answers received will be posted on our website.

After the Panel has asked its questions, we intend to give the witnesses an opportunity to ask questions of each other. We have not managed to come up with all of the questions that should be asked. I'm confident that your fellow panelists will make sure that all the questions get asked.

With that, I am going to turn the program over to you.

OPENING STATEMENT BY SETH FINKELSTEIN

MR. FINKELSTEIN: I would like to thank the Committee for inviting me here. I would also like
to beg your indulgence if I make any procedural or 
cultural errors. I am not a lawyer. I am not a 
public relations -- sorry, shall I start over again?

Okay, as I say, I would again like to beg 
the Committee's indulgence if I make any procedural or 
cultural errors because I am not a lawyer; I am not a 
public relations person. I did have a better shirt, 
but I am literally straight off the plane this morning 
to come here.

This is not my job. I am a professional 
programmer by trade. I have no training or experience 
in Washington politics. If I make any mistakes in how 
I present myself or how I answer, I ask you to indulge 
me in that.

I am here, basically, to try to explain 
why this is important, and I will try to do my best in 
educating the Committee as to why censorware is an 
important topic and why you should grant the 
exemption.

Let me begin by trying to put some things 
in context. Censorware is usually discussed in terms 
of parents and children, but that is, in fact, not the 
way I got into this and not the way that I think about 
it.

I am a 38-year-old professional programmer
with an interest in civil liberties. I am not a professional activist nor am I a professional lobbyist. I got into this because I was one of the very early users of the Internet. I was at MIT. I am an MIT graduate, degrees in physics and mathematics. I really do have two degrees from MIT, and got to use the Internet in its very early, very formative stage, and I loved it.

I loved the information exchange. I loved the ability to talk to people literally across the world. You could talk to someone in Russia. You could talk to someone in Iraq. It was a fascinating exchange of ideas.

For a decade, from around 1985 to 1995, there was wonderful, free-flowing exchange where there were no constraints on what you could say or what you could read whatsoever, and it was fascinating for an intellectual.

Then, in the mid-nineties or so, it began to become "popular," and this was a problem. In the early days, it is very hard to convey the spirit of those times, where there's the idea that you could not censor the Internet, that it was created to survive a nuclear war.

There's a very famous saying by John
Gilmore, one of the founders of the Electronic Frontier Foundation. He said, "The Net considers censorship as damage and routes around it."

When I heard that, I was never convinced by it. I always wondered, well, what if censorship is in the router? Could you control the Internet by finding the choke points and cutting off that ability, that ability to exchange information?

Now when there became a reaction as to what to do about all the information being exchanged on the Internet, I loved this freedom of exchange and I wanted to preserve it. How can I convey what it was like in the early days, when now you take it for granted that you can cross the world, but this was thought to be a precious thing at the time, and I thought that it should be preserved.

Now I have to explain a bit about the politics of censorware. This will, in fact, refer to a bit of David Burt's comments.

When the Internet started to become popular, there was almost universal reaction to people who discovered it who were not part of the original cognoscenti. The reaction went like this:

"Oh, my God, there's too much information there. We have to somehow control it." And I was
wondering about this because we were told that the
Internet could not be censored, but yet there were
people who were saying it was important to control
what was on the Internet. How could both be true?
One of these people had to be wrong.

So when we had this problem at the time to
figure out what to do with the desire to control the
Internet, then there was the issue of, could we,
basically, put the U.S. interests in a private
program, a company such as N2H2, and would that be a
good thing?

This is a complicated issue to try to
explain, but what happened was the idea was that civil
libertarians should advocate private companies because
that would avoid the means of Congress having to
censor the Internet. I thought this was a horrible
idea.

The reason I thought it was a horrible
idea was because it was turning over the Internet to
private blacklisters. I thought this was an
absolutely disastrous idea from the civil libertarian
point of view.

So this is where I come into the picture.
As a technically-skilled person with the ability to do
mathematics and decryption programming, I set out to
figure out what was actually in the secret blacklists, and this is where I succeeded.

In 1995, I first decrypted CyberPatrol, and it was fascinating. I found, for example, the feminist discussion newsgroup at the time thought that feminism was considered pornography, technically sexual acts, for example. I found that gay rights and youth support were considered pornography, sexual acts.

And this pattern was repeated all throughout every program I examined. Feminism was considered pornography or sexual. Gay rights was considered pornography or sexual, on and on and on.

This led to the expose', "The Keys to the Kingdom." Now that has been criticized as being anecdotal. "Anecdotal" is usually used as a synonym for unverified or inaccurate, but, no, it was absolutely accurate.

What it was, it was not a statistical study. It was to counter the propaganda that the Internet could be easily censored.

Now the reason that it was published in that sort of -- how can I put it? -- sensational fashion was, one, well, because of the way the writer did it, and, two, this decryption that I was doing was
extremely legally risky at the time. In fact, there were lawsuits threats from the publication of that article. There's a whole story involved with that, and that was not the end of it.

Every time there was a game of this sort, I called it "the not on the list" game, that you would expose something as being blacklisted as sexual or pornography, or some feminist site, or some youth rights sites, and the censorware companies would then say, "It's not on the list," by which they meant they had immediately taken it off and the new version of their program was perfect. This went on and on and on.

There would be fantastic marketing claims. This moves into the Loudoun County case, where the proponent, the president of the company which made the censorware there, X-Stop, went out and actually said on record that the program only blocked sites which met a legal criteria.

This is an absolutely absurd thing to say because these legal criteria, as you may know, are very hard to do. They require judicial training. There is much argument, and the president of the company was saying that the program could do it. Humans can't even agree on what's artistic merit. How
could a program do it?

So I went and did a great deal of work exposing what this program had blocked. But, again, this wasn't my job. I've never gotten any money for this. It's stressful and legally risky. When the censorware companies get their blacklists exposed, they don't just laugh at you; they do everything from make threatening noises to, in some cases, actually filing lawsuits.

When the DMCA came, I said, this is it; this is too much. It's too much legal risk. I just stopped doing this work.

Then came the exemption and some other things, and I started doing it again. In this case, I changed some of my approaches. The idea of just finding specific examples is not so much an issue now because it's embedded into people's understanding. Even the censorware companies now say that their programs aren't perfect. They actually didn't say that before, because they are moving their marketing claims in response to the exposures of people like me, and that's very gratifying.

In fact, one of the comments in Mr. Burt's reply comment about listing the loophole sites, I believe that is in direct response to my report about
it. In fact, I'm sorry I didn't submit the actual report, but there's a comment where I track when they actually started making the claims and said, "I'm glad they're reading it."

So what I have been trying to do now is to try to explain some more properties of the programs which aren't obvious. It is very easy to say these programs block pornography. That's a phrase that easily falls off the top, but there are implications in that statement which are very important.

For example, image search engines are blocked in N2H2's program as pornography. Why? Obviously, because you can use them to search any images, and some of those images might be sexual.

Now if you ask somebody, "Would you like to block pornography," of course, they are going to answer, "Yes," except for a very few people. But if you ask them, "Well, do you want to prevent people in public libraries from searching for images because some of the images might be pornographic," you get a different answer.

I'm trying to explore those aspects of these programs now, and that requires circumvention in order to be able to do it very effectively. I think I will leave my opening statement there.
MS. PETERS: Okay. Thank you very much.

Mr. Band?

OPENING STATEMENT BY JONATHAN BAND

MR. BAND: Thank you for the opportunity to testify today on behalf of the five library associations.

The reasons given by the Copyright Office in 2000 for a 1201 exemption with respect to filters applies with equal force today. As N2H2 notes in its comments, filters are becoming more prevalent and, indeed, they may become even more prevalent if the Supreme Court reverses the lower court in the CIPA case. Thus, the need to know exactly which websites are filtered and which are not is becoming more compelling.

I would like to spend the balance of my time focusing on and responding to the comments filed by N2H2 and the other filter companies. The issue today is not whether filters are a good thing. It is whether the members of the public should have the ability to find out which websites are blocked by Internet filters. We think they should be able to find this out, particularly so that institutions and individuals can decide whether to use a filter and which filter to use.
First, as N2H2's comments emphasize, the use of filters has increased dramatically since the Copyright Office and then the Librarian of Congress granted an exemption in 2000. Thus, the existing exemptions have no adverse impact that we can tell on the filtering companies.

Second, N2H2's comments seem to assume that a 1201 exemption is the equivalent of authorizing the publication of the database of the prohibited websites, but this is absolutely not the case. Copyright still protects the database. Circumvention would simply put someone in the position to make a fair use of the database. But his use would still have to qualify under Section 107. A 1201 exemption will not change that in any way.

Third, from the erroneous assumption that a 1201 exemption would authorize publication of the database, N2H2 suggests that publication of these databases would provide children with unprotected computers a road map to pornographic materials. With all due respect, I think N2H2 grossly underestimates the resourcefulness of teenage boys. If they have access to an unprotected computer, they don't need a road map.

Fourth, the reference to the Microsystems
case is completely besides the point. That case
involved the development of a bypass code that
disabled the filter. It had nothing to do with
accessing the database for fair use purposes.

Finally, the N2H2 comments discussed the
alternative of making queries. I'm not qualified to
speak to the effectiveness of the sampling made
possible by such queries, and I am sure Mr.
Finkelstein is far more qualified to comment on that,
but it is clear to me, as a matter of common sense,
that sampling can never give you the complete set of
the blocked websites. By definition, you only get a
sample, so you obviously will miss what could be
important information. You will never know what you
don't know.

Also, the filter companies can reconfigure
their software to prevent automated querying, so this
option may disappear in the future.

In sum, the Copyright Office and the
Librarian of Congress got it right the first time:
The filter companies haven't presented any evidence of
the harm this exemption has caused them. It continues
to enable an important form of fair use. Accordingly,
the Copyright Office and the Librarian of Congress
should renew the exemption relating to Internet
filters.

Thank you very much.

MS. PETERS: Thank you.

Mr. Burt?

OPENING STATEMENT BY DAVID BURT

MR. BURT: Thank you. My name is David Burt, and I am from N2H2, Incorporated, an Internet filtering software company. I am here also representing two other Internet filtering companies, that being 8e6 Technologies and Bsafe Online.

To give you a little bit about my background, I am a former librarian. I have been involved in the study and promotion of filtering software for about six years, since 1997.

I provided testimony in, as well as being a consultant in, the Loudoun County case. I testified before the COPA Commission about filtering effectiveness. I testified before the National Commission on Library and Information Science on filters, and I also testified before the Pennsylvania and California State Legislatures. I have been with N2H2 for three years. My current role there is as PR Manager.

We are pleased to be able to come here and offer comments. As I made clear in my written
comments, filtering companies were not aware of procedure last time, so we did not submit comments at that time, and we are certainly pleased to be able to offer a response to some of the claims that are made about filtering software.

What I think is most germane here about evaluating filtering software is the fact that there is this very rich, very extensive literature that has been published of filtering software evaluations that does not involve the decryption of, and the disabling of, copyright control mechanisms.

Most recently, there was a study published in the Journal of the American Medical Association that was conducted by the Kaiser Family Foundation that used a very extensive sampling and testing, and it was conducted by a panel of experts and included a professor of information science at the University of Michigan, and was, in fact, peer-reviewed.

I think that studies like that really speak to the points, some that Mr. Finkelstein raised, about concerns about what viewpoint might possibly be affected or what uneven standards might be used. The Kaiser study is an example of a study that seeks to answer a question like that.

That seeks to answer the question, do
filters affect the ability of minors to access health information? Does it very effectively, using a querying method, create a sample using a querying method? So to the point that there are concerns like that, these can be addressed with sampling.

To the other concerns that Mr. Finkelstein raised about obvious architectural features, the single example -- in fact, the only example -- Mr. Finkelstein gives during the comment period from October 28th, 2000 to the present has to do with our product, N2H2, with the loophole category in our product. By his own submission, he admits that that information was publicly available.

It was publicly available on our own website at the time that he did that. So there really was no need for him to do that because that information was not just publicly available through our URL checker. It was also publicly available in our support pages, and it was also publicly available in the logs that anyone who is a N2H2 customer could check.

Speaking to some of the points that Mr. Band raised, he talks about the need to know. Filtering companies have been extremely responsive to people who say, "I want to know what's in your
filter." I give some screenshots and some
descriptions in my written testimony about our URL
checker database. That is a web interface, and many
of the other filtering companies have them, too.
SurfControl has one. Websense has one. Smart Filter
has one.

Anybody anywhere in the world can go to
our website at database.n2h2.com, look up any site,
see if it's categorized, how it's categorized, and if
they don't like the way that it is categorized, they
can submit a request to have that changed.

So I think we have been very upfront about
making our database available to people for
researchers, quite a bit more upfront than a lot of
other database publishers. Many other database
publishers, in fact, do not provide any kind of a free
query interface to test the database, but we do. So
I think we really even go further than the typical
database publisher does in doing that.

As to the other comment that Mr. Band made
about protecting children, I just can't agree with a
comment that, gee, because there's so much porn on the
Internet, what's the harm of making 300,000 porn sites
available to children? That's not the business we
want to be in. We don't want to be known as the
world's biggest provider of pornography to children.

That's not why this company was founded in 1995 by two educators, and we initially started in schools in order to protect children. We didn't build this brand that we have called Bess that's well known -- we provide filtering to 40 percent of the public schools in the United States -- in order to be known as the biggest provider to children of pornography.

I don't have really much to add to my written comments. I think I have explained it pretty thoroughly, and I really haven't heard anything in either the written replies or today that refutes what I have in here.

As to the CyberPatrol comment, in that case I think the judge was quite clear about the potential harms. In his Finding of Facts it says -- and this is on page 38 of my testimony; I'm quoting from the judge's decisions: "By their own admission, Mr. Jansson and Skala created this bypass code to break CyberPatrol software, explicitly designed to make CyberPatrol ineffective, and its intended use can do nothing more than adversely affect the potential market for the copyrighted work. In contrast, Microsystems as well as the public, will continue to suffer irreparable harm unless the individual..."
defendants are prohibited from distributing the bypass code."

I think some of that sentiment is really echoed in a case that I submitted -- the decision to just came down this week, versus N2H2. That involves a DMCA case about wanting to access our database.

I'll point you to page 3 of the judge's decision where the judge says, quote, "There is no plausible protected constitutional interest that Edelman can assert that outweighs N2H2's right to protect its copyrighted property from an invasive and destructive trespass," unquote.

So here we have had two judges look at this issue about whether or not it should be permissible to decrypt filtering software, and both have really come to very similar conclusions about the potential harm that would be done by doing that, and really a lack, frankly, of any benefits to society.

As I point out in my comments, there are really enormous social benefits that are derived from filtering software. That, in fact, Mr. Band spoke to the popularity of filtering software. That is what is driving the popularity of filtering software, is the fact that it does have such great social benefits to people, to parents who want to protect children, to
teachers who want to protect students at schools, to
corporations that want to protect from liability from
sexual harassment claims, that want to preserve their
bandwidth, that want to enhance employee productivity.
There are all kinds of social benefits to filtering
software.

In fact, that's what Congress really said
in 1996, when they passed the Telecommunications
Reform Act of 1996. In fact, it's quite clear that
Congress was trying to encourage the development of
filtering software when they passed that law, when
they passed the Good Samaritan exemption for that.

In fact, I'm quoting from the text of the
1996 Telecommunications Act. It says, "It is the
policy of the United States to remove disincentives
for the development and utilization of blocking and
filtering technologies and empower parents to restrict
their children's access to objectionable or
inappropriate material," unquote. That's what
Congress had to say about that.

As I go into my testimony, one testing
facility after another -- we have JAMA; we have PC
World; we have Consumer Reports did a test on filters
-- they didn't need to decrypt the filtering software
in order to analyze filtering products, come to
conclusions about their effectiveness. There really is no need to do that.

The record is very clear on that, that there is this rich literature that has been published of tests that have been done on filtering software to answer the kinds of questions that Mr. Band and Mr. Finkelstein have that can be done without an exemption.

Thank you.

QUESTION-AND-ANSWER PERIOD

MS. PETERS: Let's start the questions with the General Counsel. David?

MR. CARSON: Thank you.

Mr. Burt, can you just perhaps put in a nutshell for us -- let me start by saying, you did just state that your company and companies like yours do have mechanisms whereby members of the public can find out what sites are blocked by the filtering software. Can you tell us, just in a nutshell, what is the harm in letting researchers such as Mr. Finkelstein decrypt those lists, so they can get access to the entire list?

MR. BURT: The biggest harm, No. 1, is intellectual property, because, as I go into my written comments, we spent literally tens of millions
of dollars developing our database. It is extremely labor-intensive to do that.

There are editorial judgments that are made about different sites, how to categorize them. We have 4 million entries in our database, and we had to build the infrastructure and train the staff, the people, in order to populate that database. So we don't want to just give that away to somebody.

If we were to publish our database, make it publicly available, a start-up company or a competitor could just take our database and then start using it without having to pay the start-up cost. That would put us at a huge competitive disadvantage. That is one reason.

The other reason, as I mentioned before, is to protect children. We just simply do not want to make this gigantic list of pornography available to children.

And I gave an example of what happened when a company did that in my testimony. A company called Net Nanny gave away a children's CD-ROM at Burger King in the United Kingdom that had -- they published their list, and it had 2,000 pornography sites on it. The parents in the UK were so angered about this that they forced Burger King to recall this
CD-ROM. That's a really concrete example of what happens when databases like this are published.

MR. CARSON: Okay. Now we have had this exemption in place since October of 2000. Are you aware of any instances since then when someone, taking advantage of this exemption, has, in fact, either intentionally or inadvertently, publicized an entire list, or a substantial portion of a list, of the sites that are blocked by your software or any similar software?

MR. BURT: I'm not aware of anyone taking advantage of this exemption, period, to do anything during the comment period. Mr. Finkelstein says he does, but he doesn't document how he did that. He doesn't provide any kind of documentation about decryption or any publication. The only proof he cites of that, information that was publicly available at times, by his own admission. So I am not aware of anybody, period, using this exemption in the last three years.

MR. CARSON: So it's probably fair to say, then, that you're not aware of any problems that have arisen in the last three years by virtue of the exemption?

MR. BURT: There are certainly some
serious potential problems that could arise, but I think the problems have not arisen because nobody has decrypted any filtering software that I'm aware of in the last three years.

MR. CARSON: Okay. Now you mentioned that the main part of the harm is the intellectual property, and intellectual property is a pretty broad term. Let's just explore that.

You're not a lawyer, I gather?

MR. BURT: No, I'm not.

MR. CARSON: So maybe this is not a fair question. But when you are concerned about the harm to your intellectual property, it sounds like you're talking about something like trade secrets, proprietary information, and so on. Am I on the right line there?

MR. BURT: Well, we are talking about, No. 1, trade secrets, how we construct our -- there are techniques that we use to construct our database that are proprietary, but just the information itself, we want to protect that information itself.

The categorization that we apply to the URLs on the Internet, when we create the database, there is original effort that goes into creating that database. That's what we really want to protect.
That's what gives the database its value, is that value that we add to it by those editorial judgments that we make.

MR. CARSON: Okay. Now I don't want to sound callous about trade secrets or proprietary rights of that nature; I'm not. But this is a rulemaking about copyright. It's a rulemaking about Section 1201, which is designed to address measures that copyright owners take to protect their copyrighted works.

Typically, copyright isn't concerned with secrecy of information. So I am trying to understand -- and maybe you can help me; maybe you can't -- as to why we should care about that in the context of this particular rulemaking, which is looking at exemptions to a provision of law that is designed to protect copyrighted works and access to copyrighted works.

MR. BURT: Well, our work has copyright protection to it. Databases do have copyright protection, and they can be copyrighted. We want to protect that investment that we have of our database. We want to protect that intellectual property, that editorial judgments that we make in this database that we have created.

I think you should care about that
because, once you open the door for that, for some databases, there are a lot of other databases that could be vulnerable, too. Once you start going down that road of creating exemptions for databases like that, I think the other database publishers certainly would and should be concerned about that.

Because, as this body found in its ruling in 2000, it's essential that database publishers have copyright protections to protect their investment, to protect their intellectual property. Otherwise, it's going to greatly harm the database industry. There will be much less databases available.

And the same thing applies equally, and I think probably more so, to filtering software. These valuable tools that parents need, that schools need, I think the availability of them will be drastically reduced if we cannot control our copyrighted databases, if we cannot control our intellectual property.

MR. CARSON: All right. Mr. Finkelstein, Mr. Burt just said that he's not aware of anyone, including you, who has taken advantage of this exemption in the last three years. Let's start with you. Have you? And if you have, tell us how.

MR. FINKELSTEIN: Oh, I have a wonderful
reply to his comment there. Mr. Burt, you say that I have not published information on my decryption? Well --

MR. CARSON: Mr. Finkelstein, I'm sorry, but we do need the microphone in front of you, so the court reporter can hear. I think you had better start over.

MR. FINKELSTEIN: I'm sorry. This is just such a wonderful reply.

You say, you criticized me for not publishing details of decryption? Well, the last people who published details of their decryption for the world to see got a $75,000 lawsuit for their trouble, and that $75,000 lawsuit took place right downtown from me. So there were no fancy Internet jurisdiction issues even, when you consider that case.

Therefore, could you consider perhaps why I might be a little hesitant to publish details, given that the last people who did it got a lawsuit for it? In fact, the only reason I came out and said that I had decrypted the database was in order to try to preserve this exemption.

I keep trying to convey, this isn't my job. Nobody is paying me to come here. I took the money out of my own pocket to actually pay the plane
fare back here.

David Burt is paid by the company to do this. Win or lose, he goes home after this and he gets paid and he gets a salary. If I am looking at a massive lawsuit, $75,000 -- I looked at the amount -- for publishing something versus keeping my mouth shut about how I acquired it, I think the incentive there is to keep my mouth shut about it.

MR. CARSON: Well, short of what you're willing to say or what you're willing to publish, give us a sense, first of all, in the last three years have you, in fact, engaged --

MR. FINKELSTEIN: Oh, yes.

MR. CARSON: -- in the conduct covered by this exemption?

MR. FINKELSTEIN: Yes, I have.

MR. CARSON: Okay. Can you describe for us what you have done?

MR. FINKELSTEIN: Okay.

MR. CARSON: This is your chance to tell us why it's important to let people like you continue to do that for the next three years.

MR. FINKELSTEIN: There are two different senses of the words "what you've done." I can describe to you the way I decrypted the database, but
perhaps I shouldn't, or I can describe what I've done
with the decrypted database, which is important. I
assume you're asking that second question: Why is it
important that I decrypt -- or am I mistaken?

MR. CARSON: Well, I would like to have
them both.

MR. FINKELSTEIN: This is where I asked
you earlier about immunity.

(Laughter.)

MR. CARSON: Well, whatever you feel
comfortable telling us, again, understanding that we
need to be persuaded that there is a reason for this
exemption to be granted for the next three years.

MR. BAND: Focus on the second question.

MR. CARSON: It would assist us in
determining that --

MS. PETERS: That's your lawyer.

(Laughter.)

MR. FINKELSTEIN: I know this isn't
literally true, but I would like to plead the Fifth
Amendment for grounds of incrimination on answering
the first question on how I did it. I could certainly
prove it to you by bringing you a CD of their
database, if you can use that.

MR. CARSON: All right. So you are
concerned that conduct you have done under an exemption of the law might lead to some kind of criminal liability?

   MR. FINDELSTEIN: Ah, no, you see, this is unique. I've got an answer for you there. The exemption that you have given me is an exemption for the DMCA, but it is not an exemption for copyright, trade secret, or violation of the shrink-wrap licensing.

   In fact, I am going to go on. The CyberPatrol case was not a DMCA case. The actions in the CyberPatrol case were traditional copyright, trade secrets, violation of shrink-wrap licenses, and a couple of other things which I called the "kitchen sink" charges. Every single one of those charges could be brought against me, even with this exemption.

   MR. CARSON: So you're telling us this exemption is pretty worthless?

   MR. FINDELSTEIN: No, it's not worthless. It's important in the sense that it goes to doing the act. If I said here, "I have done the circumvention," without this exemption, that would be a crime. That would be admitting or that would be violation. That would be admitting to a violation.

   Because of that exemption, I can tell you
that I have done it, but if you ask me to give you
cold-level details where I start getting into the area
which got two people sued for copyright, trade
secrets, and violation of license, I think that's
increasing liability. It is a hierarchy of liability.

Why this exemption is important is this
exemption goes to the actual action of doing the
investigation itself. It says, even if you publish
just one fair use result, if you admit in that paper
that you did the investigation by circumvention, you
have liability because you have confessed to
circumvention, and fair use is not a defense to
circumvention. It is very clear in the Remandes case.
That's why the exemption is important.

In fact, this also answers David Burt's
question in a way he doesn't like. The exemption does
not remove all the protections that the censorware
companies have already. We're not talking about
putting this on a CD in Burger King and distributing
it to little children. I've not done that. Nobody
has done that.

MR. CARSON: All right, so what good has
the exemption done?

MR. FINKELSTEIN: Now what the exemption
has done has allowed me to do these architectural
investigations. Let me try to explain these.

In fact, if I can take a couple of minutes, let me, in the course of explaining this, rebut Mr. Burt on the utility, or lack of, of querying. It's not an issue of quantity; it's an issue of quality.

All these studies that he cites are in some sense the same study repeated over and over again. It's take a couple of sites, see what's blocked, see what isn't blocked, and so forth. That's not the question I'm asking. It's like saying that you don't need to have college because you have so many high school essays. It is a bit like that.

Where circumvention is important is what I call looking for the land mines here. It's like trying to locate land mines in a mine field. In theory, one can examine every bit of territory, but it's qualitatively different to have a map of where the mines are.

Now Mr. Burt's product, N2H2, bears a semi-secret category called "loophole." Loophole category is a category which cannot be deactivated where things are blocked by installation as mine fields, little mines, but you suddenly find them blocked, and you have no idea why.
Trying to figure out what these loopholes are that will be blocked in libraries, that will be blocked in government sites where they are mandated to use censorware, is something which cannot effectively be done by sampling because it's not a statistical property. It's a property where the site is somehow thought to be a threat to the operation of the program.

Maybe I should back up for a moment, if you will indulge me, and try to explain where I'm approaching this from. I'm not approaching it from a statistical point of view. Statistical studies are well and good, but statistics are not the be-all-and-end-all of investigations. There are other types of investigations which can be done.

Now you'll note throughout the entire proceedings I have talked of censorware, not filtering software. That is not merely partisan politics. That is a very important difference in how I think about this issue.

When somebody talks of a filter, that conjures up the image of this ugly, yucky, horrible, toxic stuff that you're taking away and leaving a clean and purified result, like a coffee filter or a dirt filter. You just want to throw the ugly stuff
away.

But that's not what these products do. What these products do is they control what people are allowed to read, and that's a profoundly different issue. Because when you try to control what people are allowed to read, and you try to put them in a blinder box, you can't ever let them out.

For example, a loophole is a language translation site because a language translation site makes the information coming from the other site look like it's coming from the language translation site. So you can use the language translation site to get to the site that's been banned in a sort of routing fashion, that you route around the banned site through the language translation site.

You can use a site that checks to see if your web page has the appropriate structure to it. You know what HTML is, HTML formatting. There are programs which you can take and will say, well, your HTML formatting has this problem or it displays this way, but those are actually considered loopholes because they allow you to display a banned site, because you can say, oh, I want to check its formatting.

This is a very important part of the
debate, trying to get people to understand that what these programs are doing are not banning pornography or banning whatever. They are controlling what people are allowed to read. In order to do that, for example, what I did in my loophole paper was to go through affirmatively -- I was not querying, not sampling things, but trying to say, what are these things that Bess considers a loophole?

It was a fascinating revelation to find out that language translation sites are considered a loophole. Well, that's interesting when you think of that, but then you find out that HTML-checking sites are considered a loophole.

Then, this is the really interesting thing: The Google cache -- you know what the Google cache is? -- that's considered a loophole because you can get to any web page by using the cached version.

So when you tell people, well, you're not banning pornography, you're not letting people use the Google cache because they could use the Google cache to get something forbidden, that changes the debate. I have been trying to get this into the thinking process of people. I may not have been very success at it, but it's something I have been doing with this research.
MR. CARSON: Mr. Burt, anything to say in response to any of that?

MR. BURT: Yes, I do. I would just like to -- and I have already said this a couple of times, but I will say it again now that Mr. Finkelstein has had a chance to explain. When he was asked specifically to describe specific examples where he had used this exemption, the only example he came up with was for N2H2 to find this loophole category that, by his own admission, was already publicly available in other sources. I think that's not a sufficient record to justify this exemption, if that's the only example that can be come up with.

MR. FINKELESTEIN: May I respond to that? First of all, Mr. Burt is inaccurate to say that it was publicly available. He has made it publicly available, I believe in response to my paper. But the reason I am very certain that it was not publicly available -- and perhaps I can answer some of your earlier questions about how this is done -- is because I did not know what this loophole thing was when I saw it in the database.

Maybe I can give you some better examples by telling you what I saw. For example, when I decrypted the database, it's very hard to figure out
what these things are sometimes. Decryption is only one step. There's the encryption, and on top of the encryption, there's often a database structure. I don't know if I'm getting too technical, but there's often binary codes and special flags, and so forth, and it's very hard to figure out what these are sometimes.

In the N2H2 blacklist there's a whole list of things. As I tried to figure out -- first, there was a list, and then there was a list of flags which correspond to the codes, to the entries of the list. This isn't getting across.

There's a header of things that say that pornography, violence, and there's also other internal things that said things like, "loophole."

By the way, David, can you tell me what "anod" is? I'll catch up with you there.

My joke about this is I can't call up technical support and ask them to tell me what it means. So when I saw this entry "loophole," I'm thinking, what is this thing? So I searched throughout the web and there was no documentation for it whatsoever. The only thing that was there was the log entry that was a two-letter code, "LH," from the site.
So what you saw, if you ran a loophole site through the program itself, was a set of two-letter codes that correspond to the categories, but there's no documentation for this secret category. And I searched very, very thoroughly to find any documentation for it, but it wasn't there.

When I put one of the sites which was listed into the query database that said it was a loophole and it came back and said, "loophole sites," it didn't tell me what a loophole was. It was only by -- and this is where statistical sampling is not important, is not answering the question -- by collecting all the other sites in the database which were loophole sites and asking, "What property do all these sites have; why are they like one another," that I realized that what they considered a loophole site was something that they deemed a threat to the control of the program.

The question was basically, I have this database in front of me. I have these strange-looking sites that say, "loophole." I have no documentation whatsoever for what is a loophole.

I go through the database and I extract all sites which have the flag "loophole" on them. They're privacy sites, language translation sites.
Oh, what's this? It's an HTML validation site. That's odd. And what's this other thing? It's a site that makes things sound like Elmer Fudd. Why do they have that thing there? Oh, it's a language translation site, but it's just a weird language. Oh, there's Google cache in here.

Now what property does the Google cache, a language translation site, an anonymizing side, an HTML validator site all have in common? Aha, they're all sites where they retrieve other sites and display them to you. Bingo. I think this is a very important fact to get out in the debate, and that's how I also did it.

MR. CARSON: Mr. Burt, I may have been misreading your body language, but I got an impression I saw an urge to respond. Is that true or not?

MR. BURT: Yes, I'll go ahead. It is in my written comments, but in Mr. Finkelstein's own report, "Bess's Secret LOOPHOLE," he just referenced the website at database.n2h2.com. He says, quote, "The loophole category can be verified by using N2H2's single site blacklist checking form. Just test it into database.n2h2.com."

So, I mean, right there he says that this information is publicly available on our website.
MR. CARSON: Well, I think the question is, which came first, your revelation or his detection? I don't think that's something we're going to resolve here.

MR. FINKELSTEIN: No, no, what I'm saying is the query says it's a loophole site, but there's no documentation for what loophole is.

MR. BAND: Right, and his point is that, yes, now that you know, now that he's told you to look, that the Google cache won't be available, you can go to their website and, sure enough, you'll find, you type in "google cache," and you won't get it.

But the only way that he was able to figure that out was by the circumvention--finding this category, trying to figure out what it meant, figuring out what the common property is, figuring out why it was doing this. And now you can verify that on your own through their site. But for his encryption or his decryption work, we wouldn't know that. That's his point.

MR. CARSON: I think we've got disagreement on whether that's true or not, but we at least understand the proposition.

MR. FINKELSTEIN: Verification is not the same as investigation.

MS. DOUGLASS: There's also in our tech support pages, there's references to the whole category --

MR. CARSON: Okay. I want to get back to what I was asking before, and I understand you have expressed your reluctance to give us much in terms of concrete terms about what you've done because of your fear that we are not dealing with just 1201 and copyright, but perhaps other things.

MR. FINKELSTEIN: David, will you pledge never to sue me if I tell for this?

MR. BURT: I'm not authorized to make a statement like that.

(Laughter.)

In order to make a statement like that, I would have to consult with management, and they would have to consult with our attorneys when we get back. As a PR person, I'm not empowered to do things like that.

MR. CARSON: Let me ask this, then, either Mr. Band or Mr. Finkelstein, any help you can give us in terms of letting us know not necessarily what you personally, but other folks who have taken advantage of this exemption, what they have done and why it is
to the advantage of society to let them do that. In terms of concrete terms of what people actually are doing and have done, that would be of great benefit to us in evaluating the need for this exemption. So if either of you can help us out in that respect, that would be useful.

MR. FINKELSTEIN: Well, I could talk about some of the things that have gotten people sued for. That's an easy one.

If you want me to talk about how decryption is done or how circumvention is done, it's a very --

MR. CARSON: No, not so much how circumvention is done, but help us understand why we should care. How have people used the ability they have had under this exemption to society's benefit? How have they taken advantage of this exemption --

MR. FINKELSTEIN: Great.

MR. CARSON: -- in a way that, if you could explain it to us, we would say, "Yes, of course, people have a right to do that and they should have a right to do that, and we understand. We get it."?

MR. FINKELSTEIN: First off, I can explain to you that the work that I did was cited in the expert witness reports for the CIPA decision. Mr.
Burt's comment is very interesting in the way he walks around that, in that he says that it's not cited in the actual description.

But if you look in my comments, you see the expert witness reports themselves cite my own work. They cite the specific paper that I'm talking about here. That's his secret loophole.

Some of the things which may not have specifically my name attached to them do seem to have come from me. I have talked about the Bess's loophole example because it is the strongest example or circumvention, but there are many other things that I have done which have been helpful towards explaining what the process is, what is actually banned, and what is actually a problem in these architectural terms that I haven't actually gone out and said, "I got this information by circumvention," again, because of the legal liability here.

To back up for a moment, when we talk about sampling, nobody is going to sample the Google cache. It simply wouldn't occur from the list of things that you would use to test a program, at least not until this had been publicized. Once it has been publicized, then, of course, it's become an issue. But if you're trying to do an investigation, that
isn't something that's obvious to you.

And one of the other things where I got
the information from circumvention was the
investigation of the image search engines. For
example, to figure out that image -- what I did was I
went through the program and started looking at the
database for what some of the other Google sites were.
It was vastly easier to do this by having the list in
front of me, asking the question: If it blocks the
Google cache, what other sites from Google would it
block?

That question is a very hard question to
answer accurately by sampling, because it's not a
question of just taking the list of sites and running
it through the verifier tool, because the way that the
entry can be done can be done in a way that you can
fool the verifier tool. You have to know the exact
path to put into the verifier tool.

In fact, I put that in my paper for
verifying the Google cache blocking. If you just type
in the Google cache itself, you get back the answer
that it's not blocked because the actual site isn't
blocked, but the way that you would do the lookup, the
actual string itself, is where they have the blacklist
entry.
So in order to do the image investigation, it was vastly easier to have the database in front of me and try to see which image sites had been blocked than fumbling around in this mine field and here are the mines. This, too, is cited in the expert witness reports and in the CIPA decision.

In the future, I expect that there's going to be more of an issue where what is blocked in these terms is going to be a factor in the Supreme Court. Whatever the Supreme Court decision is, there will probably be intense interest in investigating censorware.

Without this exemption, you're basically saying that people are constrained to do that exemption blindfolded. They cannot actually look at the database. They have to go through the mine field, poking and probing every single bit of territory.

MR. CARSON: I want to get back to that issue in a minute, particularly with you, Mr. Burt. But, first of all, can either of you, just so we've got as much of a record as we can, I want to make sure I've got from either of the two of you any examples you can give us of cases where people either have been taking advantage of the exemption or are in the process of taking advantage of that exemption. So
that we, again, can understand that we're not just
dealing with something theoretical here, but in
concrete terms this is something that has been of
benefit and will continue to be of benefit.

MR. BAND: Well, again, as Mr. Finkelstein
has explained, his loophole research is a very strong
example. My understanding is one of the witnesses in
the California hearing is also going to be
specifically addressing it.

I don't work directly in this area,
typically, but my understanding from conversations
with people in this area is that, as Mr. Finkelstein
explained, that the expert witnesses do rely on the
work that he did and that others like him have done
within the past three years. But I believe that in
the Los Angeles hearing you will be able to get more
concrete examples besides what Mr. Finkelstein has
specifically alluded to.

MR. FINKELSTEIN: Let me answer that also.
There's something of a Catch-22 in your request
because, in order to come here and plead for the
exemption, what I have to do is actually confess to
violating other laws. I have to come and say, "I have
violated the shrink-wrap license. I have possibly
violated classical copyrights. I may have violated
trade secrets." There aren't many people who actually
want to do that.

I mean, I think, for myself, that I am
sort of a fool for doing this. I'm not getting any
money for it. I'm not likely to benefit. Why am I
poking my head on this?

In fact, if I knew somebody who was doing
this, and they had trusted me that they would do this,
I certainly wouldn't be blabbing that in a public
hearing with Mr. Burt here ready to take anything back
to his company. This is literally a case where
anything I say can, and maybe will, be used against me
in court.

So, again, I am going to have to ask you
to be a little bit understanding that I can't give you
a list of other people who are doing it right now
because that would be, at best, violating trust and,
at worst, getting them sued.

MR. CARSON: Okay, I get your point.

Mr. Burt, going back to something Mr.
Finkelstein just mentioned, my reaction, when I read
your comment -- and your comment made a very strong
pitch that all sorts of studies had been done --

MR. BURT: Uh-hum.

MR. CARSON: -- of filtering software, and
almost all of those studies use what you call a query
approach, which, if I understand it correctly -- and
correct me if I'm wrong -- the person who is doing the
study has a list, and I don't know how big it is, of
sites they want to check to see whether those sites
are, in fact, filtered out and runs that test with a
number of different filtering software and then comes
up and reports their results. Is that basically how
it is?

MR. BURT: That's basically how it is, yes. There are a number of different ways to get a
sample. As the Kaiser study points out, they used a
random-sampling technique. Or other people have done
a purposeful sample because they want to answer a
particular question. They want to get a big list of,
you know, gay sites or sexual health sites and see
what the results are, but that's correct.

MR. CARSON: Okay. All right, now I'm a
layperson. Lord knows I know nothing about how to run
such a study, but it does strike me that when you're
doing that, when you're taking that approach, you're
necessarily limited by the list that you, the
researcher, come up with of sites that you want to
check on. It also strikes me as a layperson that
there is a lot to be said for, and a lot more that can
be gained perhaps, from a study in which you simply
say, "I want to see the list of sites that are blocked
because then I can go down that list and I can make a
determination in each case whether that is or isn't a
site that I believe should be blocked.

Now we can then have a nice debate over
whether of those individual sites, in fact, should or
shouldn't be blocked, but at least the only way I can
know everything you're blocking is by knowing
everything you're blocking. The only way I can know
what you're not blocking that perhaps should be
blocked is by getting that list and then figuring it
out.

Now what's wrong with that? What am I
missing?

MR. BURT: Well, again, there are
intellectual property concerns in exposing our
database to somebody to examine. I think you seem to
be kind of getting at a hypothetical question.

For example, where somebody such as the
National Research Committee or Consumer Reports could
come to us and say, "We want to take a sample of your
entire database. We'll do it in our laboratory. You
can be there. We'll sign NDAs. We'll ensure that
it's protected," somebody that was like a reputable
third party that wanted to do that, I can't say for sure that we would do that, but I know that we have had internal discussions about that, and we would very seriously consider doing something like that, if there were absolute guarantees that our intellectual property would be protected and it were a reputable kind of testing facility that was doing that.

We would not necessarily be opposed to something like that, but nobody has ever asked us that question, nobody, not even the people who do research that are opposed to filters, such as Mr. Finkelstein. None of these people have ever approached the filtering companies. At least -- I can't speak for all of them at all times that I'm aware of -- certainly not my company, asked to do this kind of an approach.

So, yes, that is something we would consider, if somebody absolutely felt they needed to do that, but we don't see that need being expressed by the research community. The people who did the JAMA study didn't express that need. The people who have done the other studies, such as the Consumer Reports study, that was rather critical of filters, did not express that need; neither do any of the other professional testing labs.
ZDNet Labs and InfoWorld test labs have not come to us and said, "We can't evaluate without being able to get at your entire database." They're perfectly satisfied with the results that they get and with the research that is published using a query method.

MR. CARSON: Does anyone else have a
reaction on that particular question?

MR. FINKELSTEIN: Oh, plenty.

(Laughter.)

David, do you have the e-mail where the representative for N2H2 said that I wouldn't get a demo because, as I quote, "working with you would be like working for the opposition."?

I like his comments about reputable, too, because you tend to find out that people who are the most critical and who know the most about the flaws are also regarded as the least reputable, at least in the company's regard.

Further, the last time I tried to get the demo from N2H2, straightforwardly get it filling out my name, I was outright refused. I was worse than outright refused. I was led on, and then I got a really obnoxious e-mail from their salesperson telling -- I'm just not going to quote it; it was so
obnoxious.

He didn't care. The company's going to back him up for doing it, and he probably gets a bonus for it or a pat on the back for it. Mr. Burt thought that was great.

David, will you give me a demo? I would love one.

MR. BURT: If I could respond to that, what Mr. Finkelstein is referring to is a request for a free trial of our database, or not our database, our software, which we do offer to anybody. We give people free trials, a 30-day trial of our software, as do most filtering companies.

However, Mr. Finkelstein had conducted at least three previous 30-day trials before that, and it is not our business practice, nor is it of most software companies, to give an endless series of free trials to somebody. At some point you have to cut them off, if they are not going to pay for the product. So that was simply a standard business decision. It had nothing to do with Mr. Finkelstein.

MR. BAND: If I may respond, I think Mr. Carson, you're exactly right about the fundamental problem with sampling, that obviously it tells you something, that it can be very useful at a macro
level, but at a specific micro level it doesn't work, meaning it doesn't tell you whether a specific site that you don't know to look at, you have no idea whether or not it's blocked.

With respect to the assertion that no one has ever asked, well, typically, when people want to do independent verification, they do it independently. I would just be shocked if, when Consumer Reports wants to do any kind of testing of General Motors' products, they enter into a negotiation and then agree to do the testing at a General Motors' facility, under the supervision of a General Motors' engineer. It is not going to happen. That would compromise the independence of the survey.

MR. BURT: That's typically how product tests are done. The Kaiser Foundation, they did ask for a copy of our software when they evaluated it and did tell us what they were doing.

The other point I would like to make is that this issue of testing databases that have copyright protection, you could make the same argument about other copyright-protected databases, about Lexus/Nexus or about Dialog or some of the other ones that don't allow people to go in and access -- you can't request from Lexus/Nexus and get every single
thing in the Lexus/Nexus database, complete, total, free, unlimited access to do that. Yet, there's a very rich testing literature of Nexus using querying methods to do that.

   MR. BAND: Right, but it's a completely different situation. I mean, the whole point of the testing of the filter software is basically to get a sense of what kinds of sites it blocks. It poses very specific and very significant public policy issues. What's on the Lexus/Nexus database, that's a commercial issue. If I don't like what's on Lexus/Nexus, if I don't like what access I get, I will go to someone else. It has no public policy implication whatsoever, what is or is not available through Lexus/Nexus.

   But if we're talking about government-mandated filters in public libraries and public schools, there is a huge public interest in knowing what is or is not censored. It is a completely different situation.

   MR. BURT: I don't agree. I think simply because the government mandates the use of a product, that doesn't mean that that company loses all its intellectual property rights, just because it is government mandated.
MR. BAND: But, again, you're not losing your intellectual property rights. If Mr. Finkelstein, after doing his research were to publish the database and make it publicly available, he would clearly be liable for copyright infringement because he is violating the copyright in the database.

But if he, instead, makes a fair use and simply publishes, let's say, that the N2H2 product blocks out these 10 sites, that would be a fair use and that does not in any way compromise your intellectual property rights.

You're mixing two different categories.

MR. BURT: Well, Mr. Finkelstein, as I pointed out before, does not need to get access to our entire database to publish his list of 10 sites. He can do that with sampling.

MR. BAND: Not if he doesn't know which 10 sites to ask for.

(Laughter.)

MR. FINKELSTEIN: This is again saying that you do not need to have a list of the land mines. You can go and prod every single bit of territory. I suppose that is true in theory, but in practice it is not supportive of the sort of investigations that I am trying to do.
I want to, again, point out that, given this work that I have been doing, this decryption, this circumvention, it is immensely difficult. It has legal liability. It requires a great deal of programming skill. It requires certain advanced server tools and software sometimes which are not available to -- which are theoretically available, but not usually found with journalists and writers.

So the fact that when they do a simple sampling study doesn't mean that better research is being done. It's like saying that, if somebody does a slapdash job by walking down the street, you shouldn't let them go to the Library of Congress because they can already do something by walking down the street.

MR. CARSON: One final question: The reply comments filed by American Film Marketing Association had a number of other copyright owners, the reply comments. It made one point on this subject, which is that -- well, it made a number of points, but one of the points they made was that, if this exemption were continued for the next three years, it should not include network security software.

Now I don't pretend to be an expert on
just what that means, but, first of all, I guess I was just wondering, is there anyone at this table who disagrees with that statement and, if so, can you explain to us why?

MR. FINKELSTEIN: I haven't reviewed it, so I can't say at the moment.

MR. BAND: No, I haven't studied that issue. So I have no position.

MR. CARSON: All right, thanks.

MS. PETERS: David was pretty exhaustive in his questioning, but let's see if Rob has any.

MR. KASUNIC: Well, I'm going to have to sort through and see what's left after that, but I have a number of things to try to clarify a little bit.

First of all, just, I guess, addressing Seth first, in using the term "censorware," as opposed to "filtering software," why use that term, and is there a distinction? In your view, is filtering something broader?

MR. FINKELSTEIN: Oh, yes. I think the best public relations that the censorware companies ever did was to get the word "filter" attached to their products. When you think of a spam filter, for example, you think of something that you do not want
to see.

But, again, as I said earlier, censorware is not like a spam filter. What censorware is is an authority wants to prevent a subject under their control from viewing material that the authority has forbidden to them. This description is general. It does not apply just to parents or children. That is simply one instance of the general property. It could be the Government of China applying to citizens or it could be corporations applying to employees.

We can go back and forth as to who is right in what cases, but the general architectural properties are the same. In fact, one of the issues here is that, if censorware works for parents on children, then it's also going to work for the Government of China on its citizens. And, inversely, of course, if it doesn't work for the Government of China on its citizens, then it's probably not going to work for parents on children. This is one of the deep structural issues of the debate.

But putting that aside, a spam filter, for example, is something that you do not want to see and someone else wants to force on you for their own benefit. This leads to a different way of thinking about it.
For example, you can take something that's probably spam and shunt it off into another folder that you look at later on to see if that program has made a mistake. So you're allowed to see the decisions of the program and you're allowed to look through what it's done in order to see if it's incorrect or not.

They don't think that you have to be forbidden from reading the spam. I have never seen a spam filter that actually made it impossible for you to shut it off because there is something dangerous that might happen to you if you actually saw one of these spams.

That's the difference between the issue of something you don't want to see, which is filtering, and something somebody else does not want you to see, which is censorware.

MR. KASUNIC: Okay, thanks.

MR. FINKELSTEIN: And this leads directly into the loophole sites that I have been talking about.

MR. KASUNIC: Well, in following up on that with the loophole site -- and, again, this is just sort of to clarify -- are you saying, then, would you have been able, Mr. Burt or David -- I have talked
to all of you so many times in setting up these hearings I'm going to be informal.

    MR. BAND: We're all old friends.

    (Laughter.)

    MR. KASUNIC: David had said that you could have discovered the loophole category, even without circumvention, but is what you're saying that it's the scope? You could have identified that this existed, but you could have never identified what the scope of that category was?

    MR. FINKELSTEIN: The extent of it would never have been found by sampling. How in the world was I going to sample HTML validation sites? It's not a statistical matter. You could say that you could sample land mines, but they're not statistical properties either.

    The idea, what I was trying to do was to go through and figure out what things does Bess consider to be threats. That's not a question of, in this huge list of sites, is there anything here that Bess considers a threat. That's a different question.

    How would I ever have found that a site for testing how HTML is formatted was considered a loophole by sampling? It would be almost impossible. The language translation sites would probably not have
been found by sampling even then, because of the specific way that the entry is listed, because it's not just the sites.

The way people usually do sampling is to get a list, a long list, of sites or a long list of URLs within the sites and just run it through the program. But the blacklist itself can have the entries on the blacklist in ways which are very hard to find out. Things like the Google cache, the actual entry is something like "?q=cache," for example, and that's just not going to be found in a sampling system.

MR. KASUNIC: What about systems or methods either than sampling, like, for instance, David had mentioned the log files? Would that get you any further?

MR. FINKELSTEIN: Well, the only reason he mentions log files is because log files have the two-letter code "LH" for "loophole," and when I was looking through the log files, I was trying to match up the little codes that they had for the actual categories in the database.

But the log files don't tell you anything more than the verifier tool does that they have there. It's just a big version of the verifier tool or a
local version of the verifier tool. It is a sampling
response which can be used for a sampling study, but
it still has all the flaws of sampling and all the
limitations of sampling.

MR. KASUNIC: Okay. Then, too, in terms
of the other side of this, of the harm involved here
-- and I'll put this more generally to the Panel --
but in your comments that you cite a report, N2H2
report, that states that, quote, "N2H2 does not
believe that the final rule will affect the value of
its lists of blocked websites," meaning the previous
exemption, the rule under the previous exemption.

So has there, to your knowledge, first of
all, been any harm to the industry in general because
of -- and focusing this on the exemption on the
prohibition for circumvention because I do want to get
to some of the other aspects that David has been
raising that maybe are broader than that of just the
prohibition on the act of circumvention?

MR. FINKELSTEIN: I have not seen any
evidence whatsoever that they have suffered in any
way. In fact, the only thing that I had seen is they
probably have to pay David Burt to go here. I mean,
that's the only money that they have been out.

MR. BAND: And, also, obviously, indeed,
the N2H2 comments reflect that the industry has grown significantly since the exemption was granted. So that would seem to refute any notion that the exemption has caused any harm whatsoever.

MR. KASUNIC: Well, David, I think that you deserve a chance to talk about that. It does note, we'll note on page 11 in the report that it has a bar graph, in your comment is a bar graph of the growth of the industry, and it looks like a steady growth even up through 2001, which would have been after the exemption went into effect.

MR. BURT: And the growth is continuing, too.

Again, I'll say that the only reason this exemption hasn't harmed filtering is because nobody has done any exemptions during the exemption period. The only circumvention that we've -- we have heard that question asked three or four different times, and the only example that has been presented is Mr. Finkelstein's example of the loophole category. So that's why we think no harm has been done to the industry during this three-year period because no one has taken advantage of it.

If you look before that three-year period, if you look at the experience of CyberPatrol, it is
quite clear, looking at the judge's decision, that there was harm done to CyberPatrol by the decryption that was done to them. So that's where we stand on that.

We look at the example of what happened at CyberPatrol, and we look at what happened to Net Nanny and the bad publicity that they got, as the examples of what sort of harms can be done. That's why we look at that.

MR. KASUNIC: Well, specifically, then, you do mention some of these other cases and the specific harm that has been done. But in looking at some of those, it wasn't clear to me that the harm had anything to do with the act of circumvention. So that's what I was talking about wanting to get to.

The cases that you cite and quote talk about publication and dissemination of the tools, which would still be protected by the anti-trafficking provision and there's other areas. But what specifically related to -- what harm has been, or is likely to occur, as a result of the limited exemption based on the act of circumvention?

MR. BURT: Well, I can speak for my company in particular, because we are so heavily used in public schools. If our software is shown to be
easily disabled, our database easily disabled, that really undercuts the trust that we have with schools in the United States, with teachers, to provide a safe, secure Internet experience for them.

And that was the problem that CyberPatrol had, too. That was their biggest concern, talking to the people there, at the time of the CP hack, the CyberPatrol decryption, was that all the millions of parents that trusted CyberPatrol to protect their children were suddenly rendered insecure, and the judge goes into some detail about that in his decision.

MR. KASUNIC: But we're talking about, you're saying, "if it's disabled." We're talking about circumvention for a list of websites within; we are not talking about disabling the entire program.

So if someone is able to circumvent to find the list, they may be able to find URLs to different sites, but how will that help someone who still has the software program functioning on the site? Even if you have the URLs, if all the school children in the world have URLs to all of these, as long as they have a protected computer, won't they still be prevented from viewing any of those sites?

MR. BURT: Well, as long as the software
is functioning correctly, that's correct, they would still be protected there. But what that would do to our market, you know, to our customers, the trust they have in us, if it's widely publicized that your software has been compromised, that it has been hacked into, that the security systems that protect that software that's used to protect millions of children can be easily compromised and disabled and hacked into, that damages our product severely. It damages our ability to sell our product.

MR. KASUNIC: But, again, isn't that apples and oranges? Aren't we talking about --

MR. BURT: No.

MR. KASUNIC: -- the product being disabled?

MR. BURT: It is in a sense apples and oranges because, on the one hand, you're talking about disabling the product altogether; on the other hand, you're talking about disabling the database. But that's part of the product. That code that protects the database is part of the product. If they have compromised the code that is used to protect the database, they have compromised the whole product. They have compromised the whole software --

MR. BAND: They haven't compromised it;
they have researched it. But, again, if they disburse that beyond the narrow purposes permitted under the exemption, you know, as he said, that would be a trafficking violation. It, again, has nothing to do with the basic issue of circumventing for the purpose of seeing what the database is.

MR. BURT: It certainly does. Again, it violates the integrity of our code, and that violates the integrity of our product. Just the fact that that's public that people can do that violates the integrity and the marketability of our products.

MR. KASUNIC: Okay, well, let's --

MR. FINKELSTEIN: May I respond to that, by the way?

MR. KASUNIC: Yes, please.

MR. FINKELSTEIN: First of all, I think he is conflating two different aspects. One is researching the database, and the other is the operation of the program in use.

I had a comment about this in my submission, by the way, that the definition of harm does not encompass being shown to be a bad product in terms of parity, for example. I'm not going to find the quote, but the idea that, if you have a biting review of a play and this causes the play to shut
down, that is not a copyright infringement, even though it causes economic harm. That is not a cognizable harm to be shown to be insecure.

Let me segue into some comments that he made just earlier about the CyberPatrol case, when they said they wanted to break CyberPatrol. "Break" is a technical term in cryptography. To break something is to figure out how it doesn't work, but it is not necessarily a bragging term, in the same way as copyright infringement also has a term of art where -- what do they call it? -- irreparable harm. That doesn't mean immeasurable harm; it means you get an injunction, as I understand it.

So it is simply a legal standard, whereas to people who hear these terms "break" and "irreparable harm," they may think it far more physically harmful than it is.

I would also like to say that, for all this talk of the pornography sites, since they were blacklists, they are really bad collections of pornography sites.

(Laughter.)

I want to go into this because I get this -- no, let me go into this. People are always asking me this question: "Oh, boy, have you gotten any good
porn sites?" And I tell them, "It's really, if you want to get some good sites, don't look in this censored blacklist."

In fact, I can demonstrate that -- (laughter) -- because when the CyberPatrol blacklist went out, nobody ever said that it was such a great collection. The reason why -- this is important -- I know this is funny, but the reason why that they're such bad lists is because there's so much junk in them.

If you wanted a list of sex sites, would you want to go through somebody else's tastes, sites which didn't work, sites which had changed ownership, or so forth? No, you would want a good collection from somebody who had actually made a collection which would appeal to you, and there are people who sell them. There are people who make them for free. They have absolutely no impact on the research that I am doing.

It is something of a red herring. I know it's a, quote/unquote, "sexy" topic to say that they have these huge lists of pornography sites, but nobody has ever tried, except in a sort of snickering fashion, to use these lists as actual lists of pornography sites because they don't work well that
MR. BURT: If I could just follow up quickly with your question of irreparable harm, in addition to the harm to the security of our product, once our list is available to someone such as Mr. Finkelstein, who has it, are we at that point supposed to just simply assume that he's going to use it responsibly?

We have ceded all control over our copyrighted material, over our database, to somebody else, just on the assumption, without any kind of NDA, without any kind of contract, without any agreement, that he is not going to misuse that property; he's not going to sell it to somebody else; he's not going to profit from it. We have no guarantees of that.

That's the other part of the harm, is that we have lost complete control over our database, over the content that we worked so hard and invested so much money in, and simply trusting with nothing other than the man's good intentions to show that this is going to be used properly.

MR. BAND: But, of course, that is exactly what happens in 99 percent of the times with most works that are distributed to the public, that you rely on the copyright laws to enforce them. This is
an important point because it really goes to, what is
the DMCA all about and why did Congress enact it?

    Congress enacted it to facilitate the
development of an online marketplace in the kinds of
works that are distributed to the public. What it was
really trying to do is to say, "Look, we realize that
because of the Internet and because of digital
technology, users, once they get their hands on this
stuff, are going to be able to widely distribute it."

    So the DMCA was necessary, not to protect
a corporate owner against a competitor, but to protect
the corporate owner against infringements made by the
user. Okay? It was a different paradigm from the
typical one, where you are worried about a competing
publisher or a competing author. Here you're worried
about what the users would do.

    In this context, however, what you are
concerned about is what a competitor will do. You are
concerned, mainly, you say, about someone else who
gets your database and gets into business, or you are
worried about what Mr. Finkelstein will do. Well, you
know what, you know who he is and you know where he
is, and you also know where the competitor is.
Therefore, the existing copyright laws are perfectly
adequate to deal with this situation.
It is not the situation where, you don't have the kind of product where people are going to be interested in disseminating it widely on the Internet. It's not that kind of product. It's not like the latest Britney Spears song, for good or for bad, it's just not like that.

Because of the different quality, to the extent you are worried about the infringement that a competitor might make of it, the copyright laws provide you with a complete solution.

MR. BURT: Well, again, I think the other database, you could say certainly the same thing about other databases, that you could say they should rely on that, and no exemption has been granted for other databases, for published databases like Lexus/Nexus and Dialog.

I'm not here to get into a broader discussion about the DMCA because, first of all, I'm not qualified for what the legislative history of the DMCA was about, but we're not only concerned about competitors, but others as well.

You bring up the examples of Britney Spears and CD-ROMs, and I think the rise of peer-to-peer networks, nothing could make the dangers of allowing these copyright protections to be disabled
more clear than the rise of peer-to-peer networks and
the very quick and very easy way in which this
material can be distributed through those networks.

MR. KASUNIC: But one thing here, I wanted
to get back to that, because I know that you are not
here to talk about the broader issue, but you have
referenced all the other database discussion that was
in the previous rule and related the filtering
companies' databases to, for instance, Lexus/Nexus or
Westlaw and other ones.

But in terms of the studies as well
involved in those other databases, isn't there a
difference in quantifying those between when you're
talking about, for instance, retrieval outcomes, when
you're doing testing of those databases? I guess this
goes back partially to the sampling issue and how
effective; that that was one of the reasons justifying
sampling.

But here, where we are talking about
what's going to be excluded and what you'll never see,
Isn't there a distinction between using sampling for
receiving positive results as opposed to receiving
unseen results?

MR. BURT: I don't really think there is
that big of a distinction. I'll tell you why. It's
because, if you're using the querying to access a database such as Dialog and you don't find the record, you'll never know it's there. You have to search for it in order to find it and know it's there. So you really have the same issue because you have a copyright-protected database that you're querying and finding things in it. If you miss some of those things, you're never going to know they're there.

You're saying about a filtering database. So I think the same reasoning should apply. The same objections and flaws that these gentlemen raise about sampling apply equally to databases, is that you're not accessing the entire database all at once, but you are taking a sample of it with any kind of a sampling technique.

But, again, if you look at the published literature, that is not seen as a limitation. I think it's really important to repeat that nobody in the research community that I'm aware of that is publishing professional software, testing research, is saying this about filtering databases, that you can't test them adequately using these querying methods.

MR. BAND: Yes, but I guess, again, you're mixing categories. There is absolutely no public policy consequence of what is or is not in the
Lexus/Nexus database. That is a commercial product, and if I want to buy it, I buy it. If I don't want to buy it, I don't buy it. It has no implication on any broader issues of censorship and the ability of the public to access information.

Whereas, here you are talking about something -- Lexus/Nexus, that is the product. That is what you're trying to access. Whereas, in this whole filtering context, you're talking about what you can't access. Here we are simply trying to figure out, how do we figure out what are we not seeing? It's a completely different situation.

MR. BURT: Well, I think, as a librarian, and I think most librarians would agree with me, that there certainly are public policy implications to fee databases, how they're used, how they're distributed, who has access to them.

In fact, this Panel heard quite a bit of testimony about the public policy implications of Lexus/Nexus databases and other databases of that sort. So, again, I don't think that's much of a meaningful distinction anyway, but you could say there are public policy implications for other databases as well.

MR. KASUNIC: I have a lot of questions,
but I am going to limit it to just a couple more, to
give other people a chance to ask questions.

But since I have you here to ask some
technical questions in terms of how these filters
work, I see in your comment it lists, for instance, it
looks like IP addresses as well as domains or URLs.
Is this mixed in the filtering software? Is some of
this IP addresses and URLs, and individual pages or
whole domains?

MR. BURT: The answer is all three, and it
depends on the filtering database. There are some
filters that rely exclusively on numeric IPs. There
are some that rely exclusively on URLs, and there are
those that use a combination of both.

Some filters tend to block more at a page
level. Some block exclusively at a domain level, and
some offer a mixer. So your answer is complex because
filtering is complex.

MR. KASUNIC: So once something enters the
database, does it stay there? I noticed something in
here that refers to the fact that there is a review of
these, but, clearly, URLs or IP addresses aren't
static. These are dynamic addresses that are
constantly changing. So once something enters the
database, how often is it reviewed to see whether it
still should be in the database?

MR. BURT: Filtering companies do review their databases periodically, because, exactly as you pointed out, the Net changes and your entries in your database become stale after a while because the content changes, the site owner changes, the address disappears, and so forth.

I can't give you an exact figures on how often we check every site in the database, but we do periodically go through and check the sites. We particularly check to see, obviously, ones that are dead. That's a relatively easy thing to check for.

Then we check to see if content has changed. Typically, we don't go through manually each and every site to check if the content has changed, but if there's some kind of indication about the site, using our artificial intelligence, that there's been a change to it, we will go back and take a look at it and re-rate it, if need be.

MR. KASUNIC: So if you find there's a problem through some technical means, you'll go back and look at it --

MR. BURT: Uh-hum.

MR. KASUNIC: -- but not necessarily go through the entire list and recheck them at some
periodic intervals?

MR. BURT: At some point, they all do get rechecked, but it may be quite a while before each site gets checked.

What's really important is the user feedback, too. Through our database, the URL checker is where people can enter sites and ask that they be categorized or ask that the categorization be changed, too. So that is an important source of input for us as well, what the users do.

MR. KASUNIC: Wouldn't the input, then, from people who have had access to the entire database and who were able to find maybe more specific and broader problems with particular categories, wouldn't that input then also be helpful in that same way, that rather than the sort of hunt and peck, you would have more profound input into potential problems?

MR. BURT: We really haven't seen that to be true because what publications we've seen criticizing filtering software that used decryption -- and there haven't been any of those for quite a while, not during the period -- typically, only cited, you know, a dozen or two dozen or so examples and say, "Hey, look, here are problems with the database. This is why there's problems with it," and don't really
tell very much about it.

So any of the decryption research that I have seen, I have not seen anything particularly useful out of that that we would have a use as filtering company.

MR. FINKELSTEIN: May I reply to that? First off, Mr. Burt has just articulated a wonderful reason why decryption is important: because he is a marketing representative. That is his title. He can come to you and tell you anything, and you have no way of knowing if it is true or not, and he has an incentive -- let me put this gently -- to tell you things that put his company in the best possible light.

If researchers are forbidden by law to actually check on what he is telling you, that has profound public policy implications. He has just articulated a very interesting study which would almost absolutely require decryption to be done.

Take a list of things that you know are improper and see how often they get checked just day by day. You can't do this very well with using the validator because there will be too many, and if you start hitting the validator every single day, they'll get suspicious or they could get suspicious. Again,
this comes back to the Consumer Reports testing idea. Consumer Reports does not do their testing by going into the labs of the company which they are testing.

So then see how often the errors are corrected. I haven't done this, true, because I am volunteer. If someone gave me $200,000, like the Kaiser Foundation gave to the people who did the JAMA study, I could do more studies. But I just do what I can.

MR. KASUNIC: Okay. I want to move to just the last couple of questions to, I think, primarily Jon about some comments that were made about the burdens in the rulemaking for this exemption, a couple of things that were raised in Steve Metalitz's comment, and see what your response to some of that is, since we'll be hearing from him later in California on this issue.

Regarding the burden for continued exemption, which the library associations support here, in your view, must a proponent prove how many will be able to accomplish or have actually accomplished the circumvention during a given period in order to sustain their burden?

MR. BAND: I think certainly whether it has been used at all is a relevant consideration, but,
by definition, if the circumvention is permitted, if it's lawful, I think that a lot of things will be happening that no one is going to know about, because it's lawful. There's a lot of lawful activities going on that you don't know about. You find out more about the unlawful activity than the lawful activity.

So I think it's always going to be hard to get the full sense of what the lawful activity is, but I think it is a relevant issue. I think certainly in this instance we have Mr. Finkelstein right here who has given a very convincing example of an important discovery he made using the exemption during the relevant period.

MR. KASUNIC: Okay, and one last point is or question: Do you have any thoughts about Mr. Metalitz's suggestion that, if we do recommend an exemption in this particular rulemaking, unlike the last time, that it should be more narrowly tailored? For instance, he expresses the recommendation perhaps that the scope should be narrowed to include, for instance, requesting permission, as is used in some of the other statutory exemptions, requesting permission first of the filtering company's software.

Do you think that --

MR. BAND: No, I think that that --
unfortunately, was involved with the negotiations of those other exemptions. We very reluctantly agreed to the issue of asking permission, but that was the only way we were able to get anything at all.

I think, again, that is a bad precedent, and I don't think it's a precedent that should be followed here, especially in this context, because it is so easy for the filtering company to adjust what's on its blacklist or not. If it knows someone is going to look at it, if I have to go and ask for permission, then they might say, "Okay, sure, we'll give you permission," but in the back and forth, the conditions, and when they're going to give permission, and so forth, In that month period that might go on, who knows what they might do with their database. They might decide to scrub the database. That's exactly one of the problems of having to ask for permission, that it, in essence, compromises the whole investigative process.

MR. KASUNIC: Well, I guess just in followup, part of what I was asking, do you think that's within our scope, in order to create an exemption that would include this affirmative act by someone seeking to avail themselves to this exemption?

MR. BAND: I haven't thought about that.
I will have to go back and see whether it's -- it's probably not specifically within the statutory authority granted by Congress. But I guess, from a policy point of view, my personal gut reaction is, if the question is, no exemption or an exemption with a request, it is better to have the exemption with the request than no exemption. But I think it's better to have an exemption without any strings attached.

MR. FINCKELSTEIN: I have a comment on that. I agree with what Mr. Band just said, but I also want to say that affirmatively asking permission is like carrying a big target on yourself and saying, "Attack me. I want to do something against you. Marshall all your forces and do everything you can to make sure that my research will be hindered."

I refer to Mr. Burt sometimes as my most dedicated reader because he watches me like a hawk.

(Laughter.)

And this is his job. It sort of comes with the territory. But to make it a requirement for someone to do this is putting immense amounts of grief on them.

Again, let me just respond to some earlier comments here about something that didn't get published, precisely because of this amount of grief.
When you talk about doing a study with circumvention, I just have a hard time conveying how difficult it is. This is why you don't see so many of them. It is a great deal of effort and risk.

First, you have to actually get the software. This is not necessarily an easy thing. If you come and tell the company that you want their software in order to criticize it, when they look you up and see your record, they don't happily turn it over if they know that you're going to do this necessarily.

Then you have to do the work and consult with lawyers or do it entirely without legal counsel. Then you have to worry about what's going to happen when you actually publish it.

I had a paper that I was going to publish during the CIPA trial, and for various reasons having to do with legal things that happened right then, I just decided it's not worth doing this. It's not worth taking the risk of a lawsuit that's going to go on for years and years to publish this material. The more you increase that risk, the more you discourage people from actually doing the work.

MR. KASUNIC: Thank you.

MS. PETERS: Steve?
MR. TEPP: Thanks. I've only got a few questions left along two basic threads.

The first one is on this, as you put it, the architecture approach versus the sampling approach. I find it interesting that Mr. Burt has been able to cite to a number of studies and examinations of filtering software that employ the sampling approach.

So I guess my question to the proponents is, why is it that they seem satisfied with that and they think a reasonably sufficient study, an examination of filtering software, can be done using that method? But you don't?

MR. FINKELSTEIN: Because I am asking a different question. Sampling is easy. It answers one statistical question. If you need a publication, if you need a review, if you're a person who has to write something up for the research journal or for a computer magazine, it is the obvious thing to do.

But if you want to do a deep study, if you want to actually try to figure out, what are the requirements, that is a very difficult thing to do. It's like saying, why are people satisfied with McDonald's hamburgers when there are so many of them, when there are gourmet restaurants? And the answer is
because McDonald's hamburgers are cheap and gourmet restaurants are expensive.

When something is expensive and difficult and risky versus cheap and easy and readily available, you get what's cheap and easy and readily available. But this doesn't mean the expensive and difficult thing is somehow less worthy for being rare.

MR. TEPP: I understand your point. I guess what I'm curious about is, why no one else is interested -- I mean, those sound like interesting questions. Why isn't anybody else looking at this? Why aren't these institutions that conduct these studies interested in the architecture of the filtering software?

MR. FINKELSTEIN: Because there's no money in it and it is legally risky. There is a quote from Ben Edelman, who is part of the Edelman v. N2H2 case, a widely-reported quote: "I want to go to law school. I don't want to go to jail."

When I look at what I spent on this -- "spent" is even the wrong word -- when I look at the effort I put into this, when I could have been building a business during the IPO gold rush, there's times I really wonder if I made the right decision.

Nobody who is looking at a research
project is going to say, "Well, gee, let me put my
research into something which might get me sued, which
might get me unending legal hassles, which might get
me into trouble with the dean, which might get me bad
press, which will certainly get me enmity of these
powerful companies, or I could do something cheap and
easy." What are they going to take?

Look at what happened to Ed Felton with
the threats from the Secure Music Digital Initiative
case. People get scared.

MR. TEPP: Okay, that's segues, actually,
nicely into the second thread I wanted to pursue. You
have been quite articulate about the concerns you have
about the legal consequences of revealing the full
scope of all the actions you have taken and the
chilling effect that the law may have on others who
may be doing similar sorts of things.

But I think that puts back on us an
interesting consideration. What is the justification
for allowing an exception to the anticircumvention
provisions in 1201(a)(1) for allowing activity that,
as you have described it, may very well violate
copyright licensing agreements, trade secrets, et
cetera?

MR. FINKELSTEIN: Because that's not
within the purview of the Panel. The Panel is charged
with figuring out whether the circumvention itself
should be forbidden or not. You can't leverage it.
It's a circular argument.

The courts have the ability, the courts
have the job of judging those other items. But I
think that you have to proceed, assuming that they
judge it lawful, should the Panel itself make it
unlawful?

What I am telling you is that the cost of
going to court to find out if it is lawful is enormous
and ruinous. This often intimidates people from even
trying. That is the risk that I am taking. But when
you do your determination, you should assume that it
is lawful because the court has not decided otherwise.

MR. BAND: Also, if I may, there's a
couple of other possible responses to your question.
One is that the availability of all these other
protections calls into question why Congress enacted
the DMCA in the first place, but that's also beyond
the purview of this body. But I just wanted to
mention that.

I think also, and relatedly, it would seem
to me that in this situation, if someone did a very
close legal analysis, the most likely legal risk would
be breach of contract, but I don't think there would be a copyright violation because any dissemination of the information would probably be a fair use, because you would typically reveal a few sites out of the 4 million, and that would almost certainly be a fair use.

In trade secret, of course, you are allowed to reverse engineer. That is not a breach, that is not a trade secret violation unless, again, you're somehow violating the contract.

So that would be the issue, and I think at that point you could say, well, maybe there's preemption. So you would have to do a very close, lengthy, legal analysis. It could be that at the end of the day you would conclude that to engage in this activity would not be a breach of contract; it would not be unlawful to do that.

But it would require a legal analysis and probably at the end of the day you would say, well, maybe; maybe not, or the risks are -- you know, you will probably be sued, but you might prevail, and so forth.

But I don't think it's a foregone conclusion that to engage in the circumvention, if an exemption is granted, would clearly be unlawful. It
would be a gray area.

MR. TEPP: Okay. Just so we're clear, I am not stating any legal conclusions about what any activity conducted under the existing, or possibly future, exemption may or may not result in, but to the extent that concerns have been raised by the proponents of an exception, that they may face liability under some of the various areas we have discussed, I think it is a relevant consideration.

Certainly, at the very outset, the rulemaking is not to determine whether or not an exception generally is a good thing, but whether or not an exception for the purpose of non-infringing uses is the core question. So copyright is clearly implicated.

To the extent that the Librarian has the opportunity to take into consideration other factors, it doesn't seem to be irrelevant, as a public policy matter, to consider whether or not an exception that's being pursued may be exception for activity that violates other laws.

MR. BAND: No, I agree that it's a relevant consideration, but, again, everything here cuts both ways. I could say that the fact that there are other legal issues involved would lead to the
result that, were you to grant an exception to the circumvention, the exemption would be taken advantage of rarely by people who would be going in with their eyes open, would receive advice of counsel, and to minimize their risk would occur rarely, and therefore the likelihood of having any adverse impact to the copyright owner would be minimal.

MR. TEPP: Okay. Well, let me turn this on its head then and come over to Mr. Burt and ask: You have cited a number of cases and instances where filtering software companies have defended their legal rights against those who sought to do various sorts of things with their software, and specifically the database that's the heart of the software.

So my question to you is: Don't those also demonstrate that, even without the protection under 1201(a)(1) prohibiting circumvention, you do have adequate legal measures to protect the industry, and that, as a result, an exemption, if a new one is granted going forward, has relatively little likelihood of adverse effect?

MR. BURT: Well, we would like to get this exemption, too, just as all the other database publishers do as well, just because we think we do need this extra added layer of protection, and that
is, in fact, why the law was passed in the first place, to provide that -- Congress wouldn't have passed the law if they didn't think that there was a need for greater protection.

I think, as I mentioned earlier, the rise of peer-to-peer networks and the very rapid, widespread ability to distribute large files, large database files such as ours, makes the need for this extra protection really clear.

MR. TEPP: Well, I don't want to start a debate over the adequacy of protection. Obviously, we have, for example, the Napster case, which shows that copyright on peer-to-peer networks can be addressed through the courts in the United States.

What is it that you have seen or that you think is likely to occur that isn't protected in some other way and then that shouldn't be allowed?

MR. BURT: The circumvention of our copyright protection for our database, just to get in there. You're asking me really to talk about how specifically different aspects on copyright apply to us as a company, and I'm really kind of reluctant to go down that path because I'm not a copyright attorney. I'm not familiar with how each individual law applies to us. So I guess I have to defer that
question a little bit just because of lack of legal knowledge.

MR. FINKELSTEIN: Let me just make a remark. As you say, the exemption is for non-infringing uses. The problem is, though the use may in theory, if argued out in a four-year legal case, be determined to be non-infringing, it is very difficult to be the person who goes through that court case for four years to establish it.

I would like to quote from the CyberPatrol case, from one of the programmers who wrote about this, and what he wrote has been very affecting to me. He wrote, "What I found out was that those organizations, through no fault of their own, were able to give me a lot of sympathy and not enough of anything else, particularly money, to bring my personal risk of tragic consequences down to an acceptable level, despite, incredibly, the fact that what I had done was legal. Ultimately, I couldn't rely on anybody to deal with my problems but myself. Some people learn that lesson a bit less impressively than I had to." I'm trying not to learn that lesson impressively either.

(Laughter.)

And I would also like to quote from the
CyberPatrol case, which Mr. Burt brings up. One of the initial statements says, "The defendants don't have a fair use defense because they haven't submitted one." So he's using the case where there was no defense, and the reason there was no defense to establish that this was a non-infringing use was this personal risk of tragic consequence to the person who did it. Do you see my problem?

MR. TEPP: Well, I do. Let me turn it around on you, I guess, and say, if there are so many chilling effects from other aspects of the law, does that not limit the potential utility of an exception to 1201(a)(1) because that's only one of the myriad of possible darts that could be thrown at you?

MR. FINKELSTEIN: What it says is that this is not the be-all-and-end-all of the investigations. This is just one part of the risk.

As I said, it's a hierarchy. In this case, what we're talking about is the ability just to do it, to say that you have done it. It may not be the case -- let me make sure this doesn't get too convoluted.

If you have this prohibition in place, then you can't even do the work. You can't even say that you've done it by decryption, and if they ever
find out that you have done it by decryption, you are liable.

It is not necessarily true that, if you have the ability to do it, that you will do it. But if you don't have the ability to do it in the first place, then you will never do it at all. Is that clear?

MR. TEPP: I follow you. All right, thank you.

MS. PETERS: Charlotte?

MS. DOUGLASS: I just have a few quick checking questions, actually. I would like to know what is the -- if you could just give me a general idea of the decrypting community? How large is the group of people who are likely to need to decrypt over the next three years? Or what is the community like?

MR. FINKELSTEIN: There aren't that many people doing it because, as I say, it's risky and not a lot of money. So you either find people like me, who are extremely dedicated to civil liberties, or you find other people who have no idea of what they are getting into.

(Laughter.)

I, in fact, do know of some people who have done this work and not revealed it. I haven't
asked them why they have not revealed it, but it is
again the case, if they are not going to tell me why
they are doing it, I can't tell you that they exist.

MS. DOUGLASS: So it's not a community of
one or two, or whatever?

MR. FINKELSTEIN: It's maybe six people or
so, but who knows who else is out there that may
someday suddenly get the idea to do this either for
dedication or ignorance.

MS. DOUGLASS: Okay.

MR. BAND: But I would just make two
points. One is, obviously, this is a subset of a much
larger community that is engaged in encryption
research and security testing generally. So this is
a subset of a larger group.

I also think that if the Supreme Court
reverses the lower court in the CIPA decision, and then
schools and libraries are required by law to use the
filters, if they receive federal funding, I suspect at
that point the public interest in the issue will rise
significantly, and at that point the group of six
might become twelve.

MR. FINKELSTEIN: It might become a growth
industry.

MR. BAND: Yes.
(Laughter.)

But I suspect at that point, once people start seeing that it has more and more of and more and more businesses start using it, but especially once the public schools and the public libraries across the country are all required, if that unfortunate day comes where the Supreme Court reverses the lower court, then I think you will see -- and that would happen within the next three years, probably within the next three months that they will make their decision.

At that point you'll see, you could see a potential growth, but still it's not going to be an exponential growth because you're talking about something that's very hard to do. Again, you do have the sampling option, which is a simpler, less-refined approach, which tells you something but it doesn't tell you everything.

So the group of people who are going to pursue that, dig down to really get all the details, to really understand completely what is or is not blocked, is always going to be a relatively small group of people.

MS. DOUGLASS: Okay.

MR. FINKELSTEIN: I would like to say it's
not like Napster.

(Laughter.)

MS. DOUGLASS: Okay. I would like to ask you, Mr. Finkelstein, how many different types -- or is this something that can't be grasped by just a layperson -- how many different types of research methods are there in terms of, you know, there is decryption; there is maybe log filtering; there's querying? How many particular categories are there in order to do research on filtering websites?

MR. FINKELSTEIN: Oh, you've basically covered the main ones: sampling, log investigation, and decryption.

MS. DOUGLASS: Oh, okay. Thank you.

I have a question for you, Mr. Burt. That is about harm. Do you believe that any of the companies that are now in business would be harmed to the extent that they might not be in business; they might decide, "Well, there's all of this encryption going on; we might as well close up."? Is that the kind of harm that's taking place?

MR. BURT: I think if the decryption were to become widespread and the publication of the lists and availability of the lists were to become widespread, that would drive some companies out of
business because they would lose all of their investment, because other people would be taking it.

MS. DOUGLASS: But the publication of the lists might be a copyright infringement. So just the decryption itself, would people -- I'm thinking back to your comment on, I think someone cited to us, saying that the 2000 exemption did not have any harmful effect on your industry.

So I'm just trying to get a grip on particularly the exemption's harm to your industry.

MR. BURT: Well, again, as I said earlier, it didn't have any harm because nobody has used the exemption that we know of.

MR. BAND: But Mr. Finkelstein has --

MR. BURT: Excuse me. I'm being censored here. I've got to talk.

(Laughter.)

I'm a librarian; I can say that.

As far as I know, no one has used this exemption to do this kind of research. That's why there hasn't been any harm that I'm aware of. But, again, as I said, the harm could be quite bad. If the exemption were heavily used and people were trafficking these lists quite widely, the harm could be quite widespread.
MR. FINKELSTEIN: David, will you authorize me to send to the members of the Panel the complete N2H2 blacklist to prove that I have, indeed, circumvented the encryption?

MR. BURT: Again, as I said earlier, I can't make legal decisions like that for my company. I'm not empowered to do that.

MR. FINKELSTEIN: Well, then, will you reserve your characterization because of the fact that I have offered to prove it?

MR. BAND: Not to belabor the point, but this is a little bit like the Iraqi Information Minister saying, "No, there are no American troops in Baghdad," when, the American troops were right there. You keep on saying, "No, no circumvention has occurred," when right next to you there's a guy who has said a dozen times, "I circumvented it and this is what I did." I am a little surprised. That's all I can say.

(Laughter.)

MR. BURT: Well, I think it's certainly illustrative that you have compared the filtering industry to the Baath Party, what you think of it.

(Laughter.)

I think Mr. Finkelstein would probably
agree with you.

(Laughter.)

MR. FINKELSTEIN: I think more like China.

MR. BURT: But Mr. Finkelstein has, as you said, he said, that is the only evidence he has presented, the only --

MR. FINKELSTEIN: I have offered more evidence. You just won't let me present it.

MR. BURT: Well, you guys won't let me talk or I would finish.

The only evidence he has presented is this inference, based on inference, about this loophole category that, by his own admission, that information was publicly available. So I don't consider that proof.

So I'm curious, what exactly proof? Are you offering to mail my company a copy of our database?

MR. FINKELSTEIN: No, I'm offering to e-mail it to all the members of the Panel. I'll cc you if you want.

MR. BURT: Why don't you just simply send it to our company?

MR. FINKELSTEIN: Why would I do that?

(Laughter.)
MR. BURT: Well, okay, you're saying you want to prove that you did this. So why don't you send it to our company instead of the Panel?

MR. FINKELSTEIN: I think that the Panel might make better use of it.

MS. DOUGLASS: I actually think that I am finished with my questions.

(Laughter.)

MS. PETERS: Good.

MR. FINKELSTEIN: One more legalistic comment: Again, in N2H2's own documents -- I want to stress this -- they say, "N2H2 does not believe that the final rule will affect the value of its lists of blocked websites." That is them saying it, not me.

MS. PETERS: I hear you.

Actually, there was a lot of interaction between the panelists, which was very helpful. However, I want to make sure that, if any one of you has a question to ask anyone else, now is the time.

Jonathan says no.

MR. FINKELSTEIN: No questions at this time.

MR. BURT: No questions at this time.

MS. PETERS: All right, then I want to thank our three witnesses: Mr. Band, Mr. Finkelstein,
and Mr. Burt. It was very helpful.

MR. FINKELSTEIN: Thank you.

MS. PETERS: And we'll be back this afternoon. You won't, but we will.

(Laughter.)

(Whereupon, the foregoing matter went off the record for lunch at 12:12 p.m. and went back on the record at 1:33 p.m.)
MS. PETERS: Okay, we're going to resume this afternoon, turning to a different topic. It's the copy-protected Red Book Audio Format compact disc.

You weren't here this morning. How we are going to do this is each of you gets to make a statement. Then we'll ask questions, and then you can ask questions of each other. How it worked this morning was, though, the Panel asked questions of each other as we went along. So we'll see how this plays out.

We're going to start with the proponent of the exemption, which is you, Seth, and then go to you, Thomas, and then end up with you, Steve. Is that okay?

So let's begin.

OPENING STATEMENT BY SETH GREENSTEIN

MR. GREENSTEIN: Thank you very much.

Good afternoon.

MS. PETERS: Good afternoon.

MR. GREENSTEIN: On behalf of the Digital Media Association, first of all, thank you very much for inviting us here to testify on behalf of our proposed exemption.
Before I begin, I would like to make two important points. The first point is that webcasters also seek to promote legitimate enjoyment of music with compensation to copyright owners and to artists.

A lot of what we do involves promotion of compact discs by exposing the audiences to new music and through online commerce, "Buy" buttons and links to sites where CDs are offered for sale.

We empathize with the labels' efforts to secure that market. We recognize what's happening to the CD market. We are concerned about it, too. Music is a very important part of what we do. To the extent that the record industry is suffering because of lag in CD sales, we feel the pain as well.

The second point I would like to make is that, in fact, the exemption that we are seeking is not our preferred solution. The preferred solution really is to be able to work together with the labels to ensure that all webcasters have access to all non-protected, high-quality recordings from all labels. That would be the preferred solution.

The problem is that there are so many labels and so many webcasters that it is, frankly, not possible to do that. It's not possible, I think, for the Recording Industry Association to make any kind of
a guarantee in that regard.

Thus, we are here today, largely because we see the protected compact disc coming at us, and we are concerned about how the future will affect webcasters as a whole. Webcasters need to have access to sound recordings. Some webcasters play compact discs directly on CD audio players or from computers, more likely. But most of them make ephemeral recordings of those compact discs.

We need ephemeral recordings for a number of reasons. First, we have multiple servers to handle the level of traffic that comes into our sites. So we need to have a copy for each of the servers.

We need to have copies that are optimized for transmission in high quality at different bandwidths. Some people still connect through dial-up access as well as through various levels of broadband access. We need to have copies that are optimized for each of those transmission means.

Of course, there are different transmission codecs that are used. The Windows Media Player is one; Real Player is another; QuickTime for Apple, or MP3 streaming. Those are some examples of the different kinds of codecs that are used for making webcast transmissions. For each of those transmission
formats, there needs to be a file in that particular format.

Webcasters' libraries include hundreds of thousands of recordings for the major webcasters. Typically, for a particular channel, there will be several thousand that are active at a given time or for a particular genre. There will be several thousand that are active at a particular time, and, of course, new songs are added constantly. Some of the old songs in the catalog are cycled through, so that the sound of the service remains fresh.

A few webcasters have very sizable businesses that are capable of reaching very extensive audiences, similar to the types of audiences and size of audiences that some radio stations reach. But most webcasters are small businesses. They are startups. They hope to become big businesses some day, but they are still in their early stages of development.

The Digital Millennium Copyright Act, and particularly the statutory licenses under Section 112 and 114, entitled all of these services to have the same degree of access, the same license rights. So that all these services could have access to the same music at the same royalty rates and on the same terms.

The DMCA created a level playing field, a
secure marketplace where success would be built on the entrepreneurial acumen of the leaders of the services, on the technological innovation of the software that's used and the web developers who develop not only the music transmission means, but also the look and feel, if you will, of the site.

The sound quality of the service, of course, is a very important attribute of the success of a service, and, of course, the ears and the skills of their music programming staffs.

The basis of competition among webcasters, therefore, are the features that they offer, the visual impression of the website and of the player, the marketing acumen, the brand recognition, the ancillary services and information that are offered, the music programming skill, of course. But key among these also is the timely availability of sound recordings and the sound quality of the webcasts themselves.

Internet radio has many benefits for the public and for copyright owners of sound recordings. We play more genres of music than you will ordinarily hear in a particular marketplace of radio. You will hear music by more artists. You will hear deeper cuts off of particular artists' albums.
But, of course, they also have pop channels where consumers expect to hear the latest hits as they are being released. Webcasters, we believe, have a chance to be highly competitive with radio and to beat radio at its own game in many respects. Small webcasters have the opportunity to be competitive with other webcasters, if we are offered the chance to survive and grow.

One of the most fundamental concerns the webcasters have is the concern of having prompt access to music. Radio stations typically receive service from record companies. Some webcasters do, but, typically, most webcasters don't receive sound recordings from record labels.

Webcasters most often purchase sound recordings at retail. They then take these compact discs and rip the CDs onto their webcast servers. Another avenue for some companies is that they will contract with a third-party company that will already pre-rip the sound recordings into files and formats that can be used by various webcast services.

As I noted, many genres of music and many webcast channels rely on the influx of new music. Particularly pop channels need access to music on the day and date when they are released. A top 40s
station, top 40 channel, has to have the top 40. It's quite often the case that a song will debut in the top 10. It won't work its way up the charts from No. 200. It will debut at the top. These services need to have access to the sound recordings as soon as they are released.

For those webcasters who do receive advance copies, it is very important that their files can be on their servers before the date that the CD actually reaches the marketplace, so that they can be ready and able to webcast as soon as the date of release arrives.

But, ironically, the advance copies that are sent to webcasters are most likely to be the ones that are copy-protected. Again, it is a legitimate concern that the record labels have that these may leak onto the Internet services such as KiZaA or similar Internet peer-to-peer services, often get access to sound recordings before they are released on the street and released in stores. The way that that often occurs, or one way that that may occur is from advance copies.

These are the copies that are most likely to be copy-protected, but these are also the copies that we, as webcasters, are vitally interested in
getting access to early, so that we can rip the files
onto our servers and have them ready for webcasting on
the date that they are available for broadcast.

Well, given the webcasters' shared
interest with the record industry in promoting lawful
services for sale and consumption of music, we
understand, we share the frustrations that apparently
motivate their desire to apply these technological
protection measures to audio compact discs.

But we are concerned that the interest and
content protection will result in additional
disadvantages and impediments for the success of U.S.
webcasters. Over the past few years, there has been
talk about labels applying protections to compact
discs in the United States. There are few known
experiments here in the United States to date. The
soundtrack for "More, Fast, and Furious"; there's a
Charlie Pride CD. We have heard that the Donnas has
been released with content protection, and some
others. It is much more common in Europe, in
Australia, and elsewhere.

Recently, Macrovision issued a press
release that was picked up in the press that said that
there were 100 million discs that they had released in
other markets that were encoded with their system.
SunnComm has announced that they have contracts as well for a different kind of a system for applying protection to compact discs. Again, so far, this has happened mostly in Europe and elsewhere. But there are articles that are indicating that record labels are planning to do this in the United States as well.

Up until now, the systems that have been used have not worked very effectively. I have talked to a number of DMA members who have said that they have encountered copy-protected audio discs in the past, and the content protections don't work particularly well. They were able to try multiple times to get access to the content, and the content protection system eventually failed and they were able to do the ripping.

But systems are getting better. They are getting more sophisticated, and we can't count on getting access to the sound recordings without circumvention.

As I mentioned, recently, Arista Records, a major record company, part of the BMG family, has issued a news report saying that they are going to begin applying protection measures more widely, even in the United States, to all their products. As I noted, this has happened at least currently with
These content protections take a number of different forms. Some of them you could call copy protection; some of them you could call access control, in that some of them prevent the discs from playing on computing devices. Some of them also prevent ripping.

Some of them have what is called the second session; that is, in addition to the music in the compact disc Red Book Audio Format, they also include a second compressed version of it that is either playable on a computer but not able to be ripped from the computer onto a hard drive or may allow some limited types of ripping, but it's in a particular compressed format that is not as high quality as the Red Book Audio Format itself.

So the application of these protection measures creates some fundamental problems for many Internet webcasters. First, of course, delay in getting the recordings onto our services. Second is the impact on the sound quality.

If the only content we have access to is through the second session, which is a compressed file, then the sound quality of what we are webcasting is not going to be on a par with the other sound.
recordings that we are webcasting.

Third, of course, rather obviously, there's an economic aspect to this as well, even pursuant to the statutory licenses. As you know, the past decision of the CARP was that webcasters are to pay 8.8 percent of their license fee for performing sound recordings for making ephemeral recordings. And if we are prevented from making those ephemeral recordings, essentially, webcasters are paying for a license right they cannot use.

We believe that we meet the standards that are set by the Copyright Office and by the statute for this exemption. Clearly, the making of ephemeral recordings is a non-infringing use of the class of works.

We, as webcasters, are likely to be adversely affected by this prohibition. It's not just a matter of inconvenience or expense. This is a substantial adverse impact on the competitiveness of services, the ability to compete based on the availability of sound recordings at the time when others have access to them, and as to the sound quality. Ultimately, it has an impact as well on the dissemination of copyrighted works and the availability of copyrighted works to the public via
webcasting.

This is a measure that controls access to copyrighted works. As I noted, some are access controls, in that they do not even permit the CDs to be played on computers. Some are copy-control measures.

But I submit to you that Congress has said something important with respect to the applicability of Section 1201(a)(1) to this particular case, because the exemptions that were provided in the law, the limited exemptions that were provided, specifically note that those who take advantage of circumvention pursuant to the exemptions are not to be liable under 1201(a)(1).

If 1201(a)(1) did not apply with respect to the making of ephemeral recordings, then there would have been no need for Congress to have included 1201(a)(1) in the language of the exemption. Because they did, they recognized that there was an implication under 1201(a)(1), even with respect to the making of ephemeral recordings. Therefore, an exemption from 1201(a)(1) ought to be available to us as well.

Now if these protections are widely applied, what are the options that are available to
webcasters? Well, Option No. 1 is, pursuant to the exemption, we can ask a label to provide us with an unprotected copy. They may refuse or they may delay giving us access to the recording.

We may not know when recordings are coming out. We may not know when others are receiving promotional copies of recordings in advance of the release date.

The statute provides no definition of what is a reasonable time to delay before you are allowed to circumvent. A reasonable time in webcasting is really instantaneous, because when others have access to the content, we need to be competitive; we need to have access to the same sound recordings that others are able to webcast. Otherwise, the compulsory license and the intention of Congress to create a level playing field becomes meaningless.

Another possibility is that, if we ask a label for a copy, they may provide a copy in compressed form, and the compressed form may be in a lower sound quality to the quality that we otherwise webcast on our services.

Under the current exemption, once provided with a lower-quality, compressed version, we would have no option to circumvent. The statute itself
seems to say that, if the copy is provided, we have no ability to circumvent without a further exemption under 1201(a)(1).

Another possibility, of course, is that when we ask a label for an unprotected copy, they may give us a copy in a format that is not used by the service. They may provide it, for example, in the Windows Media Player format, just as an example, when the particular service operates using Real Player transmission means. If that's the case, then we will have to convert the file from Windows Media Player, which is itself a compressed format, into the Real Audio format, which results in yet further audio degradation of the signal.

There is a second option available to webcasters, if protections are widely applied, which is we can try to obtain the files from a third-party ripping service. That, of course, increases the expense, and that expense is not economically feasible for many smaller webcasters.

Of course, there is the possibility that even the third party's efforts to obtain access to a copy-protected file may be thwarted by the technological protection measure. So the third party may delay in having access to the file or may not have
access to it at all, if their attempts to circumvent are unsuccessful.

Option No. 3 available to webcasters is to develop your own circumvention tool. Well, that's what's contemplated under the statutory exemption. It is, of course, time-consuming. It assumes that there is a high level of skill even among small webcasters to be able to perform that circumvention.

Of course, there is no guarantee that a particular service is going to use a specific content-protection method. We will have to have available on staff someone who is able to circumvent various copy-protection means, various content-protection means, and to continually work on these means as the technological measures themselves evolve and become more sophisticated.

There is, of course, a fourth option, which is we could take the analog output signal from a CD audio player, not a PC, digitize it, and then put it into different formats as necessary. But, of course, that results, again, in lower sound quality than going directly digital to digital.

It is inconvenient. It involves additional expense, and, of course, there is no guarantee that there will not be future analog-
protection means applied. So that, in and of itself, could be a temporary solution.

I guess in closing what I would like to say is that DMA and our members really hope that this is a problem that can be resolved without an exemption. We hope that this is something that can be resolved among copyright owners and webcasters.

But, if not, and there are some practical problems to resolving it between every webcaster and every sound recording copyright owner, we need the safety valve that is intended to be provided by Congress through the 1201(a)(1) exemption. In particular, the kinds of safety valves we're looking for: the ability to circumvent without delay. Particularly, that's true in cases in which a copyright owner previously has refused access to a particular sound recording.

The statutory exemption seems to imply that the requests to the content owners have to be made on a sound-recording-by-sound-recording basis. We would think that, once refused, we ought to be able to immediately begin circumvention efforts because of the likelihood that the refusal is going to be repeated. Doing it on a sound-recording-by-sound-recording basis for the tens of thousands of sound
recordings that are issued every year is simply not practical.

Second, we would seek the ability to circumvent where the music files that are provided to us by a content-owner, if provided, are not of a quality that is equivalent to the other music files that we webcast on our services.

Lastly, of course, where the music files that are provided by a particular content owner are not provided in all formats that are needed by the service, we would need the ability to go back to the highest-quality available recording and do the encoding into a particular format. So, once again, we are certain that we are able to webcast in all formats with sound recordings of equivalent quality.

In closing, we would say that we believe that the exemption is justified, and we request that the exemption be granted. Thank you.

MS. PETERS: Thank you.

OPENING STATEMENT BY MR. LEAVENS

MR. LEAVENS: Good afternoon. My name is Tom Leavens. I'm General Counsel for Full Audio in Chicago, and we want to thank you for the opportunity to be here and provide our views on this issue with you this afternoon.
Full Audio is a digital music distribution company located in Chicago. We were formed four years ago. We launched our service in April of last year. We have recently relaunched under the name Music Now.

I should say, initially, to echo some of the remarks that Seth has made, that we support all the efforts to ensure the protection of the legitimate distribution of music. We are not against copy protection. Our interests are aligned with the record companies in that respect. We want them to be healthy. They provide the very thing that we sell. So we are very much aligned with them in that respect.

We are here today simply to talk about a very specific operational and competitive issue that we see coming. Our content partners are all the major labels. We have agreements with Universal, Warner, EMI, BMG, and Sony. We have agreements also with the independents Sanctuary and Koch, and we are also working to add additional independent labels onboard with our content. We also have an agreement with the Harry Fox Agency, which is along the lines of the agreement that the RIAA has with the Fox Agency.

So our goal from the beginning was to be a legitimate licensed business. We have achieved that. We enjoy good relations with our content
suppliers.

Our distribution partners are Microsoft. We are embedded in the Microsoft Corona Player, along with Pressplay. We are distributed through Clear Channel, through Charter, and through Earthlink.

As far as my own personal experience, I spent eight years as General Counsel for a record company prior to joining Full Audio about two-and-a-half years ago. So I can speak a little bit from the perspective of operationally what goes on within an independent record company.

The service of Full Audio initially involved only conditional downloads. In relaunch, which occurred last month, we also added permanent downloads and DMCA-compliant radio. So our experience with radio is relatively recent.

We maintain different files for each one of these features, each one of these functions, at different bit rates. For example, we have radio which is offered both at a 32-bit rate and a 128-bit rate. We also have our downloads with separate files at a 128-bit rate.

So we have a need for making sure that we have files not only at this different bit rate, but making sure that it's in conformance with the codec
and the DRM that we are using, which is .wma.

We obtain our files principally from compact discs. We also do receive some electronic files from the labels that we have that our content deals with, and we have also purchased some files from a third-party supplier, as Seth has mentioned.

We prefer to use compact discs for the reason that it is an actual object that gives us a lot of information, which is important, on publishing, but it is also important for us to be able to re-encode when we need to, for any number of reasons, whether we're going to be upgrading on the bit rate or in the case where we have loss of files, which has definitely occurred I shouldn't say a lot, but when it does happen, it is important for us to be able to replace a file very quickly. Having CD is the best way to do that.

We have on the radio side over 200,000 files currently in our service, and we are adding thousands of files to that radio service each month. It is a process that must be an automated process. We cannot have exception processes involved with the way in which we add files to our radio service. Every time we have an exception process, it adds by a level of magnitude time that is expensive for us, that puts
us at a competitive disadvantage.

Every time that we have to in some way single out a particular disc and deal with it on an individual basis, it's an extraordinary expense to us because it takes away from the systems that we have set up in order to accommodate the massive amount of music that we need to be able to put into our system in order to be competitive.

The process not only has to be automated because of its volume, but we also need to be able to identify and track the files in our system for purposes of meta-data and for purposes of being able to report usage. It's very important that each file, when it comes in, has an individual file number attached to it. We track it through the system. When anything about that file appears in the service, there has to be an associated meta-data to accurately describe it. There's all kinds of reasons why this is not something which -- it is not a system that is susceptible in any way to individual attention.

We have been following the developments in the copy protection and have been talking to our content suppliers about that over the course of our initial negotiations with them and during the time that we have been in agreements with them. It has
principally been along the lines of the consequences, the implications to us, for our conditional download service because that is what we have been doing up to about a month ago.

We have received assurances that things are going to be worked out with respect to the people that we have talked to, and we have no reason to believe that that's not the case.

We want that to happen. It is not only that it is going to be easier for us if that happens, but, of course, we are paying under the DMCA for the right to make ephemeral copies. We think that implies an obligation to deliver means for us to be able to make one.

But here are our issues: We don't know when a recording is going to be copy-protected at this point. It's anecdotal. It's maybe something that we learn for the first time when we try to encode something. But if it's part of this automated process, it's not going to come to our attention really until it gets kicked out in some way when we're trying to encode something.

We don't know what solution has been applied for the copy protection, what it is that we would need to do in order to make a copy from that,
where it is that we would go.

As Seth mentioned, we don't know really how it is that 112(a) would be interpreted with respect to whether the notice that we would give to the record company would be a blanket notice or whether it would be individual notices. If it is individual notices, again, that is something which we just really can't accommodate, given the number of files that we are dealing with on a monthly basis.

We don't know what a reasonable time would be for us to have to wait. We don't know how that is going to be interpreted by our competition either with respect to how long we keep something out of our service before we would implement any kind of any circumvention or any circumvention efforts.

We don't really know, either, what our recourse would be in the event that there is a problem with a file that is delivered to us. The problem could be the quality of the file delivered or the format or some other kind of incompatibility. We don't understand really what it is that would be our alternatives under those kinds of circumstances.

We know, we believe that the issues that we would have with respect to the type of protection that we would be getting or that we would be
encountering from the record labels is not really a question of bad intent as far as their performance. Our content providers have worked hard to deliver content to us under our conditional download service, and we see that this is probably something that is going to continue as we go into radio, although we have not been receiving any service with respect to our radio service.

I am not sure how many webcasters do receive service for the webcasting. Any of the service that we have received has been only in connection with our conditional download or permanent download service. It would not include any files that go beyond that, because, obviously, anything that the record company releases is something that we could use for radio, but we have not received any files that go beyond just what is available for our download service.

What is going to happen really is that, while there has been this productive work that we have encountered with the major record labels that we are dealing with, that as they deal with this issue of copy protection, that, first of all, there is a greater amount of content that they are going to have to deal with, obviously, as opposed to the subset that
we get licensed.

They are going to have to deal with a
greater number of companies, which are going to be in
the several hundreds as opposed to -- I'm not sure how
many are the shipment licensees, but I don't imagine
that it's more than 25 or 50-something that they are
currently dealing with at this point.

And there's the greater range of encoding
requirements that each of the webcasters are going to
have as well. To the extent that we have received
files from the record companies, they have been files
that have been according to requirements and
specifications that we have worked out with them, but
we're just one company. We would need, for example,
in addition to what we are getting for a conditional
download, we would need files for our radio that would
be at two different bit rates for .wma.

The range that the record company would
get would be -- I can't imagine the different numbers
that the other webcasters would be having or all the
different encoding requirements that they would have.
But the record companies are going to face a
tremendous number of variations in those files which
is far different than what it is that they are serving
up today.
Our fear is that the introduction of the copy-protected discs is going to overtake the ability of the record labels to service all the webcasters without creating some kind of competitive disadvantage somewhere. That ultimately is what it comes down to for us.

We also are concerned that the smaller companies, the independent companies, are not going to have the resources in order to serve the files that would be necessary in order for us to be able to use recordings that are otherwise copy-protected. Having worked for the small record company, I know the resources just aren't there to be able to do that.

The independents that we have used have been very cooperative with us, but the systems that they have are not the same as the systems for the larger record companies and they are not going to be in a position to be creating those just for the purposes of serving us as webcasters.

Then there are some companies that just may elect to give just favored service to others, and that is something that we just have to anticipate is going to occur at some point.

In essence, what is preferable for us is the record companies be able to self-execute on this
compulsory license that we have under the DMCA, that
we not be involved with a complicated process whereby
we have to be making approaches, waiting for periods
of time, having to put ourselves at jeopardy of a
competitive disadvantage of some kind of way to
exercise the rights that we have as webcasters.

As long as our webcasting is DMCA-
compliant, just as with the mechanical license that
the record company has for phonorecords, it's simply
an elective process that they undertake without having
to take any other steps dealing with the publisher.

Our goal would be to be in that same position, that we
would not have to be required to be approaching the
record companies in order to be able to exercise the
rights under the DMCA.

Thank you.

MS. PETERS: Thank you.

Steve?

OPENING STATEMENT BY STEVE ENGLUND

MR. ENGLUND: Thank you for the
opportunity to present the views of the Recording
Industry Association concerning DMA's proposed
exemption.

We appreciate the concern that the
webcasters have expressed for the piracy concerns of
record companies. We also recognize that webcasters are, in fact, licensed under Section 112(e), are entitled to make ephemeral copies, and many record companies work productively with many webcasters to make that happen in ways that are entirely outside the statutory process.

It just appears to me that, based on the things that we have heard from Seth and Tom, that it is not necessary for webcasters to receive permission to circumvent access controls in order to have access, and it may not be quite the panacea that it might first appear if they were to get that permission.

It's important to begin, though, with an understanding of the purpose of Section 1201 and this proceeding. Congress enacted 1201 because it recognized that access-control and copy-protection technology are desirable tools that copyright owners should be encouraged to use, and that these technologies can, in fact, increase access to works.

So 1201 is designed to promote the use of these technologies. We are concerned that any inclusion of copy-protected CDs on the list of exemptions will undercut Congress' intentions in creating Section 1201 to promote the use of such technologies.
But Congress did create this proceeding as a failsafe mechanism, but this failsafe mechanism applies only to technologies that control access to works. The purpose of this proceeding is to ensure that access is not unjustifiably diminished.

This proceeding is not about copying. Yet, all we have heard from Seth and Tom is about copying.

The very name of DMA's proposed class for the exemption contradicts its place in this rulemaking. Protected CDs are primarily designed to inhibit copying, not access. While it's true that some copy-protected CDs might, as a technical matter, employ both access and copy-control measures, it's very clear from what we have heard this afternoon that DMA isn't concerned about access because there can be no question that webcasters have access in a variety of ways. Their concern is about copying.

We heard from Seth that one of the options available to webcasters is to play a CD that is copy-protected on a CD player. Seth suggested using the analog output to make copies. I submit they can use the digital output to make copies, if he's concerned about analog-to-digital signal degradation, but it is very clear that a copy-protected CD can be readily
accessed and that copies can be made from it if webcasters need to make copies. They can access it in the digital domain if they need to make copies.

So, in addition, there's no assurance under Section 112 or Section 1201 that webcasters, or any other user of copyrighted works, ought to have access to works in the most convenient means. I think that it is sufficient that webcasters have access to make copies in the digital domain as they do. There's no need for an exemption.

In the last rulemaking on this subject, the Office rightfully rejected requests for DVD exemption under somewhat similar circumstances. You noted, properly, that it wouldn't be a violation of 1201(a) for an individual to circumvent copy controls as long as in doing so he or she did not circumvent access controls. That is very similar to the case that is presented here.

There the Office found that in the case of motion pictures on DVDs, anyone with the proper equipment can access the work, just as a webcaster with a CD player can access the sound recording on a CD. The Office denied the DVD exemption because of the absence of evidence that access controls were being used to lock up material in a way so that there
was effectively no means for a user wanting to making
an infringing use to get access. That, too, is the
situation here. Webcasters have access to the music
on copy-protected CDs by playing them in CD players.

So, in the absence of that evidence, I think you ought to reject DMA's proposal. But even if
there is a genuine issue here as to access, DMA has presented only hypothetical concerns that are well
short of the substantial adverse effect on non-
infringing uses that's required to support an exemption.

They haven't offered any evidence that webcasters have been unable to access sound recordings
in the past, and they have offered only speculation that the copy control might affect webcasters in the
future. As Seth noted, there have been only a very small number of copy-controlled CDs that have been commercially released in the United States. It's by no means clear that there will be a substantially larger number released in the future, certainly not sufficient to support a finding of substantial adverse effect on non-infringing uses.

But even if you thought that there could be, Congress provided the solution in Section 112(a)(2). Webcasters should ask copyright owners,
not the Copyright Office, for the means to make copies.

It has been suggested that circumvention will solve all of the problems of the webcasters. On the other hand, many of the comments we have just heard suggest that it is really no panacea.

Tom talked about his need to have an automatic process with no exceptions, but I think if you give webcasters permission to circumvent, you will end up with precisely the situation that Seth described as unworkable: every webcaster needing to have a staff hacker to circumvent access controls. As the access controls technology changes, webcasters will have to keep circumventing.

So I don't think that Tom achieves his goal of having an automated process with no exceptions because, if he is permitted to circumvent access controls, he is going to have to hack every CD that he receives. Instead, the right answer is that webcasters should do what Section 112(a)(2) says they should do, which is to ask copyright owners for the means to make copies.

Presumably, at least in many cases that will happen because, as Seth and Tom indicated, quite apart from the statutory structure or any issue of
circumvention, many record companies provide files
either in CD form or electronic forms to many
webcasters. In those kinds of relationships, people
can bargain over formats and people can bargain over
delivery and means that will achieve the needs of
webcasters.

But it appears here that the webcasters
are trying to rewrite Section 112(a). We heard
several instances in their remarks that they have
conscerns about the period of time that Section
112(a)(2) gives for copyright owners to provide a copy
that has the means to be copied.

They have particularly taken exception to
the need to have this period of time. They want to be
able to circumvent on the first day that a release
becomes available, even if they haven't previously
known that a release was going to be available. That
is just taking exception to specific provisions of
Section 112(a)(2) that Congress has provided.

In addition, DMA's approach in its
comments at least would likewise ask the Office to
stand conventional statutory interpretation on its
head. In essence, DMA argues that, because Congress
created Section 112(a)(2), Section 1201 must prevent
them from doing something they want to do, and because
Congress failed to include a similar exemption in 112(e), that "omission," as DMA's comments call it, has to be rectified.

But this isn't the proceeding to correct Congress' omissions, nor is it a proceeding to rewrite the terms of Section 112(a)(2). The Office had it exactly right in the rulemaking three years ago when you decided that you should proceed with particular caution when Congress has already made in the statute specific judgments about the scope of an exemption. Certainly, the record before you right now provides no basis for you exercising the heightened standard of particular caution, why you want to essentially rewrite Section 112(a)(2).

As I have already mentioned, this whole issue is highly speculative. DMA certainly has not provided the highly-specific, strong, and persuasive evidence that is required to establish a likelihood of future adverse impact under the standards for this proceeding to apply to the alleged future harm.

It is by no means clear that record companies will ultimately deploy copy-protection controls in any substantial numbers. Even if they do, record companies understand that webcasters may play or are an important outlet for their works. So
Accordingly, the Office should not at this time grant an exemption. The Office can certainly revisit the issue in three years, if there is more evidence of a problem then.

MS. PETERS: Thank you very much.

Now I'm going to turn it over to the Copyright Office Panel, but before I go to Charlotte and ask her to start the questioning, I'm having trouble with one piece, which has to do with access controls. Most of the testimony had to do with copy controls.

Seth, you did say that there was some issue or some of these CDs had access controls. Could you explain what the technology is and where the access control is, and is it in all, a few, whatever?

MR. GREENSTEIN: The access control that has been applied to date prevents a compact disc that is playable in a normal home audio player from being played on a personal computer.

MS. PETERS: Okay. So it can be played on -- so it's that it can't be played on it?
MR. GREENSTEIN: It cannot be played on a computer's CD-ROM drive. That's the nature of the access control that's being applied.

MS. PETERS: But it still can be played on a CD player?

MR. GREENSTEIN: It can, and if you are listening in your home or if you are in some radio broadcast studios at least of the past, they generally rely on audio players. Webcasters don't generally use audio players. It's the rare webcaster that uses an audio CD player rather than a personal computer. Frankly, even radio broadcast studios now are migrating away from pure audio players, going to personal computer-based systems.

So to the extent that this kind of control is applied to a compact disc, it will prevent webcasters from engaging in the act of webcasting at all. Even if there were no copy protection applied, the access control would prevent the ripping from occurring in the first because you could not play it.

MS. PETERS: Do you want to add anything to that?

MR. LEAVENS: Well, just to concur that we launched with 36 channels, and we anticipate that we are going to be adding more. We do not serve that off
of a conventional CD player. We serve that off the computer.

We need to be able to store, and through the programs which we developed, be able to sort and play those files off the computer, and not have somebody sitting at a device and playing a CD off of a conventional CD player.

MS. PETERS: Steve, could you comment?

MR. ENGLUND: Yes, I think Seth has accurately described the technology that is used by many of the implementations here, now not all of the implementations. There are a variety of different technology vendors here. They all use somewhat different techniques. There are some vendors that use somewhat different techniques that we probably would say are not access controls, but Seth is right that there is the large class of the evolving technologies here that could be considered access controls in that they permit access on some devices and not other devices.

But I think it is entirely sufficient for webcasters to be able to access the works on a home or professional CD player because that is all that is required for purposes of this proceeding. They have access by playing it, a CD, in a CD player. They have
perfectly straightforward means of copying that material entirely in the digital domain on their computers using methods that essentially Seth described. As a result, there's no access issue here for the Office to address.

MS. PETERS: Okay. So the record industry, in making its music available, is essentially going to make it available in just CDs that play in dedicated players as opposed to making them available to play on computers?

MR. ENGLUND: I think, as I said, it is by no means clear that record companies are going to use this technology to a substantial degree at all. That is an open question, and yet a further reason why it is premature for the Office to put copy-protected CDs on the exemption list at this time.

There are a number of tradeoffs that record companies face in considering the technology. Certainly, record companies have a substantial interest in deploying an effective technology that permitted universal access and substantially limited copying. But these technologies are not all that effective, as Seth suggested.

Technologies come at a cost, both out-of-pocket costs and perhaps a customer-acceptance cost.
Record companies will balance those considerations and make their own decisions about whether to use this technology or not. Some may, some may not. The particular configurations they use will be their decision, and it is by no means clear what those configurations will be.

Seth accurately described the kind of configuration that many people have talked about, which is a disc that would have two so-called sessions on it, a first session of conventional Red Book Audio that is playable in the ordinary course on a customary CD player and a second session that is accessible in the ordinary course by a computer.

We have heard that it may not be compressed in the way that the webcasters would like it, but, in fact, they are likely to have access on both CD players and computers. So they are asking for an opportunity to circumvent the access controls on the first session because they're not satisfied with the sound quality of the access they get through the second session. But I think that is the question that is being presented to you.

MS. PETERS: Okay, but just on that one that has the first session and the second session, those still have to be on dedicated -- can they be
used in computers?

MR. ENGLUND: The short answer is yes.

MS. PETERS: Okay.

MR. ENGLUND: The interest of record companies is in selling products that can be readily accessible by all consumers.

MS. PETERS: Okay.

MR. ENGLUND: So one of the technological challenges that record companies and the vendors of CD copy-protection technology face is how to achieve universal access, because nobody is going to make money in the record business by selling records nobody can access.

MS. PETERS: Okay.

MR. ENGLUND: The emerging way or an emerging way of doing that is to provide for access differently in the case of CD players and computer CD-ROM drives because there are technical differences in the way those two kinds of drives read the data off the CD.

So the first session provides access on a CD player. The second session provides access on a computer. But the particular files in the second session, which are accessible by the computer, may be compressed so that there's less injury to copyright
owners from having higher-quality files available. They may be secured by a DRM. There are a number of different configurations that are possible.

MS. PETERS: I was just having a real hard time figuring out where the access issue was, but I think I now at least understand it.

Did you want to say something?

MR. GREENSTEIN: I just wanted to address a couple of points with respect to whether the access that Steve suggests is available is actually sufficient. We are talking about professional users here. The kind of access that might be sufficient for a home user is different than for a professional user. Professional users have to be able to work with files in particular ways in order to optimize their services.

Again, we compete based largely on the availability of high sound quality through very small speakers. You have to start with the highest-quality product in order to achieve that. You have to optimize your product. You have to optimize the sound quality of the files to make sure that what comes out at the other end is thoroughly acceptable to the consumer, at least equivalent to the FM or CD experience.
If you start with a compressed file and then have to start processing it from there, it's, well, garbage in/garbage out. It gets worse and worse, deteriorates each time, to a level that is unacceptable and, in fact, creates some disparity of the signal.

We would like our signal to become consistent in sound quality throughout. If some sound recordings sound really good and some do not, then our service is the one who suffers. We are the ones that get the blame, not the record companies, even though it may be the record company's fault.

Finally, one other point that Steve mentioned is, well, perhaps one way we could get access to the content would be to start off with an audio CD player --

MS. PETERS: A CD player, yes.

MR. GREENSTEIN: -- and then take the outputs from that. The formats are different. Again, there's conversions that have to occur, and the conversions will, again, result in some degradation of sound quality.

We would like to be able to go directly from digital to digital in the same digital format, so as to avoid those kinds of problems and to have a
higher sound quality as our end product.

MS. PETERS: Can I just, before we go to
you, Tom, can I just ask a question? With what you
just said, you almost suggest that your recommendation
for an exemption is limited by use. It's by
professional webcasters. Is that right?

MR. GREENSTEIN: Well, inasmuch as every
webcaster has the obligation to pay license fees and
to, therefore, we hope gain some income because of
that, we think of all webcasters as being
professional.

MS. PETERS: So everybody who -- I was
actually trying to get a handle on the scope of what
you were proposing.

MR. GREENSTEIN: Yes. I mean, the
specific exemption that we are seeking is on behalf of
those who engage in the act of webcasting and who have
that need to make ephemeral recordings. It is not a
more generalized request.

Now I also understand from prior rulings
that you have said that the exemption is not on a
user-by-user basis. I would ask you, with great
respect, to revisit that, I would think for the health
of the industries that are sitting here at the table.

Obviously, a generalized exemption to
circumvention is not going to be something that is
good for the recording industry or for our industry.
But, on the other hand, our industry cannot get along
without having exemption and access to these
recordings.

MS. PETERS: Okay.

MR. GREENSTEIN: So I would ask you,
respectfully, to revisit that ruling in this context.

MS. PETERS: I hear your respectful
request.

(Laughter.)

Tom?

MR. LEAVENS: I wanted to make a practical
point, and that is that the option of doing something
in real time with a CD is not really there for us. I
am not in charge of the encoding process at our
company, but I did ask the people who are before I
came here today what the consequences would be for us
to have to do things in real time. Roughly, it
multiplies the time dedicated about 15 times.

So it's a process that we now do where we
put the CD in, and it's encoded at the bit rate that
we want within a relatively short period of time. If
we had to start doing things, playing the entire CD
through, and then perhaps going through a second
process or a third process in order to arrive at a file, it becomes economically undesirable for us to be able to offer the service that we do, which is the array of channels that we want to offer, the richness of the content that we want to offer, which requires us to have thousands of new tracks added every month to the service.

MR. GREENSTEIN: One other point that I did want to address that Steve made, which is the immediacy of the threat. It's true, at the moment all we know about are that there have been a few commercially-released CDs into stores that have protections applied to them. Some of these are access control. I think, as a matter of fact, all of them pretty much were access control as well as copy-protected. We have started to see within our services advance copies, promotional copies, that have content protection applied to them.

But there is an article that we have seen, and it's dated March 28th. This is on news.com. I can submit this to the Office, if you wish, along with a written statement. I think it would probably be useful for the Office to see.

It indicates that an analyst for J.P. Morgan says that Arista Records, a subsidiary of BMG,
"appeared to be moving to market with CD copy-protection technology. They expect volume shipments of protected CDs to ship commercially in the U.S. as early as in the May-June timeframe," using the SunnComm technology, which is a step beyond what we have previously seen in the marketplace.

MS. PETERS: You just said, "copy protection." Is it access?

MR. GREENSTEIN: Well, it's difficult to know because the SunnComm solution is capable of both. The SunnComm solution, I believe they have multiple "flavors." One of the "flavors" is this second session type of technology.

MS. PETERS: Okay. I actually wasn't going to ask questions. Yes, Steve?

MR. ENGLUND: Several miscellaneous points that people have raised: First, Seth referred a moment ago to advance copies, and I believe he did in his earlier remarks as well. It strikes me that the advance copies are probably the copies that record companies are most interested in protecting with this kind of technology, but the universe of copies that least justifies an exemption in this proceeding because the advance copies are ones that record companies are providing the webcasters. Very often,
they are ones that record companies and webcasters are bargaining over the terms in which they will be provided.

As long as there is that relationship apart from the statutory structure, one of the things they ought to talk about is whether the copies will be copy-protected. It seems to me a webcaster ought to say, "Thank you for all of those CDs you have been giving me, but I can't use them. Please give me CDs I can use." If that takes place, then I submit that some exemption is not necessary.

Second, Seth referred to processes that are workable for home users versus commercial users and suggested that, while it might be fine for a home user to make copies in real time using a regular CD player, that it is not workable for a commercial user. One of the issues that we struggle with in licensing of webcasters all the time is that there is a very small number of large commercial webcasters, the ones represented by DMA. Many of them have or are pursuing relationships with large record companies. Many of them are serviced, at least in part, by record companies already. They have the relationships to deal with the issue.

The question that arises, and the reason
Seth has said that he is here, is for small webcasters who in many cases really are home users because two people are operating a webcast out of the basement. It strikes me that it is very difficult in our licensing purpose to try to identify who is a hobbyist and who is a real webcaster. The folks who are kind of hobbyists/kind of commercial probably would find it a lot more workable to engage in exactly the kind of copying we have talked about, and it seems that they ought to have sufficient access to satisfy all the purposes of this proceeding.

Finally, I am obviously here today out of concern that you will adhere to your previous decision that you cannot define a class of works relative to a use, rather but that it must start with the identification of a class of copyright works. I think you were clearly right that you have to start with a class of copyrighted works.

I kind of assume it's going to be sound recordings, but, as I read the statute, you certainly do have the power to identify a class of users who are affected by a particular type of technological protection measure and a particular non-infringing use they would like to make. If you make such a finding, as I read the statute, it is that use by that class of
users that is privileged.

So I don't think that you ought to put copy-protected CDs or even sound recordings on copy-protected CDs on your list of exemptions. But if you do, I hope you will make clear that not everybody in the world is allowed to circumvent, but only webcasters who are licensed and making and paying for license to ephemerals under 112(e).

MS. PETERS: Thank you.

Charlotte?

MS. DOUGLASS: Yes. Seth, are you happy with the class of works that you have described in terms of Red Book Audio CDs? I'm sorry. Did you hear me? Did you describe the class of works as precisely as you wanted to in the request for an exemption?

MR. GREENSTEIN: Thank you. That's an excellent question.

I think that we described it that way because that was the threat that was known, but I think it's also correct that, in fact, the class could be broader because it could be any type of sound recording, any format that is desired to be used by a webcaster for making the ephemeral recordings.

I mean if, for example, CDs over the next couple of years go away and we move toward super-audio
CD or we move toward a DVD audio or other types of formats, or protected electronic formats, or even a higher-quality second session format, those are formats that webcasters could reasonably wish to use for webcasting purposes and for the making of ephemeral recordings that they need for the purposes of webcasting.

So perhaps you were right, in my effort to be moderate, perhaps I was too modest in defining the class, and that might more properly be defined as a class of sound recordings that are used for making of ephemeral recordings.

MS. DOUGLASS: Is sound recordings the only class?

MR. GREENSTEIN: That is all we are seeking, yes.

MS. DOUGLASS: Okay.

MR. GREENSTEIN: Because that is really what is covered under the statutory license that is at issue.

MS. DOUGLASS: Okay. Are you really concerned or unsatisfied with 112 as it is and, if so, if you could fix it, how would you fix it to more precisely help me understand what it is you want to do that the statute doesn't do for you now?
MR. GREENSTEIN: I think, again, at the risk of concurring with Steve too often, I concur with him that the real solution here is not to have to use 112 ever for this purpose. But, again, we are talking about safety valves, and the safety valve that is there in the exemption for 112 I think is insufficient in a number of ways that I described.

First, because it seems to imply that you have to make the request on a sound-recording-by-sound-recording basis, on a phonorecord-by-phonorecord basis, that becomes unworkable. It becomes extremely expensive and time-consuming.

We would submit that it ought to be that, if the requests have been made and regularly refused, that you can continue to ask from time to time, but you should be able, nevertheless, to just plunge right in and do perform the circumvention, that you need to be on the street the day and date of release with the same sound recordings that your competitors are able to play.

I think that the other aspect of it has to do with quality, that, again, the statutory exemption as written seems to imply that, if you are given a low-quality recording by the record company in response to your request, then you have lost the
ability to circumvent. We submit that that's not sufficient, that we have to maintain the high quality of our services, no matter which sound recordings we are dealing with, and should be able to circumvent for that purpose.

MS. DOUGLASS: So, for you, access control is prevention of being able to access a high enough quality of sound to transmit to your audience?

MR. GREENSTEIN: Right. I would think that you can kind of summarize the concerns in three or four ways: timing, to be able to get prompt access to recordings; quality, the sound quality; the formats that you need. Again, if, for example, you are delivered copies only in particular formats that you use sometimes but not all the time or don't use at all, that creates a problem for you, but the statute would say that you're no longer able to circumvent. Of course, there is the whole issue of the impact on competitiveness and the expense of getting around the access controls by other means.

MS. DOUGLASS: Have you all talked about it among the industries? I know the belt-and-suspenders type of approach you have to make in doing business, but have the two industries talked about it to an extent that you would be happy to -- could you
work it out among yourselves? I think that's the point.

MR. GREENSTEIN: We would like to. I think, again, that is the optimum solution. The problem is that we don't have everybody at the table. The Recording Industry Association and Sound Exchange, while they represent a very large number of companies, I think can't bind them all. This is a problem that exists for any company that applies content protection and for any large number of webcasters and the many that DMA represents and the many that DMA does not represent.

MS. DOUGLASS: This kind of proceeding, since it's every three years, it bears the burden of proof that is substantial, at least by some account. Why would you want to try to obtain an exemption here as opposed to getting a more permanent fix? Even if you get one this time, you would have to do it again. I mean, this is just a personal question.

MR. GREENSTEIN: Uh-hum. I think the permanent fix is the better one. Well, I think, actually, voluntary agreements are best. Second is a permanent fix, and perhaps the first would lead to the second by consensus between the industries.

But failing that, we have to take
advantage of the tools and the opportunities that are available. As you see, hundreds of millions -- more than a hundred million CDs have been protected elsewhere in the world. There are news reports coming out of labels in the United States looking toward copy protection and other kinds of access controls.

We see the train coming. We would like to jump on the train, but we're afraid we're going to get hit by it instead. So I think we have to take advantage of the opportunity that's in front of us now, and that is why we have submitted the request for an exemption.

MS. DOUGLASS: And you have taken this opportunity, standing on the harm that the train is coming, that you've heard that it's been done in Europe? Have any of your members, for example, actually tried to -- have any of your members been harmed by this phenomenon?

MR. GREENSTEIN: We have encountered them. Our members have told us that they have tried to rip discs and met with copy protection and met with access controls.

They said that, up until now, the methods that have been applied have been reasonably ineffective. So trying repeatedly or trying a couple
of things that I don't think anybody would consider to be circumvention per se, they have been able to get access to the material and to make the copies that they needed.

But the methods are getting more sophisticated. I think we are not going to see much longer the circumvention by taking a felt-tip pen and writing on a particular area of the disc. When we start to encounter these types of access controls, it is going to be a lot more difficult for us, and the impact of it can be much more substantial and severe.

MS. DOUGLASS: I think that's it. Thank you.

MS. PETERS: Steve?

MR. TEPP: Thank you.

Let me start with you, Mr. Englund. The TPMs we're talking about that will not allow a CD to be played back in a computer, is that the purpose of the TPMs or is that an incidental effect of the copy control?

MR. ENGLUND: Certainly, the fundamental purpose of copy protecting CDs is to protect the CDs from copying. Record companies are highly motivated to let people enjoy music on any platform they can choose.
It has been the difficulty of the technological challenge here in securing the CD format against modern ripping technology that has kind of led people in the direction of the second session technology and other approaches that we have talked about this afternoon.

It may not be completely clear whether that is, in fact, an access control since ultimately it allows access on both platforms, but it is certainly not -- it is, as you described it, more of a byproduct of how you prevent copying than of a desire to prevent access on a particular platform because record companies want people to be able to access and enjoy music.

MR. TEPP: Given that, by definition, we're talking about application TPMs prospectively, because I think everyone agrees that to date it's been a very limited application, to what extent is the recording industry looking to continue or not continue that incidental effect of the copy controls that it does apply and may apply in the future?

MR. ENGLUND: I think many record companies are interested in principle in copy protecting CDs. They are not the primary innovators of the technology here. There are a number of copy
control companies that are the technology innovators. They are testing the various technologies that are available.

They are thinking about, though, these technologies are effective and cost-effective and likely to result in more money at the bottom line rather than less, and they will make decisions based on that factor; they will make those decisions independently. It is possible that some record companies will deploy some forms of copy protection on some CDs and others won't.

Does that answer the question?

MR. TEPP: I think so. Let me toss something out for the whole Panel.

To what extent -- and this is a technical question, so I apologize asking it to three lawyers -- to what extent, to the best of your knowledge, is it possible to circumvent the copy control but not the access control aspects of the TPMs we're talking about?

MR. GREENSTEIN: Well, I'll take a whack at it.

(Laughter.)

It is the blind leading the blind here.

I think one thing I would mention first is
that one of the technological protection measures that
seems to be in the offing is something that does play
in the computer, but it permits access only to the
lower-quality second session. So the access control
that is being applied there is really an access
control with respect to the higher-quality format,
which is what webcasters would need in order to
perform webcasting.

I guess as to the technological question
you have asked, I think none of us knows the answer
because none of us really has seen the technology
that's going to be used. I mean we know that there is
a Macrovision technology out there that they acquired
largely from their own efforts, plus Midbar and
Cactus. That is the one that has been rather easily
circumvented in Europe and Australia and elsewhere.

But as far as the SunnComm solutions, they
really have not hit the market yet. So we don't know
exactly what the impact is going to be.

MR. ENGLUND: I basically agree that so
far the copy-protection aspects of copy-protected CDs
have been somewhat easy to circumvent. For the
reasons I described earlier, I think they may always
be easy to circumvent, because if the music can be
rendered in a CD player, it can probably be copied.
It is a difficult technological challenge to copy protect CDs. A lot of companies are working hard to do it. Record companies are very interested in their efforts, but it really by no means is clear as a technological matter, from what I hear from the technologists at the record companies, that technology vendors will ultimately succeed in securing the CD format to a very high degree. We hope they will. If they do, we will be interested in deploying it, but today it's not clear that they will succeed.

MR. GREENSTEIN: I think there is a perception, even on behalf of the vendors of the copy protection, that the consumer in markets outside the United States is somewhat more docile and more accepting of limitations than the United States consumer may be. So it is difficult to predict even what the reaction will be from the U.S. consumer to these technologies and how long they will persist.

We have to look out at the moment, assuming that the threat is going to be as real as it could be, that the statements of record companies that they have made on their websites, for example, in the UK and elsewhere, that they intend to move toward universal application of these technologies mean that they are going to be applied in the United States as
well. If so, the means may not be known, but the impact I think ultimately is going to be very predictable, at least for webcasters and their ability to make the ephemeral recordings that we need.

MR. TEPP: Okay, thank you. Let me turn now to Mr. Greenstein and Mr. Leavens for a question about sort of the business side of it, of webcasting. You indicated that there are some, although it sounded like a small minority, but some webcasters who do use CD players rather than computers to generate the ephemeral copies that are the subject of the requested exception. Why is it that they are satisfied with that and others are not? What's the distinction there?

MR. GREENSTEIN: Actually, to clarify, I think I was the one who mentioned that. It was not that they used them to make the ephemeral recordings, but, rather, that they used them for webcasting, similar to the way that you used to have turntables in a radio studio, radio broadcast studio, or you currently have professional CD audio players in these studios, in broadcast studies for radio, that is essentially what some webcasters do, particularly non-commercial webcasters, educational institutions, and such. But I don't know of any larger-scale webcaster
that works off of CDs directly.

MR. LEAVENS: We don't. For purposes of trying to manage and track the number of tracks that we have, we have in place software which ensures that the broadcast is DMCA-compliant. We actually have real people who program each of the radio stations in the sense of selecting the songs that are going to be there, determining the relative importance of the songs and how frequently they're going to be played, and that.

But this is a service that depends upon the able body of a computer to serve it up, to select, to track, to make sure that we're going to be paying the royalties correctly that we need to under the DMCA. It's not a circumstance where we could have somebody sitting at a player and taking out a CD and putting it in and in some way trying to -- I suppose they could be playing it off of a track list that is computer-generated, but they would then have to be somehow inputting information as to what they're playing and how long it is. It just isn't going to work for the scale in which we are working.

MR. TEPP: It's operational logistics, then, is what you're saying?

MR. LEAVENS: That's right, and to be
competitive with who we view as our competitors, we can't operate that way.

Mr. Englund: Just to be clear, I have never suggested that webcasters need to play CDs on CD players in real time as they are transmitting, but it is entirely possible to use CD players to access access-protected CDs, to the extent that's necessary to make ephemeral copies once, but would thereafter be used on a repeated basis and organized with the kind of scheduling software that Tom was talking about.

Mr. Tepp: Well, clearly, Section 112 envisions the creation of ephemeral copies. So let me turn to that for a moment.

A comment made by DMA talks about the -- and we've already talked about it today -- the exception to 1201(a)(1) in 112(a), but the absence of a corresponding provision in 112(e). I guess there are two ways to look at that.

The way that you have painted it is let's correct this omission, but I'm interested in your response potentially to the opposite interpretation, that if Congress chose to put it in 112(a) but chose to omit it from 112(e), does that reflect a congressional intent that there not be an exception to 1201(a)(1) for the purposes of 112(e)?
MR. GREENSTEIN: I'm speaking in stereo with both microphones.

(Laughter.)

In fact, I think that actually in the comment is an error because 112(e)(8) does provide an equivalent exemption.

MR. TEPP: Of course, we have it all memorized.

MR. GREENSTEIN: That's right.

(Laughter.)

The "bible" has come out now.

MS. PETERS: Speak for yourself.

MR. GREENSTEIN: I would say that statement is an error in the written comment.

MR. TEPP: Okay.

MR. CARSON: The only one, no doubt?

MR. GREENSTEIN: Ever.

(Laughter.)

MR. ENGLUND: Seth, is the request, then, to broaden the scope of (e)(8)?

MR. GREENSTEIN: No, actually, it's for an exemption of 1201(a)(1).

(Laughter.)

MR. ENGLUND: Effectively, to broaden (e)(8)?
MR. GREENSTEIN: To correct certain operational deficiencies, in light of the oncoming train. It's not to broaden (e)(8) specifically or to broaden 1201(a)(2). The issue really is that there are certain situations in which this exemption will not be workable and will continue to work substantial adverse effects on webcasters' ability to make ephemeral recordings.

MR. TEPP: That has to do with the need to request permission?

MR. GREENSTEIN: Again, it's timing, quality, format.

MR. TEPP: Okay.

MR. GREENSTEIN: And expense.

MR. TEPP: Okay, well, that leads me well into another question I had. The statute that lays out the standards for this rulemaking speaks of non-infringing uses of works. It does not speak of particular formats of works or certain devices to render classes of work.

So what is your best pitch as to why issues like format and devices, and the four principles you've laid forth, fit within the criteria of the rulemaking?

MR. GREENSTEIN: I think these are all
part of the non-infringing use that's contemplated under the ephemeral recordings exemption and license; that the reason for ephemeral recording exemption, and particularly the multiple ephemeral recording license, was specifically because of the need recognized by Congress for webcasters to have files available to them in multiple formats, multiple bit rates, multiple codecs, and for multiple servers.

So that is a use that was clearly contemplated by Congress. That is statutorily the license and, therefore, by definition, not infringing. So I think, specifically, this is the type of non-infringing use that is cognizable under a 1201(a)(1) exemption.

MR. TEPP: Well, a minute ago you were talking about the 112(e)(8) and how what you're asking for here is an exception under 1201.

MR. GREENSTEIN: Yes.

MR. TEPP: Presumably, the 112(e)(8) is meant to deal with the various factors which went into the enactment of 112(e). What you are asking for is somehow broader than that, and it has to be considered by this Panel and the Library in the context of the standards in 1201.

So can I ask you, with reference to 1201,
to talk about the concerns you have raised and how they qualify within the standard we are constricted by?

MR. GREENSTEIN: Well, I think the standard is whether there is likely to be a substantial adverse impact with respect to non-infringing uses; that is, being impeded by the technological protection measure with respect to access control.

With respect to the likelihood, again, the CDs marketplace, they're starting to show up on our doorstep where there are copies that are for promotional use only being delivered to webcasters. What are the promotional uses? The promotional use is not just to listen to it for your own personal enjoyment. It's to be able to actually use them in your webcasting activity. These protected CDs are unusable by us.

Again, we have seen the news articles. That is really all we can rely on at this point. We can rely on news articles that describe the intention of the various labels to start engaging in widespread content protection in the United States in the coming months; projections and information from analysts, reliable analysts from J.P. Morgan talking about this;
the content-protection companies themselves like Macrovision and SunnComm, Macrovision, in particular, talking about how hundreds of millions of these discs have been protected and are available elsewhere in the world.

This is, you know, likely to happen in the United States if the news reports are true and if the experiences of consumers are not so overwhelmingly negative that it forces record companies to back off on their plans.

The substantial nature of the impact, I think I have tried to describe at length how it would have a very severe impact on competitiveness of services that are by nature entrepreneurial businesses in a brand-new marketplace trying to establish a new medium. We have several strikes against us already, and we are trying to develop the means to compete.

One of the ways that we compete is on timing and sound quality. Those are two of the ways that we compete. To the extent that we are unable to compete in that way, we are disadvantaged with respect to radio, disadvantaged with respect to those entities that have prompt access and high quality, which include perhaps some of the larger webcast competitors, but also include the record companies.
themselves, which are engaging in various webcasting activities, either on their own or through joint ventures that they have entered into.

So the impact is substantial. Clearly, it's a non-infringing use, and the impact is created by the presence of a technological measure that controls access.

Again, maybe I can ask this to Steve, so he can help me puzzle through this. Because the statute refers to the fact that you would not be liable under Section 1201(a)(1) for making an ephemeral recording. Why would Congress have needed to say that if it didn't view this kind of activity as being potentially liable under 1201(a)(1), which is with respect to technological measures for access controls? If this is purely copy control, why would Congress have needed to say this at all, since there is no provision with respect to the circumvention of copy controls under 1201(b)?

MR. ENGLUND: I have wondered the same thing myself and concluded that it is perhaps not the only thing in the statute that is simply not necessary.

(Laughter.)

But, as we have talked about earlier this
afternoon, there may well be particular implementations of particular technologies on some CD products that are technically access controls.

Thank you for pointing out 112(e)(8). I shouldn't have taken Jon at his word that there is an omission.

(Laughter.)

Once you consider that there is 112(e)(8), it seems like your mantra of time and quality, formats, and competitiveness becomes simply timing. With respect to timing, Congress has provided a mechanism whereby webcasters can ask for copies, and if they don't receive them, they can circumvent. Circumvent is ultimately what you're asking for here. So you're saying that a reasonable time is, in fact, unreasonable because it impacts your competitiveness, but that is the injury you suffer.

With respect to quality, formats, and competitiveness, Congress has given you permission to circumvent, maybe not on the time table you would like, but, nonetheless, it has given you permission to do the circumvention that you're trying to be able to do in this proceeding.

So that your issues of quality, formats, and competitiveness are already addressed in the
statute to the same extent they could be addressed in this proceeding. Therefore, the mantra becomes simply timing. And the question is whether rewriting the provisions of 112(e)(8) to take out the timing requirements that Congress put in is a substantial adverse impact, but it's not.

MR. GREENSTEIN: I think it certainly is not just about timing, because, as I mentioned, if in fact I were to go to a record label and ask for a copy in order to make the ephemeral recordings for its server, and it was given, let's say, the 32-bit copy that Tom can use on the Music Now service with respect to the lower-bit-rate transmissions, but would do him no good with respect to the higher-bit-rate transmissions such as people who have cable modems or DSL at home, then the way the statute is written, it would appear that the webcaster is simply out of luck. They have gotten a phonorecord from the copyright owner, and there is nothing more to do about it.

I think the underlying presumption, I think, that everyone had when we were discussing the DMCA back in those halcyon days of 1998 was that we were dealing with phonorecords that were the types that we all knew about. They were the CD. They were the CD quality, all of equal quality, and that's
really what we were facing.

I think, since then, the market reality has proven otherwise, where, for example, the second session that we're talking about is something that is of substantially lower quality.

MR. ENGLUND: I think it's just speculation what kinds of copy a record company might provide if a webcaster asked for it. It seems to me it's as likely that they will provide an unprotected CD as that they would provide something bad, because record companies certainly care about quality. Record companies don't want their music to be perceived as sounding bad.

It's simply speculation, and the Office has rightfully found that speculation is not substantial adverse impact, particularly when it ought to be proceeding cautiously, given that Congress has provided a specific exemption.

MR. TEPP: Well, let me ask you something along those lines, Mr. Greenstein and Mr. Leavens. Has your industry used 112(e)(8) and been told the second session copy is all you are getting or has it been used at all? What is your experience with that?

MR. LEAVENS: Full Audio really has had limited experience in the whole webcasting area. So,
unfortunately, I can't say that we have encountered the circumstance where we have requested something and been denied.

We have encountered the circumstance where we have a promotional CD, which we simply tried out because it's an Arista CD and we wanted to find out whether in fact what we had been reading about was true, and it was true; we weren't able to encode it in any way. It's not been released commercially, I guess. So it's not something which we can put into the service. I don't know, when it is released, whether it's going to be copy-protected at that time, but the experience that we have encountered has been relatively little, I guess.

So we're going on the basis of what we understand to be the practice which is coming toward us, all the reports that we see, and, frankly, from the perspective of us, it makes a lot of sense to have copy protection in the marketplace in order to ensure that kind of legitimate delivery of content.

So we're not disfavoring it in any kind of way. We favor it because, as I said, we are very much involved with DRM ourselves as a company. We rely upon DRM in order to deliver secure files, which enforce the rules that we have with respect to our
So we are not inconsistent in any kind of way. It's simply that we see that there is this development which we don't know it's not going to happen. I know that perhaps could be characterized as speculation, but it does seem very inevitable, certainly within these three years, that we are going to be encountering this.

MR. GREENSTEIN: From the other webcasters that I've spoken to, they have encountered copy-protected discs, but they have not been of the second session variety yet. So they have not really had the opportunity to see whether 112(e)(8) works or not. At the moment, their experience has been simply that whatever discs they have encountered, they have been able to overcome with something that I think nobody would characterize as circumvention.

MR. ENGLUND: And nobody I've talked to in the recording industry is aware of anybody ever having asked under 112(a)(2) or (e)(8).

MR. GREENSTEIN: There's a certain chicken-and-egg aspect to this, I admit, but the problem is that we read the news reports, we see what's happening abroad, and we know that protection mechanisms are getting more and more powerful and are
potentially coming to market in the United States.
Again, if this J.P. Morgan analyst is correct, then
it's going to happen as soon as May to June with
respect to a major record label. That's the major
record label that has the copy-protected disc or the
protected disc that Full Audio's service has seen on
the promotional basis only.

So we can see the reports saying that this
is going to happen. It has not happened yet. But now
is the time that we have to come to you to make our
pitch, and so here we are.

MR. TEPP: Okay, I just have a couple more
questions. Let me go to you, Mr. Englund.

Mr. Greenstein has just repeated the
concerns based on this analyst's prediction about
upcoming use, an increase in use, of TMPs on CDs by
recording labels. Let me ask you, if it comes to pass
that the recording industry does apply TMPs more than
it has in the past -- I guess it is a two-part
question -- why hasn't it been done to date very much,
and why might it be done more in the future?

MR. ENGLUND: As I have said before,
record companies, in principle, are very interested in
protecting CDs from copying, but how you do that and
whether you do that, when you do it, are complicated
business decisions that involve a lot of factors that need to be balanced.

One is the effectiveness of the technology, and another is the cost of the technology, since these technologies do come at some cost, both internal and out-of-pocket.

Another is the potential for consumer resistance. While my impression is that there has not been a lot of consumer resistance outside the United States, there have certainly been some vocal opponents in the United States, so that one has to have some pause about that.

Ultimately, record companies need to make a decision about whether the investment in copy-protection technology and the potential for consumer backlash is justified by the potential for reducing copying. Thus far, the available technologies have merely provided a speed bump to copying, what some people characterize as keeping honest people honest.

The cost/benefit decision that people have made so far has been that it is not clearly warranted. If the technology got better, maybe it would be more clearly warranted. With more experience, maybe it would be warranted.

It is just premature to try to predict
what the problem is, and there is no need for you to try to predict whether there is a problem here because webcasters have access. Webcasters have access by copying from CDs. Webcasters have access under an explicit statutory exemption that they would like to broaden so as to have faster access perhaps, but that is really all we are talking about here, is merely a matter of timing.

MR. TEPP: Okay, let me ask my last question then of Mr. Leavens and Mr. Greenstein. Mr. Leavens, you just spoke a moment ago about recognizing the importance of DRM in your own industry, and, similarly, on the part of the record labels. So my question is, to what extent do you think that there is a legitimate countervailing argument to the proposed exception that there are genuine anti-piracy concerns that make an exception for sound recordings potentially a dangerous one?

MR. GREENSTEIN: I guess let me speak first, if you don't mind, which is I think, given the nature of what we are asking, it really poses no danger to the sound recording copyright owner at all. All we are asking is that legitimate businesses that webcast music should be able to do that on a competitive basis that is equal to other similar
services, be it radio broadcasting or webcasters that may have better relationships or more direct relationships with record companies.

There is really no threat whatsoever. Again, we are not asking for a generalized exemption or prohibition on application of access-control protection or content protection to all compact discs or all sound recordings. We are seeking the ability to circumvent in a limited class of users for a specific type of works, solely to promote lawful activity. So I cannot see how that is going to have any negative impact on the record industry generally.

We have other requests that are being made for circumvention with respect to compact discs, technological protection measures. Each of those should be judged on its own merit. This one, I think, is a narrow and particularly meritorious case.

MR. ENGLUND: This time I have to disagree with Seth. First, even if it is possible for you to create some exemption, coupled with an identified class of users and a use that is limited so as to extend the benefit of the exemption only to webcasters and only to webcasters licensed to ephemeral copies, I think that the webcasters' interest in getting their copies faster than the express statutory provisions
provide doesn't justify that exemption.

But, more importantly, there is a large risk here for sound recording copyright owners. That is the risk that other people in the larger universe, including courts, should a record company ever try to enforce the provisions of 1201, will interpret 1201 so as to find that the inclusion of copy-protected CDs on your list of exemptions allows everybody to circumvent. I think that that is a risk, given your finding three years ago.

Even though I think that you probably do have the power to limit an exemption to a particular class of users, uses or users, I certainly can't rule out the possibility -- in fact, I'm very concerned -- that a court might say, "Copy-protected CDs are on the list. Therefore, they can be circumvented."

Quite apart from the strict legal issue, I think that, even if you conclude, and you rightly conclude, that you can limit an exemption to webcasters and to ephemerals, that our experience with enforcement litigation suggests that the issue will have to be dealt in every case at great expense and great loss of time.

I can only think about Section 1008 of the Copyright Act, the limitation on actions under the
Audio Home Recording Act. The Office has found, everybody has found who has ever considered the issue, that the Audio Home Recording Act does privilege peer-to-peer file-trading networks, but the issue comes up. Every litigation has to be fought back at considerable cost.

MR. GREENSTEIN: And you win each and every time.

(Laughter.)

MR. ENGLUND: So the question is whether Arista Record Companies ought to have their legitimate efforts to bring enforcement actions hampered and delayed, sometimes by months. In the Napster case the action was delayed for a long time while AHRA issues were considered. To suffer that kind of harm while this issue is fought -- that was fought over and over again. I think that's something that the Office has to take into account in deciding whether the webcasters' desire for accelerated timing is a substantial adverse impact.

MR. LEAVENS: Full Audio has been the beneficiary of some of the litigation that the RIAA has fought. So we certainly are not advocates for hobbling them, but when you consider the kind of defense that somebody would impose here, they would
have to establish that they are a webcaster, that they have filed their notice with the Copyright Office, that they have facilities.

It is not an easy thing to do. You can't justify it on the basis of, "Whoops, I was a webcaster" or "I intended to be a webcaster." It is like defending a fair use on the basis of a review you have not ever even written yet.

So I think that the risk of, on a practical level, of creating some kind of greater burden with respect to litigation or enhancing piracy I think is pretty remote.

MR. ENGLUND: I think I have to disagree. If the Copyright Office says that sound recordings released on copy-protected CDs are an exempt class of works, I think everybody who is ever accused of circumventing access controls on them will say sound recordings are an exempt class of works. End of story.

MR. LEAVENS: Well, I suppose if that were something that we were asking, but we're only asking for purposes of being able to do an ephemeral copy for exercising our rights under the compulsory licensing provisions of the DMCA. It's very narrow, and that's a very high standard for somebody who's a simple
hacker to try to meet.

MR. GREENSTEIN: And just to emphasize a point that I think the Panel understands, but Steve seems to miss somehow, this is not just a question about timing. This is a question about timing, quality, format --

MS. PETERS: That we got.

(Laughter.)

MR. GREENSTEIN: Yes, I knew that you did. I just wanted to make sure that perhaps, having seen that you get it, Steve might also get it on the rebound.

(Laughter.)

MR. ENGLUND: I'm just being dense this afternoon.

(Laughter.)

MS. PETERS: I have consulted with my two staff members who haven't yet spoken. They tell me they have a number of questions, especially the gentleman on my left.

So I'm going to suggest that we take like a five-minute break, so that people can use facilities, so they can endure the rest of the afternoon.

(Laughter.)
Okay?

(Whereupon, the foregoing matter went off the record at 3:23 p.m. and went back on the record at 3:32 p.m.)

MS. PETERS: Our witnesses are back, the Commissioners are here, so let's go.

Rob?

MR. KASUNIC: Okay. I just have a few questions, mostly -- well, let me begin with Seth. Based on the current situation -- and let me just see if I have this straight -- that there's no actual harm in the marketplace now related to access controls on Red Book CDs or any other kind of music that you were talking about needing exemption for, right? Is that right?

MR. GREENSTEIN: We have actually encountered protected discs. Thus far, the means that have been used have been completely ineffective. Therefore --

MR. KASUNIC: Copy-protected discs, though, right?

MR. GREENSTEIN: No, access as well. I mean, for example, some of the protection systems that have been used in the past don't work on Macintosh computers at all. As a matter of fact, they would
then prevent you from reopening the drawer of your CD-ROM in your Macintosh. I actually talked to a couple of people who have had to take their Macintosh drives back to an Apple retailer to try to get it fixed because they couldn't get the CD out once it was in.

So there are those kinds of unique access controls that have been applied, but so far, at least for the webcasting community, who thrive, I guess, on Windows and other operating system environments, we have not been prevented from getting access by the control measures that have currently been applied.

MR. KASUNIC: Well, I guess just an aside then. Let me ask Steve: These measures that were precluding use on an Apple computer were not planned by the recording industry to operate as an access control in that way, to destroy Apple computers, were they?

(Laughter.)

MR. GREENSTEIN: It's part of a Microsoft conspiracy.

(Laughter.)

MR. ENGLUND: The answer must be no.

(Laughter.)

I am not sure what particular products,
what particular technologies were at issue here, but
it is certainly the case that no record company
intentionally locked up anybody's Apple CD-ROM drive.

MR. KASUNIC: So there were some
unintended access problems on limited devices that
have come into the market? Is there any reason to
believe that those will not be fixed in the
marketplace?

MR. GREENSTEIN: Again, some of the more
intended -- maybe not that one, in particular -- some
of the technologies that were applied were intended to
prevent playback on personal computing devices. So,
from that perspective, they were intentionally access
control to prevent playback as well as to prevent
copying. I guess if you prevent playback, you have by
nature prevented copying on a personal computer.

MR. KASUNIC: Okay, then in terms of that
actual harm, how substantial was it?

MR. GREENSTEIN: At the moment, as I said,
the substantiality is not with respect to what has
happened in the past. The fear is the oncoming train.

MR. KASUNIC: So it is di minimis at
present in the actual market?

MR. ENGLUND: I think he's told you it's
well nigh non-existent.
MR. GREENSTEIN: I think that would be correct.

MR. KASUNIC: Okay. Then what we're focusing on is likely harm, right?

MR. GREENSTEIN: That's correct.

MR. KASUNIC: And in order to, as we have defined likeliness in the typical sense, that it is more likely than not, what evidence is there that this is going to be more likely than not, that you will not be able to negotiate in the future, that the recording industry will refuse, that the marketplace will not take care of it, any of those other possibilities will fail to happen, and that that is more likely and that you will be denied access, that that is the likelihood?

MR. GREENSTEIN: There are several parts to the question. Let me see if I can take them one by one.

First is the likelihood that content protection is going to be applied. I think, given the experience in Europe, given the fact that we are now starting to see these discs coming in on promotional discs, these protection measures being applied to promotional discs, given what we have heard from analysts and various news reports, it's likely that
this is going to happen and going to happen in the near term.

That is what we are starting to see now, and we can see the risk. Particularly as CD sales continue to decline in the world market, for various reasons, it is likely that content protection is going to be applied. So that threat is real.

The impact, we believe, is substantial because, first of all, I guess the impact is substantial because we can say for a certainty that not every webcaster is going to be able to "one on one" with every record company. Even the largest webcasters are going to have some difficulties getting in touch with independents.

MR. KASUNIC: But that is taking another step in this. We haven't even gotten there yet. First, we have to find likelihood before we can see whether we get to the point of this being substantial.

MR. GREENSTEIN: All right, I guess I was getting to the point of the likelihood of the negotiations issues. The reason that there is statutory license, or one of the reasons that there is a statutory license, had to do with the administrative difficulty of negotiating one on one between all of the webcasters and all of the record labels.
There are thousands of webcasters and thousands of record labels. Administratively, it was impossible to say that they could predictably deal with them one on one to get the licensed content that they needed.

The same administrative difficulties are going to happen here. So the impact from that perspective, is it likely that there are going to be webcasters who are going to be disadvantaged in this way? Absolutely. Is it going to happen to everybody in the same way? I would say absolutely not.

I think it is extremely likely that somebody like a Yahoo or Real Networks or an America Online will have a much easier time dealing with the issue than will even Full Audio or webcasters that are smaller in size. But, yet, the statutory license guarantees them all equal access and equal rights.

MR. KASUNIC: When is it likely, and more likely than not? How do we know that it is going to take place? Maybe, then, at some point it is likely that copy protection or some form of access protection will be employed. What evidence is there that it is going to be employed in the next three-year period and that these problems will occur?

MR. GREENSTEIN: The evidence that we have
is the experience in Europe, the content-protected CDs that we’re starting to see coming in through the door as promotional CDs, the few CDs we have seen as experiments that have come in the door in the past using less-effective protection mechanisms, user ports, that license agreements have been signed with companies such as SunnComm that do have more effective protection mechanisms.

We have pronouncements on the websites of various record companies, particularly BMG and EMI, with respect to their intentions to apply content protection more widely to all of their CDs as possible. If this is going to happen, it is going to happen in the next three years.

We are also, we hope, moving from a purely CD-centric environment to other kinds of distribution means as well, such as DVD audio and super-audio CD and we hope greater online distribution with DRMs.

With respect to the CD copy protection -- and DVD audio is already protected, I suppose -- if this is going to happen, it's going to happen within the next three years or it will likely not happen at all.

MR. KASUNIC: Well, then, in terms of what our requirements are of having them, more likely than
not, we can look to circumstantial evidence, and the only thing that I really heard in terms of that was the deployment and licensing articles. Are those the basis, the circumstantial basis, for the likelihood, aside from your --

MR. LEAVENS: Well, I think Seth had mentioned the statements of the record companies themselves of their intention that appears on the websites.

MR. GREENSTEIN: The statements, in particular, I think are more on the websites of record companies with respect to their non-U.S. operations. So, for example, I would be happen to provide to the Office -- there's a statement from the BMG website about what their intentions are, about the importance of copy protection for CD audio.

MR. KASUNIC: In the non-U.S. market?

MR. GREENSTEIN: In the non-U.S. market, that is where the statements have been made. That's correct. The U.S. market is the largest market for compact discs, however, and to say that you're experimenting in a smaller market I think is not necessarily a guarantee that it's going to only stay in the smaller market, particularly because we have seen limited experiments happening here in the U.S.,
when you have limited experiments happening first in Europe, in Australia, in Japan, and then announced intentions to go to a more widespread protection mechanism there.

The fact that we have seen experiments here in the United States indicates that there's a substantial likelihood that the protections will become in the United States, once those experiments are through.

MR. KASUNIC: Steve, do you have --

MR. ENGLUND: I certainly agree with your line of questioning.

MR. KASUNIC: Right.

MR. ENGLUND: Seth has admitted that there is essentially no harm presently. Where there is an assertion of a likelihood of future harm, the proponent is required to show by highly-specific, strong, and persuasive evidence that the harm is more likely than not. Where proponent is seeking to rewrite an existing statutory exemption, you should proceed with particular caution.

So this proposal is positioned within the framework of this rulemaking in the position that has the absolute highest bar to be overcome. They are required to prove a lot of harm with a great deal of
likelihood, and better evidence than I have seen in
the last couple of minutes.

And, still, you should proceed cautiously. I think within that context you should deny the
proposed exemption.

MR. KASUNIC: Well, based on what Seth had
just said about the experience in Europe dealing with
the use of these controls in Europe, how does that fit
into -- does that support a circumstantial case of the
use in this country?

MR. ENGLUND: No. It is very clear that
there have been experiments, both abroad and in the
United States, with copy-control technology. If there
were effective, cheap, well-accepted copy-control
technology, the threat of universal access, there
would be a lot of interest in deploying it, but it is
a very open question today whether it will ultimately
be deployed to a significant degree in the United
States.

MR. KASUNIC: Has the recording industry
made any statements that you're aware of that they
would be unwilling to work with webcasters in terms of
necessary uses in the future, should there be problems
with certain kinds of copy protection?

MR. ENGLUND: I'm certainly aware of no
such statements.

MR. KASUNIC: Are you, Seth?

MR. GREENSTEIN: I'm not aware of any such statements. Again, we came to you hoping that we could work this out in the marketplace, but, yet, this proceeding exists as a safety valve, and that's the valve that we're looking for.

MR. ENGLUND: Yes, they say they want to work it out in the marketplace, but this sure came as a surprise to us, and they have never asked us in the marketplace to work it out, rather than perhaps it has been dealt with among the individual companies. Certainly servicing is something that is routinely dealt with among individual companies, quite apart from the statutory structure. But DMA never approached RIAA and said, "We really need to be working on legislation to rewrite 112(e)(8)."

MR. KASUNIC: Well, let me turn a question to Tom about, in terms of the automation issue, how will this -- I think a point that Steve made -- how will this be a panacea? If this exemption were to be put in place, how would this help? How would this automate the process?

MR. LEAVENS: Well, it removes the preliminaries to the process, first of all. It allows
us to self-execute without having to go through all
the notice and the waiting, and that.

    I'm not sure exactly how it is that it is
going to enhance our ability, frankly, to automate.
I just know that we need to keep our system operating
as an automated process as much as we can. One of the
things that I had overlooked in mentioning about the
need to rip the CD, as opposed to doing something real
time, is simply the way in which you obtain meta-data
at that particular point, as opposed to having to
enter that on some kind of manual basis.

    So, in terms of what we have to do in any
kind of manual process or real-time process that
involves having to simply play the CD, we are not able
to integrate the meta-data in the same kind of way,
which additionally adds to our time.

    I guess what we are foreseeing is the hope
that there is going to be a solution that would allow
us to have some kind of a circumvention that we can
build into our system that's going to be recognized
when the CD is put into the system, and kick in
automatically without it being kicked out and us
having to pay particular attention to it. I'm not a
technology person, so I don't know how all that would
happen.
MR. KASUNIC: Wouldn't this put webcasters in more competition, in more competitive disadvantages, because some webcasters would be able to circumvent and others wouldn't? Actually, this wouldn't level the playing field, but it would be based on what an individual webcaster was capable of doing?

MR. LEAVENS: It is really something that we view as being for those circumstances where we can't make agreements with people, where we can't reach accommodations.

You ask about, has there been something that has been determined industrywide? We would love that, but, as Seth mentioned, we can't get everybody to the table. We can't control the activity; RIAA can't control the activity of all of its members. Not all record companies are members of the RIAA.

So what we are looking for is something that essentially gives us the ability to work under the circumstances where we can't work out something on a consensual basis. It's akin to, I guess again, the mechanically license that record companies have for musical compositions.

The number of times in our record company that we exercised that right was very little, but when
we needed it, when we were in circumstances where we
had somebody that wasn't going to give a consensual
license, we had the ability to get the license anyway.

So I'm really thinking about this in terms
of not the labels that are going to be responsible,
who are going to have the resources, who are going to
have the inclination to work with us and work with
other webcasters. I'm thinking about the others who
may not have the inclination, may not have the
resources, may not be found.

MR. KASUNIC: If this is -- I guess to
Seth -- if this is a likely problem during the next
three-year period, how would this not be a likely
problem into the future beyond that three-year period?
Isn't this just a general problem that would be more
appropriately addressed by Congress?

MR. GREENSTEIN: It might be a problem
that occurs. Well, let me take it point by point.

I think, if it occurs in the next three
years, and I think it is likely to happen --
otherwise, we wouldn't be here in front of you --
then, yes, it is likely to be a problem that persists
into the future. It is a problem that I would hope,
once it becomes identified, finds another solution
because I think the safety valve is always, and should
be, the last resort.

There should be other ways to deal with this. It should be something that could be dealt with either by voluntary agreements or by Congress. I mean, certainly, if you're looking for the panacea, the panacea is to require, as a condition of the statutory license, that everybody who pays an ephemeral gets service by the record company of an uncopy-protected compact disc with the highest audio quality. That's not likely to happen.

So we can't look just to the panaceas. We have to look to the realities of what is second best and what is the absolute minimum that we would need. The absolute minimum is that, if all else fails, we need to have the ability to circumvent in a rapid timeframe, not on a sound-recording-by-sound-recording basis, but where it has been shown to you that you are either not going to get the sound recording from the record company on a timely basis or you are going to get it in a quality that is not sufficient for your needs, you have the ability to exercise self-help.

So, from that perspective, that is really what the request is about. Is it likely that this would be a request that would have to be renewed in three years? I think the answer is probably yes,
because a safety valve would be needed then as well, although, again, I would hope that the majority of the problem would be accommodated in other ways through marketplace discussions.

MR. KASUNIC: I know David has a lot of questions. So I have just one more, and this is to Steve in terms of a comment you made about the scope of the exemption, should we choose to find an exemption here, and that it could be narrowed to the particular scope of use.

Do you believe that we should, within the exemption itself, actually, or that we have the authority to fashion an exemption that would include a particular use?

MR. ENGLUND: No, I don't think that you ought to create an exemption, but I think the relevant statutory provision is 1201(a)(1)(D), at the bottom of page 179, carrying over to 180, in your purple books here, which says that, "The Librarian shall publish a class of copyrighted works...that non-infringing uses by persons who are users of the copyrighted work are or are likely to be adversely affected."

And the key phrase is the last one: "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."

I think that it may well be a sufficient basis for you to identify webcasters as a class of users that is likely to be affected and to privilege only the activity of webcasters that has been identified.

MR. GREENSTEIN: Once again, I'm forced to agree with Mr. Englund.

(Laughter.)

MS. PETERS: David?

MR. CARSON: All right, I would like to go back to the first question asked by Charlotte a few days ago.

(Laughter.)

Seth, this will actually follow up on that, because I think you agreed with Charlotte that in the comment you filed all you identified as a class itself was copy-protected Red Book Audio Format compact discs, correct?

MR. GREENSTEIN: That's correct.

MR. CARSON: Let me take it a step further. Maybe I missed it, but when I read the entire comment, I think the entire comment was about copy protection and not about access controls. Am I right or did I miss in the written comment about
access controls?

MR. GREENSTEIN: Perhaps it was spoken as the scope of the discs themselves, and the sound recording formats is perhaps too narrow. Perhaps it was too narrow in reference to copy protection alone.

There are other access controls that are being applied that would also have the effect of preventing playback on computers or other types of access by computers and, therefore, prevent ultimately the making of the ephemeral recordings.

I guess what was meant by the focus on copy protection was really twofold. First, that that is really the ultimate problem that we are seeking to address, the ability to make the ephemeral recordings. So any technological protection measure that interferes with the ability to make those ephemeral recordings is really what is at issue in our comment ultimately.

Second, it is because of the reference to 1201(a)(1) in the two statutory exemptions that seems to recognize that a copy-protection mechanism that prevents the making of an ephemeral recording is potentially otherwise actionable under 1201(a)(1) and, therefore, an exemption would be justified.

I guess we refer to that in the footnote,
that there are other access control means that have been applied, but that Congress made this express statement indicating that, at least from their perspective, the making of ephemeral recordings was control of access; a technological protection measure that prevents the making of ephemeral recordings was an access control under 1201(a)(1). So it is perhaps from that implication that we sought specifically to focus both on the ephemeral recordings and also brought it under the 1201(a)(1) proceeding with respect to even the copy protection.

MR. CARSON: All right. Well, apart from what you said in that footnote, referring to Section 112(a)(2) and newly-discovered 112(e)(8), I gather, what other argument do you have for us as to why we can pay any attention whatsoever to copy controls as such in this rulemaking?

MR. GREENSTEIN: To copy controls as such?

MR. CARSON: Yes.

MR. GREENSTEIN: Well, 1201(a)(1) does talk about direct controls access.

MR. CARSON: Right.

MR. GREENSTEIN: To the extent that the control that is applied prevents playback or other types of access, then certainly it is cognizable under
1201(a)(1), but, otherwise, I would say specifically that Congress appears to have spoken in this matter, that the making of ephemeral recordings and any control measure that prevents the making of ephemeral recordings is potentially actionable under 1201(a)(1) and, therefore, justifies an exemption.

MR. CARSON: And that's your best argument, is it?

(Laughter.)

Let me give you every opportunity, Seth.

MR. GREENSTEIN: That's my story, and I'm sticking to it.

(Laughter.)

MR. CARSON: Okay, very good.

Now back to the other point I was making: Again, apart from what you have just told me, I see nothing in the comment you wrote that talks about access controls as such. Why are we talking about this today?

You, of all people, know very well the process we set forth here, what was in our initial Notice of Inquiry, the process we had for filing late requests, if you didn't get it in on time. I have to say, and we are not ruling from the Bench here, but I have a very hard time understanding how you have put
before us the question of access controls on CDs. I am wondering why we are talking about it right now. How is that question before us properly at this point, given the procedures we have set forth?

MR. GREENSTEIN: I think it is before you because, again, an access control can have the effect of preventing the ability to make an ephemeral recording. Again, putting aside the argument with respect to the actual statutory language that Congress wrote in the two exemptions, anything that prevents playback or access to a file on a disc will prevent the making of an ephemeral recording. So you have to start there.

If there's an access control measure that prevents it from being played back in a CD or prevents the making of a copy of a file on a CD or another type of disc, then that is an access-control measure that ultimately has the effect of preventing the making of an ephemeral recording.

MR. CARSON: All right. Now I know this has been asked before and I know it has been answered before, but I'm a simpleton, I guess. I am having a hard time getting my hands on just specifically what kinds of access controls you have actually seen out there. So can you, as simplistically as possible,
explain to me what kinds of access controls you are aware of being used on CDs now, either in the real marketplace here or in test markets that you're aware of?

MR. GREENSTEIN: I guess the two that we're aware of, one deals specifically with the ability to even play back a protected file on a computer. The second has to do with this second session technology.

Essentially, what that does is that it prevents the computer from reading -- therefore, copying or playing back -- the full, high-quality audio, Red Book Format audio, on the disc. Instead, it allows access by the computer only to the much lower-quality, compressed Windows Media Player format, or whatever format happens to be adopted in that particular solution.

The SunnComm solution, as I understand it, uses the Microsoft Windows Media Player format, or the .wma format, but prevents access to the full, high-quality audio. Those are the two technologies that are access-control technologies that we are aware of at this point.

MR. CARSON: Okay. Now I'm pleased that I have got probably two of the world's experts on
Section 112 in front of me because I would like to ask
a question that has always bothered me about 112. It
may not sound like it's leading anywhere, but I think
perhaps it is.

So, Mr. Leavens, if you feel you're an
expert on this, by all means, you pipe in, too.

(Laughter.)

But I happen to know that Seth and Steve
are --

MR. GREENSTEIN: I thought you were
talking about Rob and Steve.

(Laughter.)

MR. CARSON: So tell me, construing the
statutory language of 112(c) -- and we'll just talk
about 112(c)(1); we won't go on to the little "A's" or
the "B's", and so on.

MR. GREENSTEIN: "C"?

MR. CARSON: Well, 112(e), I'm sorry. My
eyes -- there's bad light here. 112(e), you're
absolutely right.

How is it that that statutory license
permits you to make more than one phonorecord when in
the fifth line of the text we're all looking at, it
says it's a license to "make no more than one
phonorecord" of the sound recording?
MR. ENGLUND: The parenthetical that follows says, "unless the terms and conditions of the statutory license allow for more."

MR. CARSON: And where do we find those terms and conditions?

MR. ENGLUND: Do you want to answer that one?

(Laughter.)

MR. GREENSTEIN: I would hope they are in the regulations that were enacted by the Librarian.

MR. CARSON: Pursuant to the CARP process?

MR. GREENSTEIN: Pursuant to the CARP process and pursuant to various voluntary submissions to the Copyright Office for the regulations to implement voluntary license agreements as industrywide agreements.

MR. CARSON: Steve, do you concur with that?

MR. ENGLUND: It is certainly our understanding that the result of the CARP decision is that webcasters are permitted to make multiple ephemerals under 112.

MR. CARSON: Okay. So the CARP has the power in setting rates and terms to have -- actually, it sounds like it has considerable power to determine
the scope of this license. Is that a fair statement?

    MR. ENGLUND: I think it is fair to say that this parenthetical authorizes the CARP to deviate from the one-copy rule and permit multiple copies.

    MR. CARSON: Okay.

    MR. ENGLUND: I would not go so far as to say that it can deviate from the statute in other respects.

    MR. CARSON: Okay. Let's turn to 112(e)(8), the newly-discovered provision that may offer some hope, but perhaps not enough to some of us here.

    Does the CARP have power in setting rates and terms to construe 112(e)(8) -- and let's put it to you, Seth -- to construe it in such a fashion that 112(e)(8) can, in fact, pursuant to regs issued initially by the CARP, and ultimately by the Librarian, you can get everything you need out of it? Does the CARP say anyone, any webcaster, who needs to get access to a sound recording in the appropriate format that that webcaster needs may demand that the sound recording copyright owner make it available to him in that particular format, or would that be beyond the scope of the power that the CARP has?

    MR. GREENSTEIN: I would need to ponder
the question further. I think the answer depends on whether that could be seen as within the scope of the current language, within a reasonable interpretation of the statutory language, or if it is something that is beyond the scope of reasonable interpretation of the statutory language. I cannot say, as I sit here, that I have the right answer for you.

MR. CARSON: Okay, fair enough. Steve, anything?

MR. ENGLUND: Having thought about it for all of 30 seconds --

MR. CARSON: That's more than I think of most of the things I do.

(Laughter.)

MR. ENGLUND: My visceral reaction is that the CARP probably could not. There certainly is legislative history, more in the 114 than the 112 context, but maybe in the 112 context, of what rates and terms mean for the purpose of the statutory licenses. There are some examples that are given of the sorts of things that are like terms.

I think the CARP is permitted to authorize multiple copies because the statute says very specifically that they can. It is certainly not obvious to me, as I sit here, that the CARP could
write into the statutory license a term that says, on demand, record companies shall deliver CDs in whatever format a webcaster wants.

MR. CARSON: All right, I understand that.

Now, Steve, you said something probably 45 minutes or an hour ago that I took down, and I don't know if you will even remember having said it now. But I was curious about what you meant.

You were talking about 112(e)(8), and you said, in discussion, that the "Congress has already given you," referring to Seth, "what you want with respect to quality and format," and I think there was one other thing that I missed, "although perhaps not timing."

Can you elaborate on what you meant when you say Congress has given him what he needs or wants with respect to quality and format?

MR. ENGLUND: This is a proceeding about circumvention of access controls. All that Seth is asking for is permission to circumvent access controls. Congress has given him that.

MR. CARSON: Maybe not what he wants, but as far as it's willing to give it to him?

MR. ENGLUND: Yes.

MR. CARSON: Is that what you are saying?
MR. ENGLUND: It says in 112(e)(8) that, if he doesn't do it in a timely manner, he can circumvent. I suppose his argument is how copyright owners are going to be so motivated to prevent webcasters from circumventing that they will just give them copies of -- the term -- "terribly low quality," and that will satisfy the obligation and force the webcasters to use the low-quality copy and cut off the ability of webcasters to circumvent. That doesn't seem very practical to me.

MR. CARSON: Of course, 112(e)(8) doesn't say that the record company gives you copies, does it?

MR. GREENSTEIN: That's right. I was dealing with talking about the transmission of a copy of a phonorecord because that, to me, seems a lot more likely and practical than the likelihood of a copyright owner delivering to a webcaster a general means of circumventing the content-protection system.

I think that it would not be wholly unreasonable, despite the statutory language, for a copyright owner to fear that, having made this available to webcasters, this means they might somehow or another find their way into the marketplace in a more broad way.

I recognize that the statutory language
says that what the copyright owner is supposed to make available is the means to undo the access-control protection. I just have a very practical fear that that is not what would happen in practice then. Instead, what would happen is, at most, we would get access to copies of the files without the protections applied.

MR. CARSON: Well, why not stand on your rights? I mean, doesn't this language arguably give you exactly what you are asking us to give you? In other words, if the copyright owner has to give you the means to circumvent, if they really have to do that, you have got exactly what you want and you can get it in whatever format you want, can't you?

MR. GREENSTEIN: Well, of course, they don't have to. They could say that it is not technologically feasible or economically reasonable for them to do so.

MR. CARSON: And then you get to do exactly what you're asking us to let you do?

MR. GREENSTEIN: Right, although, again, according to the statutory language, this has to be accommodated on a sound-recording-by-sound-recording basis.

MR. CARSON: Is that clear to you?
MR. GREENSTEIN: It says, "a phonorecord" and "such phonorecord." If I were to read that language quite literally, that would mean that the request has to be made on a phonorecord-by-phonorecord basis.

MR. CARSON: Okay. Now looking at that same language, all right, the language says the copyright owner has to do this in a timely manner in light of the transmitting organization's reasonable business requirements.

Now it strikes me, Seth, that you have made a pretty compelling case that in many cases your reasonable business requirements are going to be right now or in the next few hours or, at best, the next day or two, and anything beyond that is beyond reasonable business requirements.

MR. GREENSTEIN: Uh-hum.

MR. CARSON: I think that would be, if I were in your shoes, that would be my position. Isn't that your position?

MR. GREENSTEIN: That would be my position.

MR. CARSON: And, Steve, do you acknowledge that there may be circumstances where that's exactly the case?
MR. ENGLUND: I don't know whether it's hours or days, but I understand that webcasters have a legitimate interest in getting new releases on quickly. I certainly see the language here, which speaks for itself.

MR. CARSON: So, Seth, what's your problem with this particular provision when you're talking about timing? Isn't the timing here good enough, given your reasonable business needs?

MR. GREENSTEIN: The problem is that, again, it has to be done on a phonorecord-by-phonorecord basis. That leads to the timing issue. Because if you have to make the request on a phonorecord-by-phonorecord basis, then you have to give an appropriate amount of time for the record company, for the copyright owner, to respond. That seems rather implicit.

If they don't respond within five minutes, when I needed the sound recording on my air yesterday, does that give me the right to circumvent? I don't know the answer to that. None of us knows the answer to that.

To say that the way that we should go about this is by, essentially, filing a lawsuit against the sound recording copyright owner to get the
court to enjoin them positively to provide these means
to us I think is not economically within reach of most
webcasters and not practical, given the needs of the
webcasters themselves.

    MR. CARSON: All right. I think, just in
response to the last question Rob asked, both Steve
and Seth suggested that we do have the power in
determining classes of works to narrow the eligibility
of people who can take advantage of exemptions for
particular classes of work.

    So have I misconstrued what either of you
said?

    MR. GREENSTEIN: That's correct.

    MR. CARSON: Okay. Now that's interesting
to hear. Let me just remind you that that was not the
conclusion this Office came to three years ago. I
mean, we, in no uncertain terms, made our
interpretation of how this statute works.

    It strikes me a little puzzling, I'm a
little puzzled to be sitting here today in a hearing
and hearing you for the first time suggest that it
ain't necessarily so and there may be another way of
interpreting it. I have seen nothing in writing. I
have seen no legal analysis.

    I think if you read the Notice of Inquiry,
we said certainly we're not locked into any legal analysis or legal interpretation we did three years ago, but we're going to expect you to make a pretty good case because those decisions of interpretation that we made a few years ago are decisions that we put a lot of thought into, and we've got a relatively firm conviction they're right. And if they're not right, then someone really does have some kind of a burden to persuade us that it is wrong.

Do you really think that you have carried that burden, just by coming in here today and orally, in about 30 seconds each, telling us what you think?

MR. ENGLUND: I'm not the proponent of the exemption.

MR. GREENSTEIN: Well, I don't know how much I can add to the arguments that were made last time around by those organizations that argued to you, I thought convincingly, that exemptions ought to be available to certain classes of users in particularly meritorious cases.

The language of 1201(a)(1)(B) talking about how -- it talks about non-infringing uses by persons who are users of a copyrighted work and that the prohibition shall not apply to such users with respect to such class of works. It seems to open the
opportunity for the Office to apply exemptions to particular users for particular classes of works, and particularly meritorious circumstances.

If the circumstance that I have put before you, at least with respect to the non-infringing nature of the use and the justification for the use, doesn't seem to be meritorious, I don't know what would. But it seems to me that under the circumstances and under the statutory language, one could reasonably say that an exemption could be granted to a particular class of users, so that the prohibition would not apply to such users.

MR. CARSON: Okay.

MR. ENGLUND: I think an exemption has to be made with respect to a class of works.

MR. GREENSTEIN: Yes.

MR. CARSON: No, we understand that. Yes, I think you do say that's at least a starting point. Okay.

Steve, I want to make sure I understand what the point is of the second session. Why is there?

MR. ENGLUND: Record companies want people to get their music. A way of doing that is to provide different access or access through different means on
different kinds of devices. The second session is a means of providing access on PCs.

MR. CARSON: But is it necessarily part of that that the quality of what you get in the second session is poorer than the quality of what is on the first session, or whatever you call the other session?

MR. ENGLUND: There are inherent limitations on the space and the capacity of the CD carrier to hold data. In order to have a typical number of recordings in the first session, you would probably almost certainly compress the data in the second session.

MR. CARSON: It almost has to be more than that, doesn't it? I mean, why bother having two different forms on there unless there's something different about the second form?

MR. ENGLUND: In addition, the second session is to protect it, so that -- it may be compressed, and it may also be protected with a digital-rights-management system, so that copying is limited.

MR. CARSON: Okay. But I'm not sure I heard a response from you to the point made by Seth, and perhaps by Tom, that when you're webcasting -- and we all understand, I think, that most webcasters,
probably all webcasters, are transmitting from server copies, not from CD players; I think at one point you finally acknowledged that — that they are necessarily going to have to use the second session copy and not the better-quality copy in those cases where you are using the second session features. That's understood, isn't it?

MR. ENGLUND: I don't think it is.

MR. CARSON: Okay, so why is that?

MR. ENGLUND: For a couple of reasons. First, thanks to newly-discovered 112(e)(8), they can circumvent the access controls in the first session.

MR. CARSON: Okay. So even if they've got the second session, because they can copy that, 112(e)(8) gives them the ability to circumvent to get the first session copy, is that true?

MR. ENGLUND: Interesting question.

MR. CARSON: Great. Seth, do you still need to be here?

MR. ENGLUND: I may have misspoken.

MR. CARSON: Let me give you a moment because this may be important.

MR. ENGLUND: Section (e)(8) begins, "If the transmitting organization entitled to make a phonorecord" — and it's a webcaster with a license —
"is prevented from making such phonorecord by reason of the application of technical measures that prevent reproduction of the sound recording." There's a bit of a disconnect there, as has been noted.

I suppose the answer has got to be that, if they have access, that they can't circumvent, but they've still got the opportunity to work with the copy in the second session and they've still got the ability to copy the first session.

MR. CARSON: Okay, I was curious about that because I don't quite understand it. When you say, "copy the first session," put it in a CD player, I gather, and then what do you do with it? How do you get it onto that server? Because that's where it's got to end up.

MR. ENGLUND: You string a wire from the CD player to the server.

MR. CARSON: Okay, and that works?

MR. ENGLUND: Yes.

MR. GREENSTEIN: No.

(Laughter.)

MR. ENGLUND: I've never tried it.

MR. CARSON: Okay.

MR. ENGLUND: But it's clearly the case that you can transmit the output of a CD player to the
sound card of a computer. It may be slower than ripping, clearly slower than ripping. You have heard from Tom that ripping is much faster, but it is clearly possible to send those bits over a wire, capture them, and format them into the same bits that would have been rendered on the CD player.

MR. CARSON: Let me hear what our other two panelists have to say about that.

MR. LEAVENS: Well, I suppose one can make their own gravel, too.

MR. CARSON: I'm sorry, their own what?

MR. LEAVENS: Their own gravel, too. I sounded a little facetious, but from the sense that you are describing a process that is entirely inappropriate to the systems that are set up for us to operate and the benefits that we're supposed to be enjoying by this digital technology.

So I can't speak to the technical aspects of the statute that you're talking about, but we have no remedy really, from what you are describing here, as far as being able to play something in real time and then somehow get that translated into a digital file. There are far too many processes involved, far too much time involved.

MR. CARSON: Well, let me make sure --
Seth, go ahead.

MR. GREENSTEIN: I'm just trying to understand exactly how this would work, because the output of a CD player, let's say analog or digital, it's not the same format that is computer data. It's a different data format. Dealing with digital data first, it's a different data format.

So you would need to convert it into the data format that the computer understands. Then the computer can record it, and then you can start manipulating it, then, to have it encoded for different bit rates and different codecs, a much more cumbersome process, much more expensive, and, frankly, when you're talking about doing this in real time for tens of thousands of sound recordings per year, prohibitive.

If we are talking analog, then you would have to go through a very similar process where you would have to go at the analog output and digitize it. And each time you perform transformations on data, you are losing some sound quality. As hard as you try and as good as the technology is, you are losing some data each and every time as you go from one format into another, which has an impact on the sound quality.

MR. CARSON: Steve, do you disagree with
that?

MR. ENGLUND: To some degree. It is true that the data format used in Red Book Audio is different from the .wav file format that is commonly used on computers and commonly used as the input to encoders and compression software.

But the process of turning Red Book Audio into a .wav file is something that happens all the time in a computer when you rip. It is not a computational matter. At least it is not clear to me that it is a computational matter.

It is much different from the process that would have to take place to convert the so-called S/P-DIF output of a CD player into a .wav file on a computer. It seems like the kind of data transformation that could be accomplished by somebody writing software, if the software doesn't exist already. I have never had occasion to look for it.

MR. CARSON: You folks may get a subsequent question from us on this, because it sounds like you think this is a significant point, Steve, and I'm taking it as a significant point.

MR. ENGLUND: To the extent that Seth's concern here is quality and not timing --

MR. CARSON: Yes, yes.
MR. ENGLUND: I mean, he says, "The second session isn't sufficient for me."

MR. CARSON: Right.

MR. ENGLUND: I think the second session ought to be sufficient access for purposes of 1201. You have previously found that there is no right here to get access in the best, most convenient possible way.

But to the extent that quality consideration is material here, a way to get CD quality audio is to play it in the CD player.

MR. CARSON: Well, let's be clear in what we said before. I think what we said before was, when you are talking about fair use, for example, someone who under the doctrine of fair use is able to make a good claim, "I should be able to get a copy of this," doesn't necessarily have the right to get that copy in the optimal, best digital format. There may be other ways of doing it, and that may meet all the requirements of fair use.

We are talking now about a statutory license where people who comply with the terms of the license do have, in effect, a right to transmit performances of those works to their customers, and that is what you want them to be able to do, I
believe.

So, under those circumstances, are you, nevertheless, saying they have no reason to expect that they are going to get good quality content that they can retransmit?

MR. ENGLUND: We’re not talking about good quality versus bad quality.

MR. CARSON: Well, I thought that was the whole point.

MR. ENGLUND: No, we were talking about less-than-full-CD quality, but they transmit in less-than-full-CD quality. I think the considerations are very similar to your past finding, which was, in fact, made in the fair use context, as you indicated.

The statutory license does not address access or quality. There is no requirement in the statutory license that if a record company has chosen to release a recording only on cassette tape, that it provide access on CDs to webcasters who might want higher quality.

MR. CARSON: Yes, but we are not talking about that. We are talking about a CD which has high quality here and right next to it somewhat lower quality. Because of the way you set it up, you are necessarily, at least according to Seth’s scenario,
not to your scenario, you are necessarily relegating them to the lower-quality copy.

It's not that you only put it out in audio cassette. You've got good quality and so-so quality, and you're telling Seth, "Sorry, you're stuck with so-so quality."

MR. ENGLUND: I think you should not rush to assume that the quality is so-so.

MR. CARSON: Okay, that was my next question.

MR. ENGLUND: The quality is whatever the author of the CD chooses to encode it at, and that will be based on a number of product design considerations. It is not the desire of record companies to sell a low-quality product. Record companies want consumers to be able to buy and enjoy the music and pride themselves on selling quality product.

Occasionally, it has been suggested that one way of securing the CD format is to offer a second session that is somewhat degraded in sound quality, but a better technological approach is probably to secure it with a digital rights management system.

In any event, I'm not a "golden ear."

There are some people called "golden ears" who listen
to recordings and can tell such differences, but I
don't know that I can tell the difference between an
MP3-compressed file and a CD-quality file, at least
when listening to it on my computer speakers.

So I think you should not rush to assume
that this is lousy quality.

MR. CARSON: Okay, so you're telling us
there is no reason for us to conclude that the second
session copy is going to be of such quality that it is
not going to be as useful for webcasting purposes or
to put it --

MR. ENGLUND: It would be commercially-
acceptable quality because record companies don't want
to put out a product that is not commercially-
acceptable.

MR. CARSON: And, again, the only reason,
is it a fair characterization of what you said earlier
that the only reason that the second session may be
lower quality is simply because there's not enough
room on the disc to put two equally-good-quality
copies on it, or might there be other reasons why the
quality of that second session one isn't going to be
as good? Had there been a choice, we don't want it to
be as good of quality? Is there any reason to think
that is going to happen?
MR. ENGLUND: That may play into the analysis. It may largely be a matter of the technology vendor's choice of how the second session technology is implemented in terms of what kinds of formats are supported in the second session.

MR. CARSON: Seth, I think you are straining for the mike or no?

MR. GREENSTEIN: Yes, I was. I wasn't straining, but reaching.

(Laughter.)

There is an important difference between the types of users that are targeted for the second session versus webcasters. The type of users targeted for the second session, that's the end product that they are going to use. That's the end product they're going to listen to.

Probably, you know, is it as good as the kind of MP3 file that you would rip for yourself? Probably yes. But webcasters don't use it as the end product. It is the source material for them. That is the starting point from which they have to make additional transformations, from which they have to make better-quality recordings for the high-bandwidth users, lower-quality recordings for more optimal transmission over lower bit rates. They have to go
from one media format to another, to another, to another, to make sure that they've got the full range of copies that they need to provide full service to all of their potential users.

From that perspective, broadcasters, webcasters, always like to start with the very highest quality. A television broadcaster doesn't use a VHS tape when they show movies. HBO doesn't use VHS tape. I mean they use digital beta tapes. They use the highest-available quality format. They don't use DVDs. They use professional-quality media.

CD audio is not the highest quality available, but it is the highest quality that is commercially available in retail that webcasters have easy access to if they don't get service of higher-quality copies from the record companies.

They need to start with the highest-quality source material in order to perform the transformations, in order to afford the public and to offer to the public a competitive service.

MR. CARSON: Steve, when I was asking an earlier series of questions, there was one followup I think you were suggesting but I wasn't hearing it very clearly. Does it still seem pertinent?

MR. TEPP: Well, it's a short one. I'll
just jump in with it.

It went back to the question you were asking about 112(e)(8) and the phonorecord-by-phonorecord concern that was expressed. And the question was, to what extent can you, of your own initiative, simply bundle requests? There is nothing in the text of 112(e)(8) that appears to prohibit that.

So couldn’t you engage in a little self-help on that problem by bundling the appropriate requests for accessible phonorecords and address that concern?

MR. GREENSTEIN: By bundling requests, you mean, essentially, to make requests in advance, to say that for everything you release over the next coming three years, we would like to have access to them?

MR. TEPP: I don’t think that would work under — well, I want your opinion. That’s not what I was asking about.

MR. ENGLUND: I really wouldn’t rule out the possibility. That’s precisely the right marketplace solution here. This is all speculation, but if a webcaster were to ask a record company, "Are you ever going to service me when I ask you for a copy," and the record company says, "No, I’m not ever going to service you," that seems like wholly
sufficient. It seems like the sort of thing that we shouldn't be speculating about, proceeding where there is a very high burden of proof to be overcome before an exemption should be granted.

MR. GREENSTEIN: I guess we have the reverse concern. I mean, suppose the answer comes back and says, "Well, no, ask me on a record-by-record basis. I'll let you know what's available for that and whether it's appropriate to give you the circumvention tool, whether it's appropriate to give you a file, or what level of quality file I'll give you. Ask me in particular cases, and I'll give you particular answers."

MR. TEPP: Let me just follow up with one thing, and then I will give it back because I've already had my chance.

But, given, as Rob has articulated quite well, the standard we are dealing with here of likelihood, is there any reason to think that particular CDs, even within a single label, are going to get that sort of disparate treatment, where they will give you "yes" to some, "no" to others, "We'll give you the tool here, but we will give you something else; we will give you an unprotected copy there."?

MR. LEAVENS: Do you mean track by track
within a CD?

MR. TEPP: Either track by track within a
CD or CD by CD within a label's repertoire.

MR. LEAVENS: I suppose there may be some
artist considerations that go into whether there is
something that is granted. There may be some
particular artists more concerned about that kind of
thing than others, or there may be -- I know there are
provisions in our contracts with the labels for our
conditional download service that allows the record
labels to withdraw tracks from our service simply on
the basis of artist relations issues.

When they get involved with contractual
negotiations with the artist, they are not compelled
to stop exporting through services such as ours, but
they may want to remove them from the marketplace, so
that is not an issue when they are talking to them.
We have actually encountered that a couple of times,
not a lot, but it is the kind of thing that does go on
all the time in the record industry. The labels are
very sensitive about their relationships with their
artists. They are protective of that. It is the most
important relationship that they've got.

So there may be reasons, for purposes of
artist relations, that there could be a variation in
how it is that they are granting consent or not granting consent.

MR. TEPP: So I know I promised that was the last one. I'll really keep to this one.

Is it fair to say, then, that what this whole request boils down to is the problem with the potential phonorecord-by-phonorecord approach of 112(e)(8), and that barring that, 112(e)(8) does everything you need?

MR. GREENSTEIN: Again, depending on the response that you get from the copyright owner, it could. It has the potential to offer everything that is necessary, but there's no guarantee in it that, if it is literally applied, that the problems would be addressed. Literally applied, the problems would not. That is the reason why we are spending so much time, and that Tom flew in from Chicago, and that lawyers are getting paid to address this issue.

I guess one other way to look at it is maybe by analogy to the experience of the motion picture industry, where they don't apply copy protection to every motion picture cassette. They apply it somewhat selectively, depending upon the value of the title, whether it is being sold at a low-price point, whether it is being sold at a higher-
price point.

Certain motion pictures they can apply the technological protection measures at various levels of intensity, depending upon the need. A lot of it is business marketing philosophy. If a particular work is especially valuable, they may apply copy protection to it using a very strong, robust system. If it is another artist, they may apply it less or they may not apply it at all.

It is difficult to predict, although I think in the marketplace, if the experience in the motion picture marketplace is any guide on this, then I think it is quite likely that there will be different reactions with respect to different sound recordings, the same way that there are different copy-protections mechanisms and modalities applied with respect to motion pictures.

MR. TEPP: I will keep my promise this time. Thanks.

MS. PETERS: Guess what, we're finished. I want to thank each and every one of you. This was a long session, but it was a very helpful session for us. I can't speak for you.

In any case, thank you.

(Whereupon, the foregoing matter went off
the record at 4:32 p.m.)