LIBRARY OF CONGRESS

+ + + + +

UNITED STATES COPYRIGHT OFFICE

+ + + + +

PUBLIC HEARING
ON
EXEMPTION TO PROHIBITION ON
CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS
FOR ACCESS CONTROL TECHNOLOGIES

+ + + + +

37 CRF PARTS 201
DOCKET NO. RM 2005-11A

+ + + + +

FRIDAY
MARCH 31, 2006

+ + + + +

MUMFORD ROOM
LM-649
JAMES MADISON BUILDING
LIBRARY OF CONGRESS
101 INDEPENDENCE AVENUE, SOUTHEAST
WASHINGTON, D.C.

+ + + + +

PRESENT FROM THE U.S. COPYRIGHT OFFICE:

MARYBETH PETERS, Register of Copyrights
DAVID O. CARSON, General Counsel
ROBERT KASUNIC, Principal Legal Advisor, OGC
JULE L. SIGALL, Associate Register for Policy and International Affairs
STEVE TEPP, Principal Legal Advisor, OGC

COMMENTERS:

MEGAN CARNEY,
EDWARD FELTON, Princeton University
STEVEN METALITZ, Joint Reply Commenters

JOSEPH V. MONTERO, JR., Spectrum Software, Inc.
DEIDRE MULLIGAN, Samuelson Law, Technology & Public Policy Clinic
MATTHEW SCHRUERS, Computer and Communication Industry Association and Open Source and Industry Alliance
JAY SULZBERGER, New Yorkers for Fair Use

I-N-D-E-X

P-R-O-C-E-E-D-I-N-G-S

9:38 a.m.

REGISTER PETERS: Good morning. I'm Marybeth Peters, the Register of Copyrights, and I would like to welcome everyone to our Washington, D.C. hearing in the Section 1201 Rulemaking. As you know, this hearing is part of an ongoing rulemaking process mandated by Congress under Section 1201 (a)(1), which was added to Title 17 by the Digital Millennium Copyright Act in 1998. Section 1201 (a)(1) provides that the Library in Congress may exempt certain classes of works from the prohibition against circumvention of technological measures that control access to copyrighted works for three-year periods.

The purpose of this rulemaking proceeding is to determine whether there are 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. Pursuant to the Copyright Office's Notice of Inquiry published in the Federal Registry on October 3rd of 2005, the office received 74 initial comments proposing the exemptions to a prohibition on circumvention, and 35 reply comments, all of these,

the comments and the reply comments, are available for viewing and downloading from our web site.

This is the third day of hearings in this rulemaking. We had originally set four full days of hearings here in Washington and two days in Palo Alto, California. But based on the number of persons who requested to testify, we did not need all of those days. We have already conducted hearings last week in Palo Alto on March 23rd, and we had in D.C. on March 29th a hearing. After today, we will be conducting another hearing on Monday, April 3rd in the morning. We intend to post the transcripts of all of the hearings on our web site when they are available a few weeks after conclusion of the hearings.

The comments, reply comments, the hearing testimony, all of these will form the basis of evidence in this rulemaking, which, after consultation with the Assistant Secretary of Communications and Information of the Department of Commerce, will result in my recommendation to the Librarian. The Librarian of Congress will make a determination by October 28th of 2006 on whether exemptions to the prohibition against circumvention shall be instituted during the ensuing three-year period and if exemptions should issue what particular classes of works should be

exempted from the prohibition on circumvention.

The format of the hearing will be divided into three parts. First, witnesses will present their testimony. This is your chance to make your case to us in person, explaining the facts and making the legal and policy arguments that support your claim on whether there should or should not be a particular exemption. The statements of the witnesses will be followed by questions from the members of the Copyright Office Panel. The panel will ask some questions of the participants in an effort to define and refine the issues and the evidence presented by both sides. This is an ongoing proceeding, and no decisions have yet been made as to any critical issues in the rulemaking.

In an effort to fully obtain relevant evidence, the Copyright Office reserves the right to ask questions in writing of any of the participants in these proceedings after the close of the hearings. After a panel has asked its questions of the witnesses, we intend to give the witnesses the opportunity to ask questions of each other. If we have not managed to come up with all of the questions that should be asked of each of you, I'm confident that one of your fellow witnesses is likely to do the

job for us.

Let me now introduce to you the other members of the Copyright Office panel. To my immediate left is David Carson, the General Counsel of the Copyright Office. To my immediate right is Jule Sigall, Associate Register for Policy and International Affairs. To David Carson's left is Rob Kasunic, Principal Legal Advisor in the Office of the General Counsel. To Jule Sigall's right is Steve Tepp, also a Principal Legal Advisor in the Office of the General Counsel.

As most of you know, the first panel consists of Deidre Mulligan of the Samuelson Law, Technology & Public Policy Clinic; Ed Felten of Princeton University; Matthew Schruers of the Computer and Communication Industry Association and the Open Source and Industry Alliance; Jay Sulzberger of the New Yorkers for Fair Use; Steve Metalitz, the Joint Reply Commenters; and Megan Carney. Are both of you going to testify?

MR. PERZANOWSKI: Yes, that's right.

REGISTER PETERS: Okay. So Aaron Perzanowski is with Ed Felten. I think maybe what we'll do is just go down the row. Okay. Why don't we start over here with Ed and Aaron.

MR. FELTEN: Thank you for inviting me here to testify today. I'm Ed Felten. I'm a professor of computer science and public affairs at Princeton University and founding director of Princeton's Center for Information Technology Policy.

In September of last year, Alex Halderman, a graduate student working with me, discovered security problems, serious security problems in two separate technologies being shipped on compact disks by Sony BMG, and other record companies. The problems that Alex discovered exposed people who listened to those compact disks on Windows PCs to significant security risks. On finding these problems, we immediately called our lawyers.

We spent a significant period of time consulting with counsel both within Princeton University and outside, including multiple outside counsels. And for about a month, we were in consultation with counsel on and off without telling anybody what we had found.

Ten years ago, it wouldn't have worked this way. We would have called the vendor immediately and informed them of the problem. We would have described it as fully as we could. And we would have started preparing immediately for a responsible

disclosure to the public about the nature of the security risks and what consumers could do to protect themselves.

But that was before Section 1201. Since 1201, our research on technical protection measures has been slowed, as it was in this case, and limited. We do not embark on any new research projects in this area without first consulting with counsel, as we did in this case. Many other independent researchers who have a lower tolerance for lawyers than we do, have simply left the area entirely.

During this month in which we were consulting with counsel and not telling the vendor and not telling consumers about the nature of these problems, a great many consumers were at risk every day. Our exemption request, fundamentally, is asking for protection for those consumers.

The best example of the problem that our exemption is aimed at is the well-known Sony BMG copy protection software. And for information on that, I would refer you to the academic paper that Alex Halderman and I prepared, which we would be happy to share with you. It's currently in peer review.

But let me give you a little bit of background on these technologies. First of all, there

are two separate copy protection technologies at issue known as XCP and MediaMax produced by different companies and shipped on CDs by Sony BMG and other record companies. The installation of either of these pieces of software cause security vulnerabilities, and installation was, in one case, the default when the user listened to one of these compact disks. And in some cases, the software installed even when the user did not consent. If the user clicked "decline" on the end-user license agreement, in some cases the software would install anyway.

So in that case, mere insertion of a compact disk into a personal computer to listen to it would expose users to security risks. Some of these disks had labels indicating in a vague sense that some software might be installed if the user inserted the disk, but some were not labeled at all.

Now, once this software is on the user's computer, removing the software would enable the user to listen to the music, to make that lawful use, namely listening to the music, without security risk. The Joint Reply Commenters engage in some verbal gymnastics on this point, but the simple fact is in this case that removing the dangerous software re-enables lawful use of the music, listening to it.

To illustrate the need for this exemption further, I'd like to consider the plight of a user who owns one of the affected compact disks and wants to listen to it on a personal computer, as many users do. Many of my students, for example, have Windows PCs as their only way to listen to compact disks. I myself do not own a traditional audio CD player. If I want to listen to a compact disk in my home or my office, anywhere but my car, I'll be doing it on a Windows PC.

Initially, Sony BMG claimed that there was no reason to remove the software, that the security problems either did not exist or were not worthy of notice by users. And during this period, the user's only recourse, if the user wanted to safely listen to this music on a Windows PC, the only recourse the user had was to remove the software manually or to use an unauthorized uninstaller, simply because Sony BMG did not make an uninstaller available.

Later, Sony BMG issued an uninstaller, uninstallers for both of these technologies, but these initial uninstallers both turned out to make the security vulnerabilities considerably worse, as Alex Halderman and I discovered. Once these initial uninstallers were available, again the user's only safe course, if they wanted to listen to the music on

a Windows PC, was to either remove the software manually or to use an unauthorized uninstaller, and we made such an uninstaller available.

Later, Sony BMG did issue uninstallers that did not introduce new security problems, and that's the current situation. Sony BMG now offers these other uninstallers. But, still, unauthorized removal procedures are the safest course for users even today. The authorized uninstaller does nothing to prevent re-infection of the computer by the dangerous software.

Suppose, for example, that a consumer has a compact disk containing MediaMax Version 5 software, one of the two systems shipped by Sony BMG, and that the consumer has listened to that compact disk on their computer in the past. If the consumer uninstalls MediaMax by using Sony's authorized uninstaller but then later wants to listen to that compact disk again, and I would note that Sony BMG has not recalled the MediaMax disks, if the user in this circumstance simply inserts the compact disk into their computer, the dangerous software will reinstall itself, even if the user does not consent. In fact, simply inserting the compact disk into the computer will reinfect the user's computer, and the authorized

uninstaller shipped by Sony BMG does not do anything to block this reinstallation. There are other uninstallation procedures, unauthorized uninstallation procedures, that do prevent the reinstallation of this dangerous software.

So to sum up, let me explain the current situation, the current situation with this software after Sony BMG claims to have solved the problem as clearly as I can. It is still true today that listening to a MediaMax compact disk in a PC exposes a consumer to security risks, even if that consumer has previously used Sony BMG's authorized uninstaller. It is still true today that only unauthorized uninstallers will protect users fully against this risk of reinstallation, and it is still true today that these problems are impeding lawful use of the music on these CDs by scaring users away from inserting the compact disks into their computer at all.

Now, to close, I'd like to point out that the basic design strategy used by this software, so-called active protection in which software that is shipped on the media, on the compact disk, is installed onto the user's computer. That basic design strategy is still in use today. There is reportedly

a new version of the MediaMax software supposedly in development and all indications are that it will use the active protection method, as well.

There's another technology shipped by Macrovision on other compact disks which we are currently studying. We are not in a position to give a verdict on the security of that software as of yet.

Now, these other technologies may or may not introduce security bugs like those of XCP and MediaMax. We don't know for sure until we've studied them. But we do know this: we've studied two technologies so far that use active protection, and both of them have suffered from these problems, causing serious security flaws for users, and both of them have impeded lawful use of music, namely listening to the music on a personal computer.

And if experience in working with computer security teaches us anything, it is that security bugs are a fact of life. If this type of technology continues on its current path, it's only a matter of time before a problem like this reoccurs, before some vendor makes a security mistake and users are again exposed to this kind of security flaw.

Granting our exemption request will ensure that when more problems like this do occur, users can

still enjoy safe and unimpeded access to their music. Thank you.

REGISTER PETERS: Thank you. Mr. Perzanowski?

MR. PERZANOWSKI: Good morning. My name is Aaron Perzanowski. I am a student at the Samuelson Law Technology and Public Policy Clinic at the University of California Berkeley School of Law. And for the last year and a half, under the supervision of Professor Mulligan, I've been working very closely both with Professor Felten and Alex Halderman in providing advice on potential liability under the DMCA for the security research that they do.

So purely from the perspective of my own professional development, this has been an incredibly valuable experience for me. I've had the opportunity to learn a lot about a very fascinating area of law, to work with incredibly intelligent people who are doing very important work that I both respect and admire. So this opportunity has been one that I've been very thankful to have the chance to take part in.

But as someone who's concerned with the development of sound public policy, I must admit that this experience has been quite troubling for me. I find it very disturbing that academic researchers,

like Professor Felten and Mr. Halderman, who are incredibly well respected within their field, who conduct their research at one of the most well-renowned institutions of higher learning in this country, and whose research is directed at protecting the public from significant harms are forced to have such close and ongoing relationships with their attorneys. So while it's been a great experience for me, I would certainly prefer, as I'm sure Professor Felten would prefer, that he never have to speak to me again. So part of my job today is an attempt to make the knowledge that I've gained over the past year and a half obsolete, at least for the next three years.

So Professor Felten has done an excellent job of providing the factual basis for the exemption that we seek, and just to remind the panel the exemption that we are requesting is one for sound recordings and audio visual works distributed in compact disk format and protected by technological measures that impede access to lawfully purchased works by creating or exploiting security vulnerabilities that compromise the security of personal computers. So I think Professor Felten has done a great job of giving you the factual basis for this exemption.

So I'd like to spend my time this morning addressing some of the arguments that were made in the Joint Reply Comment. And I'd like to start with the notion advanced in the Joint Reply Comment that Section 1201(j) already addresses the concerns that we raise in our exemption proposal. We think there are very good reasons to doubt that Section 1201(j) provides meaningful protection for security researchers. In fact, we think there are good reasons to doubt that Congress, in enacting Section 1201(j) had this sort of activity in mind at all.

Now, it may seem to some of you, as it often does to me, that when we enter this discussion we enter sort of an alternate reality where copyright holders are arguing that security researchers are exempt from DMCA liability, while the researchers themselves and their attorneys are arguing that they face serious liability. The irony of this situation is not entirely lost on us. But to be perfectly clear, if Professor Felten or Mr. Halderman were to face the DMCA liability in a future lawsuit, we would certainly argue that Section 1201(j) provides them protection, and we are equally certain that the Joint Reply Commenters and the copyright holders that they represent would argue that Section 1201(j) offers

absolutely no protection.

So, admittedly, neither the Joint Reply Commenters or we are perfectly positioned to make the arguments that we are forced to make in this proceeding today. However, I see it as my responsibility to, as candidly as possible, outline the reasons to doubt that Section 1201(j) provides meaningful protection from liability. And I think we can start that conversation just by thinking about the title of Section 1201(j). 1201(j) is the security testing exemption, and we can contrast that with Section 1201(g), which is the encryption research exemption. So this discrepancy in terminology seems to point to the fact that Congress, when it's concerned about research activity, knows how to make that clear in the statutory language. Section 1201(j) it seems, since it does not actually mention research in particular, was designed with another purpose in mind.

So what is the scenario that Section 1201(j) envisions? I think that looking at the statutory language makes it pretty clear that there's a very narrow set of circumstances under which Section 1201(j) applies, and those circumstances are not very well mapped on to the sort of research that Professor

Felten is engaged in.

1201(j) requires a prior and ongoing relationship between the copyright holder and the circumventer, since that statute requires authorization from the copyright holder in order for circumvention to be protected. The statute also prefers very limited disclosure of the results of security testing. Ideally, I think the statute would prefer a situation where the results of security testing were shared only with the copyright holder and were not disclosed publically at all.

So this scenario works very well for people, for example, who are in the business of creating firewalls to protect computers. They have ongoing, often contractual, relationships with people whose computer systems they are in the business of protecting, and they have no need for public disclosure of the information that they discover in their testing.

I think this becomes even more clear when we look at the definition of security testing in Section 1201(j), which is limited to "accessing a computer, computer system, or computer network solely for the purpose of good faith testing." Now, as the library copyright alliance explained in its comment in

this same proceeding, Section 1201(j) appears to permit the ethical hacking into a computer system for the purpose of detecting security flaws in the firewall protecting the system.

Now, it's far less clear that Section 1201(j) applies in the scenario that we have here where the technological protection measure in question does not protect a computer, computer system, or computer network, but instead protects copyrighted content that is stored on removable media that may be accessed through a computer. And I think that this narrow reading of Section 1201(j) is supported by the sole judicial opinion to directly address that particular statutory section, Universal City Studios versus Reimerdes. In that case, the court considered a scenario that, in very important respects, is factually similar to the one that we're faced with here. We have removable media, in that case a DVD, that included a protection measure that limited the ability to access it on a personal computer, just as we have here. And there the court said that 1201(j) could not apply because DCSS, the program at issue, had nothing to do with a computer, computer network, or computer system because the protection measure was not designed to protect the computer but was designed

to protect the copyrighted content on the removable media.

The Reimerdes also importantly highlighted the authorization requirement of Section 1201(j) when it held that since Reimerdes had not received explicit authorization from the copyright holder to circumvent that Section 1201(j) was not available as a defense.

Now, requiring authorization is a particularly inappropriate fit for the sort of research that Professor Felten and Mr. Halderman are engaged in, given the fact that their research is intended to publicize and identify security vulnerabilities in protection measures that have already been distributed. Copyright holders have very little, if any, incentive to give their seal of approval to that sort of research.

In addition, the two factors that are listed in Section 1201(j) that courts must consider in determining the applicability of that defense also weigh against security researchers having that defense available. So courts must consider first whether the information derived from security testing was used solely to promote security of the owner/operator of the computer and, secondly, whether the information derived was used or maintained in a manner that does

not facilitate infringement. These two factors seem to suggest that this defense is rarely, if ever, going to be available for security researchers.

Their sole purpose, if they have one at all, is the disclosure of information. It's central to the academic enterprise that these researchers are engaged in that once they discover this information it is disclosed. That's the way they advance knowledge in their field. That's the way that they promote sound policy, and that's the way that they protect consumers.

Now, certainly, as Professor Felten has mentioned, when they do make disclosures, they take great care to make sure they do so in a responsible way, first contacting the vendor so that they can begin working on a solution to this problem before it can be exploited by malicious hackers. But once the information has been disclosed and has been disclosed in an academic paper or been disclosed publically, there is some risk, of course, that people will use that information to infringe copyrights. So under both (j)(3)(A) and (j)(3)(B), it seems unlikely that this defense is available for security researchers.

So those two factors, in conjunction with the authorization requirement of the statute, seem to

suggest not only that Section 1201(j) is rarely, if ever, available for these researchers, but that Congress had a completely different set of activities in mind when it crafted this exemption. So legally there are strong reasons for this panel to find that Section 1201(j) simply does not address the concerns that we raise in our comment.

Now, the argument raised by the Joint Reply Commenters that Section 1201(i) already addresses our concerns faces similar difficulties. Section 1201(i), of course, exempts circumvention when the protection measure in question collects or disseminates personal information about the online activities of a natural person. Now, there are three major protection measures currently on the market. Two of them certainly do collect and disseminate some sort of information, those being Macrovision's products and XCP's product. I'm sorry, not Macrovision, but SunnComm. Macrovision, to the best of our knowledge, their products do not, in fact, collect and disseminate any information so clearly do not fall within 1201(i).

Now, even for those products that do collect and disseminate information, it's doubtful that the information that they do collect qualifies as

information about a natural person. XCP and MediaMax, for example, both collect information that includes a unique identifier that corresponds to a particular CD title that has been inserted into a machine, and when that information is relayed to the copyright holder it includes the IP address of the machine that the disk has been inserted into.

It's far from clear that an IP address alone constitutes information about a natural person. From an IP address, we certainly can't tell who is using the computer at issue.

Regardless, Section 1201(i), since it requires that the act of circumvention have the sole effect of identifying and disabling the capability to collect and disseminate information and has no other effect on the ability of any person to gain access to a copyrighted work, seems pretty clearly to disqualify the sort of research that's going on here.

Circumvention of the class of works that we've described certainly has more than one effect. Primarily, the effect of that research is to remove an independent security threat that may be completely distinct from the protection measure's ability to collect and disseminate information. And, moreover, access to the copyrighted work is granted once the

protection measure has been removed.

So, finally, the Joint Reply Commenters argue that deleting or removing a protection measure is not circumvention if no access to a copyrighted work is granted. We believe that that statement is certainly true. However, the hypothetical protection measure that is described in the Joint Reply Comment where somehow once the protection measure is removed the copyrighted content, in some sense, self destructs, it is no longer available for any use whatsoever, simply does not exist in the real world. I'm positive that if copyright holders and their protection measure vendors were sophisticated enough to come up with a protection measure like that it would certainly be on the market right now, but the simple fact is that none of the protection measures on the market function in this way. Once the protection measure has been removed, users have unfettered access to the underlying copyrighted works.

Now, the Joint Reply Comment also argues that since Sony was kind enough to eventually provide a removal tool to uninstall this rootkit that somehow the need for our exemption has been obviated. Aside from the fact that authorized tools require undue delay and often introducing dependent and even more

dangerous security risks, there's another really good reason to think that authorization is simply incapable of addressing the concerns that we have. I think the Joint Reply Commenters conveniently forget the actual chain of events that occurred in relation to the Sony rootkit and, in some sense, they put the cart before the horse.

In this situation, what occurred was that a series of independent security researchers brought to Sony's attention the fact that these vulnerabilities existed, and only after that information was publically accessible and there was an ongoing public outcry did Sony act. So if researchers had to wait for authorization, we probably still wouldn't know about the Sony rootkit situation, and we certainly won't know about the next one down the line.

And, of course, as I mentioned before, authorization for this sort of research is not easy to come by. We have spent considerable time and effort contacting both record labels and protection measure vendors asking them for assurances that they will not file suit against Professor Felten and Mr. Halderman for their research in this area. And so far those efforts have met with incredibly disappointing results. Even Sony BMG who has publically made

statements that it will not file suit against researchers, legitimate researchers engaging in this sort of research, has so far, after several attempts stretching over the course of months, has so far been unable to provide us with any assurance that they will not file suit against these two particular researchers.

So to conclude, this research is vitally important. It is the only thing that's preventing serious harms from being visited on consumers, harms that they simply cannot understand and cannot know without the research going forward. But this research requires legal clarity. The existing statutory exemptions likely provide little, if any, protection. And any protection they do provide is certainly ambiguous at this point.

This rulemaking proceeding, however, offers a unique opportunity and the perfect vehicle to establish the sort of clarity that is needed for this research to move forward. So in light of the failure of the Joint Reply Commenters to present any arguments that overcome the pressing need for security research that protects consumers and the information infrastructure as a whole, we strongly urge the Register to recommend our exemption proposal. Thank

you.

REGISTER PETERS: Thank you. Ms. Carney?

MS. CARNEY: Hi. My name is Megan Carney. I am also grateful for this opportunity. While I work in computer security, I'm only here as a consumer, so I'm representing myself today because I am also very troubled by the direction I see these laws going. And before I start my prepared statement, when he mentioned undue delay, it really was undue delay when Sony first released the patch. You had to call up Sony, where they would direct you to a web page where you were allowed to download it. But it wasn't publically available for people who just wanted to go download it. They had to call up Sony first. So in that sort of situation, yes, it was available, but was it really easily available to the people who needed it?

Well, I'd like to start out my statement by saying that I think the rights of copyright owners are important. I think it's a measure of how convoluted the debate about intellectual property laws has become that I need to reassure you first that I don't mean to abolish the rights of copyright owners. I only mean to present that there should be restrictions on them. Anyone these days who seems to

propose restrictions on the rights of copyright owners somehow gets labeled as someone who wants to take away copyright laws entirely, and I think this is a false position.

Intellectual property rights are and always will be a difficult balance between creating for original work and the public good. It is, of course, necessary that artists, authors, musicians, and actors have the ability to profit from their efforts when they make original works. It is just as necessary to make sure that these rights are balanced by the rights of consumers.

Right now, it is illegal for consumers to bypass the copyright protection on CDs even if playing that CD as intended installs software that could harm your computer. Practically, this puts the average consumer in a very difficult position. When they put a music CD in their computer that has harmful software on it that could violate their privacy or damage their computer, they can either break the law or purposely violate their own rights, and I think that's a false position to put consumers in.

The digital rights management software Sony used on their CDs that was discovered in 2005 was just of this nature. And unless there is an exemption

in the future, it is likely to appear again.

Furthermore, research showed that Sony's software was installed on at least 500,000 systems. Some of these were in the government and on military domains. This means that Sony put our nation's infrastructure at risk to prevent users from putting songs on their iPod. And while as I said before, I recognize that copyright owners have certain rights with regards to their works, I don't think it extends to that sort of Draconian protection.

Where I work, we've seen at least 10 or 20 infections this year from the Sony rootkit. Some of them have been in areas that have protected data, such as medical data or financial data, that we are obligated to protect. And to put consumers in the position of being weary of every CD they put in their computer or they might lose their job because something got leaked, I don't think it's tenable.

We must remember that the purpose of intellectual property laws set out in the constitution is to promote progress in the arts and sciences. And while this law provides for exclusive control of a work for a certain period of time, it only does so to create incentive for original works. It does not imply that the copyright owner's rights are absolute

or that they extend over the user's computer. When a copyright law does not promote progress in the arts and sciences, it contradicts its original purpose.

Certainly, requiring consumers damage to their computers and violate their privacy in order to follow the law does not promote progress. It is imperative that the Library of Congress allow consumers to protect their rights by exempting CDs and DVDs with software that can harm consumers' computers from the anticircumvention laws.

REGISTER PETERS: Thank you. Mr. Schruers?

MR. SCHRUERS: On behalf of the Computer and Communications Industry Association, I thank the Copyright Office for the opportunity to appear here today. I am here in support of our proposed exemption to the Digital Millennium Copyright Act's anticircumvention rule, which would permit the circumvention in the case of particular works protected by access controls that threaten critical infrastructure.

As written, the Digital Millennium Copyright Act undermines the ability of security application vendors, security professionals, and end users to adequately protect infrastructure. Even

though access controls or the works that they protect may threaten our infrastructure, it may, nevertheless, violate Section 1201 to remedy that threat by circumventing the dangerous access control. In this way, the prohibition has inadvertently prioritized profits over security and could put our nation at risk.

The Sony BMG rootkit debacle illustrates that very clearly. Previous testimony I think has covered a lot of the problems that we've seen. Conservative estimates of the infected DNS name servers are 350,000 compromised dot gov servers. All branches of the United States military were represented in the compromised dot mil servers. And, yet, the security vendors seeking to protect us from that risk threat risk violating Section 1201 and potentially incurring criminal actions.

So, not surprisingly, patches were not prompt. Some vendors released patches that removed only the cloaking device but left the protection scheme itself in place. And as I understand Professor Felten's research, certain inappropriate patches of the protection scheme itself created the risk of remote code execution by hackers, and that's probably the most serious problem that we have to worry about

today. And that problem was not remedied. So in short, the DMCA impaired the security industry's ability to respond to a threat of global proportions.

So as I see it, the question here should not be whether to allow the circumvention but whether the act already allows it or whether we create the necessary exemption to ensure that we can protect ourselves from this risk. Section 1201(i) and 1201(j) are the only current exceptions to the statute that have been suggested that could have any bearing on this. 1201(i) addresses technological protection measures that are collecting or disseminating personally identifiable information. It permits circumvention only to disable that collection capability. Rootkits, in general, function to cloak registry processes. They don't function, as a natural matter, to collect information, although they may. So you could have other problems of this nature that are not collecting PII, personally identifiable information. And there are other applications that do collect PII or information that could be PII, such as keystroke loggers, although not necessarily. So there is a host of threats out there that would not be covered by 1201(i).

Mr. Perzanowski also referenced the

natural persons in Section 1201(i). It allows exemption to protect the data of natural persons who seek to gain access to a protected work. So that would appear to leave unprotected non-natural persons, like the government's militaries and corporations that were threatened by the rootkit, and it would also appear to leave unprotected the innocent bystanders, users who are not interested in gaining access to the protected work but happen to be using the compromised machine.

1201(j) is the other exception that's been put forward. It only allows accessing computer, computer system, or computer network. It does not permit access to the offending work itself, it would appear. Nor does it appear to permit accessing an electronic device that's not a computer. Joint Reply Commenters have told us that 1201(j) is satisfactory, even though it withholds protection from accessing the underlying work, because in the Sony rootkit case the underlying work wasn't the threat. This blindly assumes that the underlying work will never be a threat, and, yet, we saw here in the rootkit case how virus writers appropriated the rootkit to protect their malicious code. So it would be irresponsible for us to assume that malicious hackers might not

appropriate technological protection measures to protect their code.

On the second problem with 1201(j) as we see it, 1201(j) does not allow the sort of, apparently, the broad understanding of computer as is embodied in the Computer Fraud and Abuse Act. The Joint Reply Commenters suggest that it was probable that a court might interpret it that way, although as Mr. Perzanowski indicated, that seems unlikely. And I should point out that the Joint Reply Commenters themselves offer no certainty on this matter, which sort of embodies the whole problem here. There's the suggestion that researchers and professionals, like Professor Felten and Ms. Carney, have to prove that what they're doing violates federal law before they can get an exemption to protect us. And the Joint Reply Commenters aren't offering any assurances one way or the other. It suggests to me that the Joint Reply Commenters don't know either, and it's this uncertainty that creates the very risk.

So that raises for me a perplexing question: why on earth are we putting cyber security in the hands of copyright lawyers? Protecting infrastructure should not require advice from counsel. When Professor Felten finds a vulnerability, he picks

up the phone and calls a lawyer. If I found a vulnerability, I would think I should be picking up the phone and calling him.

So if you have to bet who on this panel is best suited to protect our networks, you wouldn't bet on the lawyers. You'd be on the security researchers, the security professionals, and the businesses like them that specialize in this area. So don't let us, the lawyers, prevent them, the professionals, from doing their job because they're trying to keep us safe. Thank you.

REGISTER PETERS: Thank you. Mr. Sulzberger?

MR. SULZBERGER: My name is Jay Sulzberger, and I'm a working member of New Yorkers for Fair Use. I'd like to address Matthew Schruers' last statement and expand on it. I think lawyers are terribly important here and, of course, the part of the law that is terribly important in these considerations is not copyright law. It's the law of private property. It's the law of privacy. Those are the parts of the law.

Now, Matthew also mentioned that should we be handing the entire computer and communications infrastructure of the United States and the world over

to copyright holders in cooperation with hardware manufacturers and Microsoft? And the answer is of course not. But we have to first be clear on this. This is so obvious when stated in those terms that I believe there's not a single person in this -- just a moment. Is there anybody here who is disabled from understanding the concept of private property? If anybody is not clear on it, and I know lawyers will raise all sorts of objections because there's a too simple notion of a perfect freehold, a perfect ownership of a chattel. But look. Your computer and your house, your relationship and ownership to it, if you've bought it and are legally running it and you're not violating, you're not committing copyright infringement by publishing for profit other people's works for which you don't have a license, copyright holders should not be inside your computer, and they shouldn't have pieces of code that you can't look at to get control of your computer.

And I had a sentence in my comment up on Professor Felten's proposal for an exemption, and, of course, people would think, "Oh, he's being witty." I'm not being witty. Who are the copyright holders? For whom do you have to give authorization under the Section -- I'll have to check it -- J, I think, of the

1201(j) of the DMC, you have to get authorization from people who've written a piece of malware that's gotten on your machine without your express consent that's damaging your machine. I think there's no member of the panel and I think there's no member of the people up on the dias who can possibly defend the concept that United States copyright law is going to require me to go and get permission from somebody who's invaded my machine, done damage to my machine, cost me hours of effort, and, if I'm a business, perhaps cost me thousands and thousands of dollars. These are the issues.

Now, why are we unclear on this? It's because we don't know what a computer is. Copyright has already been misused to allow Microsoft and Apple to place stuff in our machine when we go to the store we're not allowed to look at. It's my right to look at every darn piece of code. It's my right to publish what the code does. It's my right to decompile.

You might find me agreeing it's not my right to sell an improved version of their operating systems without getting a copyright license for it, but that's quite a separate issue. The issue here is private ownership and wiretapping. And this is ridiculous that the DMCA should be misinterpreted so

as to actually defend people who write malware. We have heard testimony from people who have tried to get the people who wrote the malware to do something about it, and their response was nothing or, "We promise not to sue you," or, "Maybe we'll sue you." This isn't okay.

Every lawyer here has taken a course or one or two or more on the law of private property. And, my gosh, copyright law can never say that I lose my right of ownership of a computer because some copyright holder appeals to the DMCA after they've written a trojan, a virus, whatever it is they've written, something that goes into my machine, a rootkit.

Now, I was going to explain more, but I think I've come to the end of my time. I see these introductory comments are short. And what I wanted to do was explain how Sony BMG rootkit is negligible in its damage compared to what the DMCA anticircumvention clauses are enabling in the near future. They're enabling Microsoft, as announced, it announced in 2002 that it was going to install and license a rootkit to anybody who paid the money. The system, the OS, and the hardware together, let's briefly call them Palladium -- they've changed the name, I think I made

the same joke three years ago, into mom's apple pie and the anti-terrorist loveable operating system with lots of bright, shiny colors. I've forgotten if that's their latest name for it.

Look. They've got something called the curtain. When you pay Microsoft a certain amount of money in the future, they claim they will let you write programs that are hidden behind the curtain. You can never look at them. The Sony BMG rootkit is a joke today. It's based on the Microsoft operating system. You can get around it in a few weeks, if you're really competent and have hotshot students or if you've a professional and know what you're doing and know about Microsoft operating system. You can get right around it, and, of course, it always has the joke get-around that I think if you press the shift key while the thing is loading there's certain circumstances it doesn't get installed.

Look. That's nothing. You should hardly be concerned about it, except we know that people who write viruses and trojans that damage your machines will appeal to the anticircumvention clauses in the DMCA. It's a joke how little damage it's caused compared to what's coming down the pike real soon unless you act.

I know it seems ridiculous. You're specialists in copyright. You're specialists in learning, publication, making sure authors get paid, what are the rights here, what are the rights there. It's because the country has gone crazy and because people don't know what ownership of computers means that we have this thing.

I think I've come to the end of my opening statement. I'm sorry to rant so hard, but I know that you're prepared for it. Thank you.

REGISTER PETERS: Thank you. Mr. Metalitz?

MR. METALITZ: Thank you very much. I'm pleased to be here, again, on behalf of the 14 organizations that joined as Joint Reply Commenters and welcome the chance to present their perspectives on this issue. I think it was Professor Felten who said at the beginning of our panel that security bugs are a fact of life, which I agree is true; and, therefore, I think it's very timely that we're having this discussion.

The Joint Reply Commenters do oppose any recognition of any exemption in this area, and I'd like to just briefly explain why that is without getting into all of the issues that have been raised

here this morning. I think the main reason why we don't believe an exemption is appropriate here is if the activity that members of this panel wish to immunize, wish to protect against legal liability, is not circumvention. It's uninstallation. It's removing the code, in the case of the Sony BMG example, removing the code from the computer system secures any of the security vulnerability that might have been created.

In fact, as I think Mr. Schruers mentioned, you don't even need to necessarily remove the code itself to address this problem to a great extent. You simply need to uncloak it because as I understand the vulnerability that's created, it derives from the fact that some of this code cannot be perceived. So that would leave the code in place, but it would be visible to the user. That is not circumvention. That isn't even uninstallation. But if you are talking about uninstallation, removing the code from the computer, that cures the problem, and that's what people wanted to do. That's what Professor Felten and his colleagues were recommending be done and created tools to do. That is not circumvention as it's defined in this statute.

Second, even if it is circumvention, I

think there's a serious question about whether it's circumvention that's actionable under the statute because as far as the record shows the circumvention to a very great extent was carried out with authorization. It was the, it's the comment of Professor Mulligan, the comment six, that points out all the different places where people offered advice on how to do this, including the sites of artists and record labels.

So I think that has to be taken into account in assessing whether there is a, whether this circumvention, whether access control measures with the description of this class of works have ever been employed in the market to more than a de minimus extent in a context in which the right holder did not authorize their removal. Because if the answer to that is that they have not, then I think the issue is whether we're looking at a situation of isolated harm in the past or speculative future harm, or whether we're looking at something that rises to the level of justifying an exemption.

So third, if it is circumvention and if it is actionable circumvention, our view is that it is, the activity that is in question here is capable of being addressed by existing statutory exceptions,

which is the standards of the Register and her recommendation has suggesting at least great caution on the part of the Librarian, if not a decision not to recommend an exemption. If Congress has already addressed this problem, then that's a pretty strong indication that recognition of additionally exemptions in this area are either unnecessary or contrary to congressional intent.

There has been a lot of discussion here about 1201(j), and I think we've set out briefly in the Joint Reply Comments why we think it is applicable here. Let me just briefly respond to a few of the things that have been said in rebuttal to that, I guess, by some of the previous panelists, particularly Mr. Perzanowski.

First, the title of the section, I don't think that really tells you very much. We looked at the words of the section and the activity that's involved here: accessing a computer, a computer system, or computer network solely for the purpose of good faith testing, investigating, or correcting a security flaw or vulnerability with the authorization of the owner or operator of such computer, computer system, or computer network. I think if you match that language up against what the activity that this

exemption is aimed at immunizing, there's a pretty good fit.

On the question of authorization that has come up here several times from several speakers, including the last two, again, I would emphasize this is a question of, in this section, there's a question of authorization of the owner or operator of such computer, computer system, or computer network. If you are engaging in this type of testing on your own behalf, on your own computer, then I think you have the authorization of the owner or operator of such computer, computer system, or computer network. Even if you're doing it for somebody else, the authorization in the case of Section 1201(j), unlike some of the other provisions of the DMCA, it doesn't go to the authorization from the copyright owner of the work that is protected by an access control measure. It's the authorization of the owner of the system, and I think that criterion was met here.

I think the citation of the Reimerdes case doesn't tell us very much because I don't believe there was any allegation in that case that CSS, the Content Scramble System, created any type of security vulnerability that needed to be addressed by Section 1201(j). Mr. Perzanowski pointed to the factors that

are listed here in Section 1201(j)(3), and I would emphasize that in the text of that section it talks about factors to be considered. When Congress wanted certain criteria to be met as an ironclad rule in order to qualify for an exemption, it knew well how to say so. It said so, for example, in Section 1201(g)(2), which specifies permissible acts of encryption research, and it sets out criteria there that have to be met.

Then it says in 1201(g)(3) factors in determining the exemption. So here are a number of factors that a court can consider. That same language is in 1201(j)(3) in determining whether a person qualifies for the exemption under paragraph two, the factors to be considered shall include. It's not an exclusive list but it is an indicative list of some of the factors the court could take into account.

If it is the case that what Professor Felten was aiming to do or what others wish to do who are seeking this exemption, if it's the case that it doesn't match up so well with 1201(j)(2), I don't think that's fatal to the issue of the defense there since these are factors. I should say 1201(j)(3), which is where the factors are listed.

And, finally, on 1201(j), I think there's

some confusion about whether the underlying work is the threat here. I don't see that it is. In the Sony BMG case, we're talking about 113 in total, this is all three technological protection measures that have been alleged to be problematic here. There's the XCP, and there's two versions of MediaMax, and there's 113 titles in total that have been identified in the settlement of that litigation as having been issued with these protections.

So I don't think the issue here is that "A Static Lullaby" by Faso Latito or Alicia Keys Unplugged or Art Blakey's Drum Suit is really threatening the security of America's computer networks. The concern was about the technological protection measures, so it's not the issue of getting at the underlying work because it constitutes the threat I think is a red herring here.

And, finally, if this is circumvention, if it is actionable circumvention, if it is actionable circumvention that's not capable of being addressed by existing statutory exceptions, then I think the office has to look at the question of the impact and what is the impact on non-infringing use of the presence of these exceptions. And I think the submission from the Samuelson Clinic really laid out four non-infringing

uses. I think we've responded to those in our Joint Reply Comment, the clear non-infringing use here versus listening to the recording. I think it is worth pointing out that in the Sony BMG case every title that was affected, every compact disk that was involved here could be played on a stand-alone player, could be played on a car stereo, could be played on a computer hard drive even after uninstallation of the software, and, perhaps most importantly, could be played on a hard drive or on a portable device after being downloaded from the internet. To my knowledge, every title that was affected by this controversy was also available for legal download from sites such as iTunes and the many other sites that are now or many of the services that are now available to provide this.

Now, I hasten to add those services do have technological protection measures associated with them. There is DRM associated with them. But it's DRM that does allow a degree of copying, a degree of format shifting and platform shifting and so forth. And certainly the use that the people wanted to make to listen to the music was completely achievable through that method. So the fact that there were 113 titles to which this problem, in which this problem

has been raised, I think you would have to look at the availability of other ways to achieve the desired objective with respect to those titles, and I think you would find that it certainly was accessible.

I think besides assessing the, qualitatively, the arguments that non-infringing use was seriously impacted in this area, I think you also have to look at the quantitative side of this, which, of course, the Office did, in 2003, when issues regarding access controls on compact disks, on sound recordings were raised the first time. You found then that I believe it was 0.05, the evidence was that 0.05 percent of the titles that had been released in the market might have had some type of technological protection measure associated with them. And I think you properly judged that to be de minimus.

I think what we're looking at here is 113 titles, and I'm advised, I don't have the figures for 2005 unfortunately, but for 2004 there were 44,476 titles, albums released in the United States. So we're looking at about one-quarter of one percent of all the titles that are involved. So I suppose if you get to this point in the analysis, if you conclude that this is circumvention, that it is actionable circumvention, that it's not capable of being

addressed by existing statutory exceptions, and that there has been some discernable impact on non-infringing use, then I think you have to get to the de minimus question and decide whether the change from 0.05 percent, that is one in 2,000, to 0.25 percent, that is one in 400, makes a difference.

I think you also have to, of course, take into account the climate that we are living in now, and I know there have been a number of references to the settlement that has been reached between many of the plaintiffs in the lawsuits that were brought and Sony BMG that includes safeguards and procedures that will be followed before the introduction of technological protection measures by that label in other context, and I think that also ought to be taken into account.

I'll just briefly mention the issue of 1201(i). I'm pleased to hear from the other panelists or some of the other panelists that the recognition that the only information that was collected in the Sony BMG situation was the IP address of the computer in which the CD had been inserted and that this is probably not personally identifiable information. That makes 1201(i) obviously not relevant in this case because it deals with the undisclosed surreptitious

collection of personally identifiable information.

And I think the conclusion that the Office might draw from that is that Congress, having addressed this issue, having looked at this issue, decided this is as far as we want to go in allowing circumvention in situations where there is collection of information, and it's not disclosed. We want to provide a remedy in a situation in which what's collected is personally identifiable information. But Congress declined to provide a remedy in the case where there's the collection of information that's not personally identifiable information. I think this is a situation where, as in the 2003 proceeding, it would make great sense, it would make sense for the Office to exercise great caution in its recommendation for providing us an exemption that goes beyond the statute in an area in which Congress did obviously consider enacting the statute.

Finally, I'd just like to conclude by noting that many of the submissions on this topic really are calling for the Copyright Office to make a statement to the Librarian of Congress to send a message and to express disapproval of what Sony BMG did or did not do in this particular case. I would submit this is the wrong place to be sending that

message because this is not an issue of circumvention or actionable circumvention or actionable circumvention is not addressed by an exception. That doesn't mean that there is no public policy issue here. It does not mean that cyber security is in the hands of the copyright lawyers. There are many other avenues to address these questions, and there is certainly many other laws that may be relevant in this circumstance, and that's why lawsuits were filed against Sony BMG in a number of courts on a number of theories, none of which had to do with Section 1201 or with copyright. But there were allegations of violations of a number of other laws which are on the books in effect, and the courts are open and sitting to adjudicate those claims.

The suggestion, for example, in one of the submissions that one of these technological protection measures constituted spyware. If that's the case and if there's a law against spyware, then it needs to be evaluated based on, it needs to be lined up against the criteria for spyware in that statute and, presumably, if there is a law against spyware, there are also legal remedies that apply in that case.

What the Copyright Office recommends or what the Librarian of Congress does in this situation

really has no impact on that and should have no impact on the question of whether or not what Sony BMG did or did not do violated any law or violated anybody's rights. The issue for the Copyright Office in its recommendation and, ultimately, for the Librarian and his decision is whether a case has been made that the prohibition on circumvention of access control measures is inhibiting the ability of people to make non-infringing use of, in this case, sound recordings with these technological protection measures and, if so, to what extent whether that is an isolated problem or whether it's a problem that's likely to recur in the future.

That, I think, is the question that's before this panel, ultimately before the Librarian, if not the issue of sending a message or making a statement. Thank you very much.

REGISTER PETERS: Thank you. We're going to turn to questions of the Copyright Office, and we're going to start with Steve Tepp.

LEGAL ADVISOR TEPP: Thank you. Let me begin just by confirming what I don't think will be controversial, that Section 1201(a)(1) prohibits the circumvention of any measure that effectively controls access to a work protected under Title 17,

copyrightable work. Am I correct that no one would take issue with that reading? Okay, good.

Then my first question is what is the copyrightable work that is protected, and what is the technological measure that controls access to it? Because we've talked a lot about a general situation and some general dissatisfaction, but I'm still not clear on exactly what is the work and what is the access control, so please help me out.

MR. PERZANOWSKI: From our perspective, the work at issue here, the copyrighted work are the sound recordings, the raw CD audio files that are contained on these compact disks. The protection measure at issue here varies, depending on the particular deployment that is used by the record labels. But, in general, they share the characteristics of being active software protection measures, you know, pieces of code that are installed on computers and, once they are installed, they restrict access to the underlying copyrighted work.

Now, in some cases, it seems that the protection measure itself may well be, and Professor Felten can correct me if I'm wrong here, the protection measure itself may well be inseparable from the security risk that it introduces, so it may not be

so simple as removing the security risk while leaving the protection measure intact.

MS. CARNEY: And Sony in this case, and I can't speak to the others, it was a rootkit, which is on a computer the equivalent of replacing the man behind the curtain with a new man, and that means that at the heart of your computer the thing that approves or disapproves of whatever software asks to do was compromised by Sony so that Sony could protect its works by, say, preventing them from being put on iPods or being ripped to MP3. And I know it's complicated. If anybody has a better explanation . . .

MR. FELTEN: Without addressing the legal issue of what is or isn't a technical protection measure from the 1201 standpoint, I can talk a little bit about how these technologies at issue in the Sony, in the two Sony technologies worked. Both of them involved several interlocking parts, if you will: a so-called device driver, which is installed on the computer and tries to regulate which programs can read information off the compact disk; other software which uses that, other software which is designed to sort of turn on and off that function of allowing access; and some player software, which, in some cases, applies rules to try to limit or control which uses the

consumer can make of the work once it's been read off the disk.

So it's a complicated technology with different moving parts, and I'd hesitate to give you a cartoon description of exactly what the technical measure is. I do want to say, though, that the assertion that a rootkit is the only problem here, the only protective measure, or the only source of security vulnerability is not correct. There are other aspects of these systems that do involve, that do involve both attempts to limit or control use of works and which do, as well, introduce security problems.

MR. SULZBERGER: Very shortly. This is a somewhat complex statement. You've often heard mention that I think copyright has been misused to prevent people from decompiling the Microsoft operating system or pieces thereof in publishing and doing research. By the way, let me just mention the good that would come of legally permitting this is already clear in the past few weeks. There was a bad bug in a piece of Microsoft code, and two companies issued patches before Microsoft could. Their patches, of course, were in the form of source code. People could look at it. There's still problems because the

law has allowed vendors of operating systems to prevent people from setting them.

Just quickly to address and relate what I just said to your question. There are two pieces. I'm reminded by my colleagues. There's the work in most of these cases. Alicia Keys is singing a song and the recording of that, and there are then bits of code, which are conceptually distinct and distinct in various ways and, of course, the law can distinguish them, I think, pretty easily.

But those pieces of code are themselves under copyright, and, as copyright, it's practically interpreted under our present legal regime. It's the issue in general of publication. If I find something really wrong and it has nothing to do with copyright here but something except the rule that you can't decompile and publish stuff. Obviously, I've got a right, I think, to decompile and publish anything running on my machine if I hadn't gone out of my way to grab it just to do that, if it's the only thing I can buy at the store and it's doing something I don't like.

So what happens is you have a mutually reinforcing impairment of my rights of both free speech and my right of private ownership. Anyway,

because it happens because copyright law is incident in two levels, incident at the DMCA for power copyright law and then copyright law itself, the business about I'm not allowed to decompile and publish.

I just want to make one statement in praise of Steven Metalitz's recognition of the importance of private property and rules against invasion of it, which I liked. Thank you.

LEGAL ADVISOR TEPP: Thank you all. I didn't hear any disagreement with Mr. Perzanowski's assertion that the underlying copyrightable work is the sound recording, or I guess you've also mentioned audio visual works, so I'll just incorporate that as well.

MR. SCHRUERS: If I may, I'm sorry.

LEGAL ADVISOR TEPP: Please.

MR. SCHRUERS: Maybe this goes without saying, in this case the underlying copyrighted work is the sound recording. That's happenstance. You know, it's not clear with future works you could have, as was suggested, more closely intertwined works and protective measures, in which case it may not be immediately clear how to distinguish them.

And so as I say, it's just happenstance

that in this case the underlying work is a sound recording. But, you know, in the Sony example I think we agree on that. But looking prospectively, I would not be comfortable saying that we will always be able to say there's a work and then there's a protection measure, and the protection measure is the problem, and the work is just a WAV file.

MS. MULLIGAN: Does your question go to the point as to whether or not the technical protection measure itself is being considered the work?

LEGAL ADVISOR TEPP: No. Well, it might. I mean, first I'm trying to identify what the work is and then, more to the point, what is the access control?

MR. METALITZ: Could I clarify? Are you asking what is the work in the exemption that's proposed? What's in the proposed class of works? Or are you asking what was the work in the Sony BMG case?

LEGAL ADVISOR TEPP: Well, I'm really asking both because, from what Mr. Schruers just said, it sounded like he's talking about a situation that might extend beyond the proposed exemption, and so I'm trying to figure out if the exemption is, in fact, just about the Sony case and very similar ones, or if

there's a broader matter at issue here.

MR. METALITZ: I think his proposal, it goes well beyond Professor Mulligan's proposal. Professor Mulligan's proposal I think is for the sound recordings and audio visual works associated with them, and I guess one question that I think would be useful to clarify is is it just audio visual works that are associated with sound recordings, such as music videos? Or are you also talking about a broader category of audio visual works?

MR. PERZANOWSKI: The reason that we included audio visual works in the class of works more generally is that, oftentimes, these protected CDs are distributed with what is termed bonus content. Bonus in that you're only able to access it if you install this software. It's sort of a means to entice consumers to put this malicious code on their machine in the first place. So often this is in the form of music videos, for example, and we wanted to make sure that works that included those sorts of audio visual components were also within the class, so we wanted to broaden it slightly from sound recordings solely.

But that said, we did try and I think we succeeded in keeping our proposed class narrowly tailored to address the Sony situation and other

situations that may come up in the future that are factually similar to that problem.

MS. MULLIGAN: This is, of course, a deep desire to appreciate the delicate balancing tests that you're faced with doing and to try to provide -- I think Mr. Metalitz tried to suggest that this was a speculative harm, that what we're talking about here are de minimus risks. And the fact of the matter is that the, you know, extent of damage to the underlying information infrastructure and the potential for this to turn into a quite massive security disaster is something that I think there's a deep desire here to understate. And this is not a case where we're asking you to address kind of prospectively a potential risk. This is a class of works that's narrowly tailored to address a very specific form of harm that has been identified and that had the potential to cause great damage.

LEGAL ADVISOR TEPP: Okay. I want to come back to you, but we have a little bit of a disconnect between some of the different proponents, so maybe it would help to parse it out a little bit and take them one at a time. So let me start with Professor Mulligan, Mr. Perzanowski, and Professor Felten because you're all on pretty close to the same page.

MS. MULLIGAN: To be very clear, we've been representing one of Professor Felten's students for about a year and a half and, more recently, Professor Felten himself. So, yes, if there's any discrepancy, please ask us to clarify because there should be none.

LEGAL ADVISOR TEPP: I wasn't suggesting discrepancy amongst you three, but there is discrepancy between the three of you and what Mr. Schruers and CCI have to say. So with regard to the sound recording and audio visual works as the underlying work, Professor Felten, you spoke about, in fairly general terms, the technological protection measure, the rootkits. What exactly does that technology do that prevents access to the sound recording and/or audio visual work?

MR. FELTEN: Well, I could speak to -- let me try to avoid diving too deeply into the technical details and give you a general summary that applies to both the XCP and MediaMax technologies. And let me note that the rootkit function itself was in the XCP only. MediaMax posed other security problems. But let me describe very briefly how these systems work.

First, they install a so-called device driver, which is a piece of software that tries to

insert itself into the operating system at roughly the point where the operating system is interacting with the compact disk itself and reading the digital music off the compact disk. And this device driver tries to know which program is reading the compact disk at the moment and to either allow unimpeded access to it or to cause either meaningless or garbled responses back otherwise.

So the idea is that if some unauthorized program were to try to read the compact disk, the result would come out garbled because the device driver would garble it. But if some program that was shipped as part of the, that was shipped on the compact disk by the record label were to try to read the compact disk, that would work okay.

Now, bundled with this is a player, is a music player application provided by the record label, which, when it's working right, allows the user to press the play button and listen to the music and, in some cases, allows the user to make limited copies and so on. In addition, on some of these technologies, there's a third general category of software which tries to frustrate removal of the first two, tries to frustrate users' attempts to remove the first two. And the rootkit is one example of that. It tries to

cloak aspects of the first two software components so that users have a harder time removing them so that antivirus or anti-spyware programs have a harder time finding them and so on. That's a general sketch, which I hope is sufficient.

LEGAL ADVISOR TEPP: It's helpful. Let me focus in on the aspect that you described wherein unauthorized software, from the perspective of the software included on the CD, will result in a garbled playback of the underlying sound recording.

MR. FELTEN: That's the intention anyway.

LEGAL ADVISOR TEPP: Under what sort of circumstances might an authorized user of the compact disk encounter that sort of access control?

MR. FELTEN: If the user, for example, tried to use their ordinary, the audio jukebox program that they ordinarily use, for example Real Player or some such or even iTunes, to play the compact disk, they would get that result. You get that sort of garbled result. The music sounds terrible.

MS. MULLIGAN: Can I just prompt you because I think you actually probably know the statistic but, to the extent that people are using kind of out-of-the-box, pre-configured computers that are set to have autorun enabled, this will be their

experience unless they accept this program.

MR. FELTEN: That's right.

MS. MULLIGAN: And that percentage is?

MR. FELTEN: That's the majority of computers as they come out of the box and as users configure them. We've done surveys where we go around the Princeton campus, for example, and try sticking these compact disks into ordinary computers and see what happens, and most of the time the result is that the jukebox or music player software which was configured to run ordinarily will try to play the disk and get a garbled result.

MR. PERZANOWSKI: So I think it's important to point out that in the scenario where we have these three separate components, all of which in conjunction operate as the technological protection measure, so they don't work independently of each other. They all sort of fit together, and each of them serves an important function in restricting access.

Also, I think it's really important to point out that it's not just the rootkit itself, the cloaking device that creates the security risk. It certainly creates a really big security risk. But the other components, the device driver and the playback

software themselves are capable and, in these cases, have caused additionally independent security vulnerabilities.

MR. FELTEN: That's correct.

LEGAL ADVISOR TEPP: Okay. Surely, Sony wouldn't have sold disks that couldn't be played on computers at all. I don't think that's what you're alleging. It's just that you couldn't use a different playback device than the one that came with the disk; is that --

MR. FELTEN: That's almost right. If Sony's software is installed on your computer, the software that came on the compact disk, then that software is the only software you can use to play the -- let me back up. If Sony software that came on the compact disk is installed on the computer, then ordinary music player software will not work and only the Sony music player software will work. On the other hand, if Sony software were never installed on the computer or if it were installed and then removed, then an ordinary music player will work. So a user who succeeds in removing the Sony software will be able to play the music with their ordinary music player. So it's not the case that the Sony software enables access to the music. It's more accurate to

say that it blocks access to the music by other plays.

LEGAL ADVISOR TEPP: Is there any circumstance then under which an authorized user of this CD, using it on their Windows-driven PC, would not be able to play the CD either through the Sony driver software that came with the CD or through some other software, if that Sony driver wasn't on their computer for whatever reason?

MR. FELTEN: The scenario where the Sony software is installed on the computer and it raises a security risk such that playing the CD is dangerous, then the user's only option to listen to the CD on that computer is to first remove the Sony software. And that's the scenario that I was talking about before. Once the Sony software gets on the computer and if the user is unwilling to face the security risk, then their only option to play the music is to remove the Sony software.

MR. PERZANOWSKI: I think there's another scenario where playback would not be possible. So one thing that I don't know that we've made perfectly clear yet, the device driver at issue here is installed using the autorun feature on Windows. So you put the CD in, and before you do anything, before you click "I agree," before you touch any button, that

device driver is loaded and is restricting access to the music on the CD.

Now, after that point, when the user is prompted with the installation program for the rest of the software, some of which has already been installed, if the user declines that installation with the device driver installed, it just spits your CD back out and essentially tells you, "Sorry, you're out of luck. Go use a different device to play this back." So in that scenario, if the user is unwilling to agree to the software installation, which has already occurred, they're just out of luck and they can't listen to the CD on that machine.

LEGAL ADVISOR TEPP: Let me make sure I understood that. The software installs itself before the EULA, then, if the EULA is declined, the CD spits itself out?

MR. PERZANOWSKI: That's right.

MR. FELTEN: Correct. Although in MediaMax, if the EULA is declined, the software stays installed and continues to run in most scenarios.

MS. MULLIGAN: So you get the security vulnerability and no access, to be clear.

LEGAL ADVISOR TEPP: So is the access control the driver to the EULA, the EULA click-through

to be precise?

MS. MULLIGAN: It depends on whether or not you're talking about actual access or conceptual access. These things certainly merge, and, to the extent that you decline the EULA, it leaves with one version, the disk gets spit out, but the technological protection measure that would have limited your access, unless you were willing to accept the security vulnerability, remains on your machine.

LEGAL ADVISOR TEPP: Okay. I think I understand where you're all coming from. Ms. Carney, did you want to add something?

MS. CARNEY: I wanted to echo Professor Felten's comment that, while the Sony rootkit is the most public example of this, it's certainly not the only one. And I think by focusing on the Sony rootkit, it's important, but it's also important to look at the broader question of whether I, as a consumer, should be forced to install a special player software to play a CD which I lawfully purchased and, you know, I've paid my money and I've purchased that content.

MR. METALITZ: If I could just add, the description you just heard about the EULA, about installation of the XCP prior to presentation of the

EULA is not what is stated on page four of the submission that proposed this exemption, which states that if the consumer accepts the EULA terms, and I will note that it puts the word accepts in quotation marks, these protection measures install software that the consumer may use to play the CD and copy DRM protected Windows media files. And if they don't, if they refuse the EULA, then this is not installed and they don't play it on the computer.

MR. PERZANOWSKI: That second statement does not actually appear in our comments. Your first sentence is an accurate quote, and it's true.

MR. METALITZ: My point was I think that's different than what I just heard stated about five minutes ago.

MR. PERZANOWSKI: I don't believe it is. Let me explain. It is true that if the consumer accepts the EULA there are some additionally software programs that are installed. However, it is also true that, regardless of whether or not the EULA is accepted, some of the software has already been installed. Those two statements are in no way logically inconsistent.

MR. FELTEN: And that installation before without consent happens automatically as a consequence

of inserting the disk into the computer in the first place.

MR. PERZANOWSKI: So our statement may have been unclear, but I hope that we just clarified it.

MR. SULZBERGER: Mr. Tepp, actually, I was laughing when you said what's the protective technological measure. You said is it the software or is it the EULA. It's a slightly logically complex thing. Some software goes on there no matter what you do. Then if you say "accept," other software goes on there which, in cooperation with the software already installed, allows you to play this particular CD through your computer system. If you say no, it doesn't remove the stuff that was put on that could cause trouble, but it also doesn't install stuff that allows you to play the CD. It spits it out. I'm laughing because it's absurd at many, many different levels.

But just to get in my usual rant, it's the whole climate of opinion here that allows EULAs that seek under copyright law to tell you what you can use something you bought and own. I don't believe those EULAs would actually stand up, but I think nobody is willing today to go to the Supreme Court.

And then, of course, once again, I don't want to get distracted, although that is the intention of some people here, by issues of access. Look. We're talking about serious collateral damage. The damage done to people is not that they can't access the work. That's a minor damage. And even if it's only 113 titles -- what's the number? What's the undisputed number of machines infested with this stuff? Five hundred thousand? A million? What is it? That's the issue.

And if the DMCA, we need an exemption, then I think we do. To stop that kind of damage in the future or to dissuade a big company with deep pockets from putting out such malware, yes, let's get the exemption.

LEGAL ADVISOR TEPP: Mr. Schruers, I promised to come back to you, so I'll do that now. As I read CCIA's written submission, it looked to me like you conceded that the argument being made by Professors Mulligan, Felten, and Mr. Perzanowski are actually not access controls, but you had a deeper concern. So let me --

MR. SCHRUERS: Well, what I actually would like to say is on this -- let me first clarify the scope of the work. I hope that the previous exchange

didn't create the impression that the exemption that we sought is limited specifically to sound recordings and audio visual works. I mean, that is, as I said before, just happenstance, and the class of works that could be relevant under these circumstances could be broader than that. Tailoring the exemption to those circumstances would sort of be a backwards-looking exemption.

And for that reason, the exemption that we sought includes, for example, computer programs and compilations which could, even in this particular circumstance, be protected by the access control. And it's possible that there's bonus material on the CD that is neither sound recording nor an audio visual work. And going forward, there's no reason to expect that we couldn't be dealing with a technological protection measure on a computer program, a visual video game, a compilation, or so on.

So I want to dispel the idea that we're only, at least that CCIA is only concerned about protection measures on sound recordings or audio visual works. Did I answer your question?

LEGAL ADVISOR TEPP: Part of it, yes. So thank you for that, but let me follow it up with what is your view, CCIA's view about what is the access

control? And when you answer that, please describe not only what the technology is but how it controls access to any of the underlying works that you've just enumerated or could theoretically.

MR. SCHRUERS: Having heard Professor Felten, I'm weary to contradict anything that he would say on this matter because, obviously, his computer expertise is broader than mine. But we need to recognize that there are, there's the possibility of separate access controls, which are applications that stand alone from, in this case, let's use it because it's easy, a stand-alone sound recording or audio visual work, which is the application which happens to be protected by a EULA but need not be.

There are also cases where, and a number of comments identified this, the work protected by the access control could be more closely intertwined with the access control and sort of trying to disentangle those would sort of become an exercise in legal philosophy. You know, it's sort of devising arbitrary limits.

So we need to recognize both those situations in devising an exemption. And for that reason, I would say that our comments seek a broader exemption to be recommended by the Office.

MR. FELTEN: If I could comment on this point with respect to the CCIA exemption request. It's worth noting that there are protection measures on the market now on some DVDs and on some computer games which rely on the installation or automatic installation of software onto consumers' computers when they insert the DVD or the medium containing the computer game. And in the case of computer games, I think the CCIA's point that it may be difficult to distinguish easily between the underlying work, namely the computer game software, and the protection measure software that comes bundled with it is a well-founded concern. I haven't studied that technology carefully enough to say whether it is or is not the case, but I think it's a well-founded concern in that context.

MS. CARNEY: I would also like to make a short note. I think it's important here to recognize that EULAs, with respect to the average consumer, are almost incomprehensible. And for a consumer to really understand what kind of privacy they're giving up when they install a program, most of the time in my work I see that they don't. They click something that essentially says, "I send all my web traffic through you and you can see whatever I do," but they don't understand that. All they understand is they had to

click "I agree" to get through this program. So I don't think EULAs are a very good protection for the consumer.

LEGAL ADVISOR TEPP: Okay. Let me, we've spent a lot of time on what's the access control. I want to move on a little bit to the level of evidence and examples that anyone on the panel may have that, in the next three years, we're likely to face this sort of issue. Mr. Schruers, I'll start with you this time. Since you've posited some hypothetical developments where it's not only different types of works that are encumbered, I'll say, perhaps pejoratively but not intentionally so, by some sort of technology. And as I read your submission, you acknowledge that, while the Sony XCP was not an access control, the next version of that type of technology could be. So my question is, starting with you, what evidence is there to believe that that is more likely than not a development we'll see in the next three years?

MR. SCHRUERS: I guess I should begin with two preambles. The first is just that there are other arguments that have been advanced that this particular software was, in fact, an access control. And I believe the Office in 2003 suggested that copy

controls could in some situations, copy controls like the software here, could function as access controls. I can't provide a citation for that, but I'm simply observing that those arguments are out there, and I don't think it's within my domain to say that those people are necessarily wrong. Although here, this software did appear to function primarily as a copy control.

Then the other preamble is I don't want to appear to concede our position that the Office's burden of proof, more likely than not, is correct. Our exemption did say that Congress's use of substantial evidence, and some of the other commenters, even those opposing our exemption, refer to substantial evidence, and the Copyright Office's reference to substantial evidence in the Federal Register Note is not the same as a preponderance of the evidence, and the DC Circuit has actually said it's less.

But setting aside whatever burden of proof is applied, I would say the similarity between this situation and only a slight tweaking of these facts into another hypothetical should be enough to convince us that we've dodged a bullet. And if it got any closer to reality, we'd sort of be saying, you know,

"Don't buy fire insurance until the house burns down."

So we need to be forward looking in the exemption and see what the number of possibilities are created by the software that we're seeing the market today because the likely development is going to happen at a rate faster than the tri-annual rulemaking can keep up.

REGISTER PETERS: Mr. Sigall has to leave in a few minutes, so what we're going to do is let him ask his questions, and then go back to you.

ASSOC. REGISTER SIGALL: Thanks. I just have two questions and possibly a follow-up on those but, basically, two questions. The first is to Professor Felten with respect to your research into how these technologies work. I understand that most of them rely on the autorun feature of the Windows operating system, and I understand that, in most cases, people do not disable that feature or bypass it when they put the disk in. But in the cases where you have disabled autorun or bypassed it when the disk has been placed into the CD-ROM drive, what has your research shown as to the types of access that the consumer that has in that situation to the underlying musical recording or the audio visual work on the disk?

MR. FELTEN: If the user, every time, if the user either disables autorun or holds down the shift key every single time they insert one of these disks, and I'll note that the disks are not all labeled, so a user who wants to do this would have to hold down the shift key every time they inserted any disk. If the user is able to do that consistently, which I've found they're not -- I myself have installed this software accidentally on a few occasions, I'm embarrassed to say. If the user, nonetheless, is able to do that, then they will have access to the music by other means, yes.

MR. PERZANOWSKI: I would add to that that there is an argument that I certainly wouldn't adopt myself, but I think it's plausible that the mere act of holding the shift key itself could constitute circumvention.

ASSOC. REGISTER SIGALL: Actually, I understand that. Let me ask Mr. Metalitz essentially that question. Is informing people about the ability to disable autorun as a means to avoid the installation of the software or the shift key bypass of autorun at the time the disk is put in, does that create the potential for liability under 1201?

MR. METALITZ: Informing somebody about

something wouldn't create liability under 1201(a)(1), which is the only provision at issue here because that only deals with the act of circumvention.

ASSOC. REGISTER SIGALL: How about the actual act of disabling autorun or bypassing it at the time the disk is put in? Does that create --

MR. METALITZ: Well, we've seen that, going back to the old felt-tip pen maneuver of a few years ago, we've seen that happen quite a bit, and we've even seen, in some cases, copyright owners providing this information. I don't think anyone has ever been sued for it.

MR. FELTEN: If I could just interject here, I think this is a good illustration of the difficulty that we have. That when we put the question to Mr. Metalitz or his clients, we get an answer like that, "We haven't sued anybody yet."

ASSOC. REGISTER SIGALL: My second question, it relates to the applicability of 1201(j). One of the factors that the statute lays out as to whether the exemption may or may not apply is whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement. If this exemption were to apply to the situation that has been described with

the Sony BMG disks that were put out late last year, it would seem to me the most logical way for someone like Professor Felten or his colleagues to provide the information to the consumers to address their security vulnerabilities on what we've heard is 500,000 computers, the logical way to do that would be to post a web site or to provide a place that's easily accessible to give this information.

The question is to Mr. Metalitz. Would providing the information in a relatively public and open forum like the internet or generally accessible form, would that be in a manner that does not facilitate infringement under this title for the purposes of interpreting this factor as weighing in favor of applying the exemption, as opposed to against applying the exemption?

MR. METALITZ: Well, I guess I have to respond only in terms of the particular situation we're talking about here, where there's been some concrete activity, and we can evaluate it in that context. I don't think, I'm not aware of anything that Professor Felten has done in this whole controversy that would argue for the inapplicability of 1201(j) to his activities. And so I don't think any information, for example, that he has posted on

his web site would be, I'm not aware that anything that he's done has been done in a way that would facilitate infringement, so I wouldn't consider that factor to be applicable in this case.

It's a little hard to answer that question in the abstract without knowing more about what the particular measure was, what the information was that was derived, and how it was communicated. But I don't think in this case, to my knowledge, there's no evidence that he has derived any information or maintained it, disseminated it in a way that facilitates infringement.

ASSOC. REGISTER SIGALL: I guess my question is we can conclude that it's possible that the circumstances in which this exemption applies go beyond simply where individual privately-hired security consultants provide that information relatively secretly to their clients, as opposed to someone providing it to anyone who might have this problem and not necessarily a direct relationship between the person who discovered the vulnerability and its correction and someone out there who might be suffering it.

MR. METALITZ: It certainly can in some cases, but I wouldn't want to be understood to say

that in every case posting this information on a web site would not fall afoul of this factor. And, again, I emphasize it's a factor, not an ironclad criterion.

REGISTER PETERS: Okay. Back to you.

MR. PERZANOWSKI: If we could briefly address that last question. Professor Felten did provide on his web site essentially a step-by-step set of instructions for disabling the copy protection and access protection methods, which, if users follow those instructions, are left with completely free access to the copyrighted works on those disks and, certainly, some users can do any number of things, upload them to peer-to-peer networks for example, which seems to me that any sort of public dissemination of that information could certainly lead to copyright infringement.

LEGAL ADVISOR TEPP: I was reminded of two questions I wanted to ask, and then I'll come back to the line that I was pursuing with Mr. Schruers. Professor Felten, is it correct that the CDs that come equipped with this technology can be played in a traditional dedicated CD player without security risks?

MR. FELTEN: Yes, if the user, if the consumer has such a player. As I said before, many

students don't. I don't, other than in my car.

LEGAL ADVISOR TEPP: I understand. Second question is in order to do what you want to do to this technology, deactivating it and/or removing it entirely, do you first have to disable the rootkit, which I gather is the cloak?

MR. FELTEN: Yes. On the technology that uses the rootkit, the XCP technology, yes. Disabling the rootkit is the first step of removing the software.

LEGAL ADVISOR TEPP: Is it possible to disable the software without touching the rootkit?

MR. FELTEN: I'm not sure. It's certainly not possible to protect oneself from the security risk. If it's possible at all to remove everything else without removing the rootkit, it would be considerably more difficult, and we have not figured out how to do it.

LEGAL ADVISOR TEPP: Okay, thanks. All right. Back to Mr. Schruers. We were talking about the likelihood of the developments in this area in the next three years, and, as I recall, your last response had been that essentially we've dodged a bullet here, this could have been worse. Agreeing that the technology could have been slightly different, I guess

my question, and this goes to both Mr. Schruers as well as back to Professors Mulligan, Felten, and Mr. Perzanowski, from what I understand no one is particularly envious of the Sony Corporation in its role in these events. It sounds to me like Sony Corporation has lost money, public relations, suffered public relations harm, and maybe lost some customers on a more long-term basis. So given that, what contravening evidence is there to think that another company is going to rush to fill the gap left by Sony, which has now apparently vacated this space?

MR. PERZANOWSKI: I think the best evidence here is that Sony got themselves into this mess in the first place. Sony did not set out to make this happen, and had you told them in advance that this would be the consequence of deploying this technology I'm quite certain they would not have done it. And, yet, they did go ahead and deploy it, presumably because they didn't understand what the consequences were. And that could equally be the case with some other companies. Sony, in fact, was not the only record company that deployed even this technology. There were others, as well.

So while Sony certainly is sort of the bad guy in this situation, they're not directly

responsible for the creation of these tools. They contract out with these protection measure vendors, Macrovision, SunnComm, XCP. Some of these companies have less than storied histories in this industry. Some of these companies probably won't be around for very much longer, XCP in particular. I doubt anyone is going to be hiring them again any time soon to do a protection measure.

So when direct responsibility is not necessarily in the hands of the record labels that are overseeing the creation of these protection measures and they certainly don't have staff on hand who are particularly well versed in the way that these computer programs function, it seems pretty likely to me that, while no one is going to set out to take Sony's spot here, another protection measure like this could certainly slip through the cracks, and it's going to be these sort of researchers who catch it.

MR. FELTEN: If I could say one more thing, it's worth knowing too that the problems with the Sony technology are far from over. There are many, many disks still out there, and it's still the case that whenever a user inserts a MediaMax disk into their computer they are re-exposed to these problems.

MR. SCHRUERS: Maybe just to finalize, I

guess the question appears, there's this unspoken assumption which I think we should examine, which is that all vendors of access, all creators of access controls care about the public's perception of their access control. And even in the commercial space, it's clear that that's not necessarily the case. Professor Felten and Mr. Halderman's paper, which I strongly recommend on this, indicate that there are different degrees of risk aversion in the industry, and small start-ups have higher degrees of risk aversion and, therefore, a greater willingness to do something potentially stupid.

And then once we move outside the commercial space, again, the sort of the retribution of the public by voting with their dollars doesn't necessarily affect all actors.

LEGAL ADVISOR TEPP: Okay. Mr. Metalitz, did you want to add something?

MR. METALITZ: Well, just to say I think your question is a good one. I think the bell that is rung here cannot be unrung. I think the entire industry is quite aware of the situation. As far as Sony BMG, of course, there is a proposed settlement that would affect what they do as far as rolling out technological protection measures in the future. It

also, just to get it on the record, provides that anybody who still does have one of these disks and hasn't, and wants to return it can do so and get either a replacement CD or a download. It varies depending on the particular disk involved.

So this settlement which Sony BMG has entered into I think seeks to respond to that concern, but I think your question is a good one.

MS. MULLIGAN: Can I just respond briefly? I think if you look at the history of privacy invasions using technology, there's a little bit of a foreshadowing that one can see here. You know, one would have hoped that when Doubleclick got raked over the coals for installing little cookies on people's machines without notice and consent or Microsoft was taken to task or Real Audio for programs that phoned home and provided information about how people were using their computers that we wouldn't have seen those things again in the future. Nobody likes to be on the front page of the Washington Post. Nobody likes to be Sony. Nobody wants to have this experience, but we see it happen again and again and again.

And I think the question here about whether or not someone will accidentally or, you know, without kind of thinking through all of the risks end

up being the next Sony BMG. We can all hope that won't be the case so that there won't be a repeat player.

But I think that whether or not there's going to be a repeat player doesn't tell us whether or not there should be an exemption that says if somebody does do this again that consumers and security researchers can take actions to protect the public, that those things don't have to be mutually exclusive. We can both hope that the industry will proceed in a logical, thoughtful way as they introduce DRM technology and back strap this by saying that, to the extent that they don't, consumers or national information infrastructure doesn't have to be at risk where people act in a hasty and unthoughtful way.

LEGAL ADVISOR TEPP: Professor Felten, let me just follow up on your point about, I used the term reinfection risk. Are the existing patches and uninstall applications sufficient to rectify a reinfection?

MR. FELTEN: If the consumer gets reinfected and if they realize they've been reinfected then they can after some time re-patch and put themselves back into the initial state. But, again, the next time they want to listen to that CD and they

put it into their computer they will get reinfected yet again. The consumer gets infected and has to remember to disinfect every time they listen to the CD, unless they use unauthorized uninstallers.

LEGAL ADVISOR TEPP: Would it be any different if they had this exemption in the law?

MR. FELTEN: Currently, the best way that consumers can protect themselves against this is to uninstall the software using an alternative uninstaller or alternative uninstallation method other than the one that is provided by Sony BMG. If they use other measures besides the authorized ones to remove the software, then they can be protected against reinfection. As to what the legal status of that is, I'd leave that to the lawyers.

LEGAL ADVISOR TEPP: Okay, thanks. Mr. Sulzberger?

MR. SULZBERGER: I think actually we should be clear what a rootkit is, and I should also like to argue that the risks here are not speculative because Intel and Microsoft, which, in effect, control the industry at this level have agreed to place rootkits in all machines sold. They expected to have them by this hearing at the 2003 hearing, but they're pretty incompetent. Actually, Intel isn't. Microsoft

is.

A rootkit is a device by which somebody other than the owner of the machine robustly controls the machine that the owner thinks they're in control of. All hard DRM necessarily includes a rootkit because, otherwise, you do SU space minus, to use some jargon. I'm now going to use incorrect syntax, but I've modified so it will work.

You then say kill all space DRM, and it's off your machine. If you are in full control of your machine, no DRM scheme can succeed. You have to give up control in the ordinary sense.

Now, most people who run a Microsoft system aren't in control of their machines, of course, neither legally nor effectively nor practically. And this hearing is about whether or not the DMCA will be used to effectively remove the right of private ownership of the computer in the next few years. I thought it would have happened by now, but Microsoft is so incompetent, and Professor Felten thinks they'll never be competent in the timescale of five years I think. Am I wrong? If I'm wrong, I take it back, Ed.

And that's the issue here. And details about one incredibly and unimportant harm, even though it affected 500,000 machines, the Sony BMG rootkit.

What this hearing is about is whether you're going to allow you are going to allow your office to take part, to be part of a legal mechanism whereby Americans in a few years, as soon as Palladium is complete and ready to be sold, will be the only operating system for low-cost computers available. Doubtless Apple will go along. It would be wonderful if they didn't.

But that's what this hearing is about, and it's not about details of access and whether they get it some place else or the details of exactly how it works. Nobody has a right to take over my machine under the legal protection of the anti-circumvention clause of the DMCA. If this is not clear, it's only because you are not completely clear on what a rootkit is. A rootkit is a device that takes away your control of your computer from you. That's it. And every bit of hard DRM does that.

Now, there exists, since 2003, we have one example of absolute hard DRM, and I'm in a debate with a few people who cracked the old Xbox. The Xbox 360 is a completely ordinary computer. It's as good as any other computer, except for the fans maybe and maybe the scratching of the disks. It has a nicer CPU and organization of the motherboard, I think, than the X86. It's a cutie-pie of a machine.

Why can't I buy one and install my operating system on it? Why? Because of the anti-circumvention provision of the DMCA coupled with the fact that it's effective. The stuff is hard.

Sony BMG, you hire Ed Felten if you want, and he'll get rid of it from your machine, I'll guarantee, and he'll do it right. Nobody on earth today can remove Microsoft's rootkit from the Xbox360. That's not okay. And if somebody were to discover how to do it, they couldn't publish the results. That's not okay. You should not lend yourselves to this broad of an assault on the rights of private property and the rights of free speech. You just shouldn't do it.

And as I said in 2003, it's within your commission to say, "We now know what a rootkit is, and we want Congress's direction on this because we're not going to be part of this. It's not our duty to decide that the anti-circumvention clauses trump private property."

MS. MULLIGAN: I actually want to suggest that this actually is about access controls, and it's about the installation of security vulnerabilities through the use of this particular kind of technical protection measure. And we're actually not looking

for you to become the policy-making body about trusted computing, Microsoft, Intel, or anything else. We're looking for a very narrow exemption that will protect consumers and enable security researchers to pursue their work without having to talk to me and my students very often. I have no doubt they'll still have to talk to us a minor bit, but this is actually, you know, you are not the right body to consider the future of trusted computing, and we wouldn't ask you to do that.

And I just want to say that, respectfully, we're actually asking for you to do something much more narrow. And I'm actually going to turn some of this back over to Ed.

MR. FELTEN: Again, what we are asking for is a relatively targeted, a relatively targeted exemption which is based on a really detailed technical study of what has happened in the Sony BMG case and, based on that study, a concern about the same issues being important going forward. We spent significant care making sure that our request was tailored to that issue and that we could justify it based on the detailed study of these technologies. We're not asking for a very broad exemption, and we would ask you to take, to look carefully at these

issues. We'd be happy to provide any level of technical backing for this. We'd be happy to provide you with copies of our paper, which details all of our study of this technology.

GENERAL COUNSEL CARSON: Please do provide that to us as soon as you can. That would help.

MS. CARNEY: I think perhaps I'm being cynical here, but the environment that brought out Sony's rootkit is still very much in force. People are still unsure what new technology means for various media industries, and I think it's actually very likely that DRM is going to come out in the future that compromises security, that compromises privacy, and users will again be left with a choice of whether they want to break the law or whether they get to use the content that they purchased.

MR. SULZBERGER: Could I answer Professor Mulligan? Professor Mulligan, what if the method that was in access under the strictest meaning, it was -- suppose a working Palladium appears tomorrow and the curtain is in place and Sony makes a deal with another little company and they do put something that could strictly be considered to be an access control, a technological protection measure under the protection of the curtain. Suppose that the curtain is also used

by people who write frank malware. Let's assume that the access protection just annoys you by not letting you play it when you want to play it or perhaps even commit copyright infringement.

GENERAL COUNSEL CARSON: You can have that conversation afterwards. We're running overtime right now.

MR. SULZBERGER: I'm sorry. Don't you think --

GENERAL COUNSEL CARSON: Excuse me, Mr. Sulzberger, you're going to have to ask him that afterwards.

MR. SULZBERGER: Sorry.

GENERAL COUNSEL CARSON: If we had more time, this would be wonderful, but we're over our time. We still have some really focused questions because we're trying to get some specific information. So I don't mean to squelch you, but we've got to try to get what we need to do what we need to do.

MR. SULZBERGER: Okay. You know what a rootkit is.

GENERAL COUNSEL CARSON: Steve, go ahead.

LEGAL ADVISOR TEPP: All right, thanks. I actually have a lot more in deference to some of my colleagues, including my bosses. I won't ask all of

them, just a couple more. Mr. Metalitz, on the issue of the applicability or non-applicability of 1201(i) as a possible alternate authorization for the type of activity that the proponents here would like to engage in, they have expressed the concern that because information is gathered relative to non-natural persons that that is not a fully sufficient exception, and I'm curious to hear your response to that, if you have one.

MR. METALITZ: I don't think the natural person is the issue. It's whether or not the technological measure collects personally identifying information, 1201(i)(1)(a). And I think it seems to be clear that, in this case, that did not occur and, therefore, 1201(i) really wouldn't have any applicability to this case. My point is that I think it does indicate to the Office or should indicate to the Office that when Congress studied this issue about whether circumvention should be allowed to disable information collection functions, they only went as far as undisclosed functions of collecting or disseminating personally identifying information, reasoning, I think logically so, that this had the greatest threat to privacy and, therefore, you should take that into account in determining the

applicability of 1201(i) or whether you should step beyond to provide some type of exemption that would step beyond the circumstances to which 1201(i) applies.

But I think it's agreed, and I may be wrong and I prepare to be stand corrected, but I think it's agreed that in this case what was collected was an IP address and that's generally not considered under U.S. law personally identifying information.

MR. PERZANOWSKI: Our position would not necessarily go so far as to say that an IP address is not personally identifiable information. I think we agree that 1201(i) does not apply. I think we disagree on the precise reason that it doesn't apply. I think an IP address could constitute personally identifiable information, but it's certainly not information about a natural person. But I think in the end we come to the same conclusion on that point.

LEGAL ADVISOR TEPP: Okay. Well, let me jump to 1201(j) and ask Mr. Perzanowski when you were making your initial presentation you quoted in part from the language of 1201(j), and Mr. Metalitz pointed out that, and it occurred to me as well as you were reading, that your quote ended before you got to the word "correcting" for the solely for the purpose of

good faith testing, investigating, or correcting. And, further, as some, I can't remember whether you raised this, but I know several of the panelists did, that the concern that the authorization of the copyright owner in the underlying work be required where it appears that the statute actually requires the authorization of the owner or operator of the computer, computer system, or computer network, which presumably is the person who is actually doing the circumvention or has authorized it. So I just wanted to get your reaction to that in terms of the applicability or non-applicability of 1201(j).

MR. PERZANOWSKI: I think both of those points support the notion that Section 1201(j) is intended not to protect or not to exempt circumvention of protection measures that protect copyrighted content on removable media but that, in fact, the whole purpose of Section 1201(j) is to allow circumvention of technological measures that are designed to protect a computer itself. So certainly the authorization to circumvent a protection measure that protects a computer needs to come from the owner or operator of that computer. But if you look at the Reimerdes case, there the court read Section 1201(j) when applied and likely misapplied to a circumstance

where the protection measure was not designed to protect a computer, computer system, or computer network but removable media that the authorization had to come from the copyright owner.

Now, it also seems that the computer, computer system, or computer network that is at issue in Section 1201(j) necessarily contains copyrighted content. Often, that copyrighted content is going to be copyrighted content where the rights are held by the computer owner or operator. So in that circumstance, I think that distinction sort of collapses and we're left with a scenario where authorization has to come from the person whom the protection measure was designed to protect. I hope that answers your question.

LEGAL ADVISOR TEPP: Well, I'm still a little confused, I have to admit.

MS. MULLIGAN: The argument that the permission or the authorization has to come from the owner of the computer system basically makes our point perhaps better than we did. What we're talking about here is removable media that's been put into the system, not the system itself, and that the way in which this entire exemption is crafted, it's about a computer system, you hire somebody to come in and

install a firewall and then do security testing, either they bring in a red team, they do some kind of penetration testing of your system. It is not talking about the actual content that the DMCA was designed to protect, these creative works --

LEGAL ADVISOR TEPP: Just a second. I understand what you're saying, but I'm perceiving a disconnect between that response that you and Mr. Perzanowski have just provided and what I hear is the general theme of all the proponents on the panel, which is it may originate on removable media but it's deposited on the hard drive of a computer or computer network and it's taking control of people's computers and it's putting people's computers at risk for security problems. So let me say this: rather than talking about broad philosophical or intentional applications of 1201(j), can you please take me through the actual text of the exception and explain to me why that wouldn't work? Because as I read it, accessing a computer system for the purpose of correcting a security flaw or vulnerability sounds a lot like what you want to do.

MR. PERZANOWSKI: Well, I think it may be helpful to clarify the point that you just made. The protection measure is installed on the computer. The

underlying copyrighted work remains on the removable media, so it's not actually part of the computer, the computer system, or the computer network.

So I think, although Section 1201(j) does talk about, as you note, testing and investigating and correcting security flaws, they are security flaws that are inherent to the system itself, not security flaws that are introduced because of removable media.

LEGAL ADVISOR TEPP: Where do you see that in the statute? Well, all right, I don't want to take up time. If there's something there that I'm not seeing I'm sure there will be a post-hearing opportunity for some sort of submission.

GENERAL COUNSEL CARSON: I don't want to interrupt you, but I'm going to because I want to follow up on your question.

LEGAL ADVISOR TEPP: Okay.

GENERAL COUNSEL CARSON: That's why I want to ask it now. So we're talking about a protected measure which is originally on this removable media. It gets installed on to the computer I gather. Everyone accepts that's what's going on, correct? All right. Is that protection measure, once it's installed on the computer, is it in any way controlling access to, in the words of 1201(j), the

computer, the computer system, or the computer network?

MR. PERZANOWSKI: It is not controlling access to the computer, the computer network, or the computer system. It's controlling access to the underlying copyrightable work that is on this removable media.

GENERAL COUNSEL CARSON: Everyone agrees to that?

MR. SULZBERGER: No, of course not. The rootkit prevents DIR from working. That's controlling access to the computer. Really, this is extreme. If the rootkit is part of it, then it ruins DIR. DIR is your main means of access to files on the machine. It's controlling access to the machine. Am I right?

MR. FELTEN: The rootkit is only present in one of these two Sony technologies, and it's only part of the total picture of how the protection technology works.

MR. SULZBERGER: Is the rootkit on there, and does it disable DIR?

MR. FELTEN: It depends on which system --

MR. SULZBERGER: Either one under discussion that does that?

MR. FELTEN: There is one technology that

uses a rootkit, yes.

MR. SULZBERGER: And the DIR doesn't work, it doesn't show you certain files, names of certain files when you run it?

MR. FELTEN: When the rootkit is running, there are certain files that are harder to see.

MR. SULZBERGER: Right, okay. End of my case.

MR. FELTEN: This is one of the things that this technology broadly does in one of the two technologies at issue.

MR. SULZBERGER: I understand exactly why they want to say it doesn't because then Counsel Metalitz will say, "Well, look, you already got it because it's controlling access," but it's important that we understand the thing does take over and control access.

GENERAL COUNSEL CARSON: To be clear, if I understand what I've just heard, it's controlling access to certain files on the computer. Is that accurate?

MR. SULZBERGER: That's the mechanism by which the computer runs and is under the control of the individual. Sorry.

MR. FELTEN: The effect of the rootkit is

to make some files on the computer, not the underlying audio works, but some other files on the computer either invisible or more difficult to access. But it's not --

MS. CARNEY: I think what's being confused here is what the rootkit could be used for and what DRM rootkits are normally used for. Normally, they're narrowly tailored to do the CD or DVD or whatever work they're trying to protect. But potentially, yes, they can be abused to protect other things.

MR. SULZBERGER: If DIR doesn't work, that's a severe disablement of the workings of the operating system I would say.

GENERAL COUNSEL CARSON: Professor Felten?

MR. FELTEN: It does limit the ability of software to do some of the things it wants to do in the system where the rootkit is present, yes.

LEGAL ADVISOR TEPP: I'll reserve whatever questions I have left for a possible second round so that other people can join in the conversation here.

REGISTER PETERS: We're going to you, Rob.

LEGAL ADVISOR KASUNIC: Okay. Well, I'm torn as to which place to start, but let's go back for a minute to just how -- and I do want to focus on the XCP system because that's something we have some more

specific facts about. And I guess one place to start would be are you all aware of the Mark Russinovich's blog and his analysis of this? Because just so that you have it, I'm going to give you copies so we can at least be talking about the same software and thinking about one context that has been published in which information about what the problems were and how he ultimately got around this were achieved.

Okay. Stepping back for a minute to how this might work, so if I placed one of my CDs that were protected by this XCP content protection system, a Trey Anastasio CD, Frank Sinatra, or one of the other 52 CDs that are protected when they were released by that system into the computer in order to play it, initially, if the autorun feature was enabled, that would install the rootkit software into the computer initially?

MR. FELTEN: That would run some software on the computer and then, depending on whether, and assuming that the user agreed to the license agreement, it would then install the rest of the XCP software, including the rootkit.

LEGAL ADVISOR KASUNIC: And in agreeing to that, part of that would be installing a proprietary Macrovision player?

MR. FELTEN: Not Macrovision.

LEGAL ADVISOR KASUNIC: Macromedia player. Wasn't that the type of player that was actually used?

MR. FELTEN: I don't believe so. I believe it was from First4Internet.

LEGAL ADVISOR KASUNIC: Okay. I think that's what it was delivered from, but it is from what I handed you. That was what some of the evidence was. And I will note, too, that this blog entry was introduced into the record not by me but by three of our initial comments, in comment 3126 and 18. It was footnoted, and let me just take a moment to appreciate when people introduce some of the factual evidence like that that helps us understand how this might work.

So if you agree to the EULA, then it would install some type of player software that would be the way that you would access the copyrighted sound recordings?

MR. FELTEN: That's one of the things that would install, yes.

LEGAL ADVISOR KASUNIC: Okay. If I did not allow that, if I had the autorun feature disabled, would I be able to play that with any of my existing players on my computer?

MR. FELTEN: In that scenario, you would, yes.

LEGAL ADVISOR KASUNIC: So as long as I had autorun disabled as the default or if I pushed the shift key when I put that CD into the computer, I had unfettered access?

MR. FELTEN: If you did that every time and if you knew in advance to do that.

LEGAL ADVISOR KASUNIC: But if I had it set as the default, then, okay, let's ignore the shift key for a minute. If I had the autorun feature set as not running as the default, there's no access issue?

MR. FELTEN: If autorun is turned off, you can access the disk, yes.

LEGAL ADVISOR KASUNIC: With any player I had on my computer? iTunes, Real Player?

MR. FELTEN: That's correct.

MR. PERZANOWSKI: If I could add to that, the bonus content, the audio visual content, and I believe, on some CDs, additionally auto content is only available if the software is installed. So for those bonus videos, for example, unless you install the software by agreeing to the EULA, you'll never have access to those particular --

MR. FELTEN: So if you look at the fifth

page, the front of the third page, there are two images here, and the one on the bottom is the image of the player, and you see the tab for bonus content. You see the tab for bonus content that you could click to get that, and that would not be available to you except by using this player.

LEGAL ADVISOR KASUNIC: Okay. So if it wasn't set, it would limit certain access to the content that was on the CD?

MR. FELTEN: Well, access to that bonus content.

LEGAL ADVISOR KASUNIC: That particular bonus content. Now, the default setting for autorun, is that how Windows comes pre-set?

MR. FELTEN: With autorun enabled. That's the default, and that, in our informal studies, we found is the predominant state.

LEGAL ADVISOR KASUNIC: Okay. Mr. Metalitz, just leaving aside the issue and we might want to get back to that with the shift key, but if somebody, when they purchased their computer shows to change the default settings across the board and disable autorun on the computer, do you see any violation of 1201 if someone then puts a CD in that was geared toward someone who had the default setting

in a different context?

MR. METALITZ: I guess my initial reaction to that scenario is that it's questionable whether the access control has even been installed in that case and, therefore, I'm not sure that any of the verbs that are in 1201(a)(1) about bypassing and removing and so forth are necessarily applicable.

LEGAL ADVISOR KASUNIC: Well, if it could conceivably fall into avoiding it, but if you're doing it even before you put that CD or even purchase that CD or any knowledge of that, then it would seem like it's hard to make a case. So what if software, do you think that it would be a proper software system that would automatically, if I disabled autorun feature on my computer, and this is hypothetical, but if the software on the CD changed my default setting to an autorun setting and required this to be installed on the computer, would that fall within a protection system that would be covered? Could a copyright owner do that?

MR. METALITZ: A copyright owner could do that. That's not a question of 1201, that's a question of what are the features of an access control measure.

LEGAL ADVISOR KASUNIC: But if they did

that, it would fall within an access control feature.

MR. METALITZ: Yes. An access control could have a feature of changing settings on your computer or it might not. I mean, I'm sure there's different ways to do it, but the fact that it changes settings on your computer doesn't disqualify it from being an access control measure, if that's your question.

LEGAL ADVISOR KASUNIC: Okay. What about if someone published information about the safest course of action for computer users would be to disable the autorun feature on their computers, do you think there would be any problems? It might be a little outside of 1201(a)(1), but do you think there would be any 1201 problem generally there?

MR. METALITZ: Well, that gets into the question of whether someone who publishes information about how to do something is providing a service, which is the 1201(a)(2) question. You're correct that it wouldn't violate 1201(a)(1).

LEGAL ADVISOR KASUNIC: But does it make any difference if they're providing a prudent service for all consumers that would protect security generally?

MR. METALITZ: Does it make a difference

as a practical matter as to how likely it is they would be sued under 1201(a)(2)? Yes, I think it probably would. But I can't really answer in the abstract whether someone who posts these instructions is violating 1201(a)(2), and I would also, of course, suggest that it's not relevant to this proceeding.

LEGAL ADVISOR KASUNIC: Okay. Then specifically with XCP, if we're in agreement that it would be all right to change the default setting, what is the realistic difference between the knowledge that you can manually change that feature with the shift key whenever you want?

MR. METALITZ: What is the difference between? I'm sorry, I didn't --

LEGAL ADVISOR KASUNIC: Manually changing that autorun feature with the shift key, would that violate 1201(a)(1)?

MR. METALITZ: Well, I think the same issue would present itself, which was whether the access control had been installed. I'm not sure there's a difference between what you do to prevent its installation is something you do manually or something you do in a pre-set fashion, if that's the question.

LEGAL ADVISOR KASUNIC: But if you avoid

installing a technological protection measure, couldn't you be violating 1201(a)(1)?

MR. METALITZ: Well, I know the word "avoid" is in 1201(a)(1), and I don't know what its application would be in this circumstance. I read that more likely as applying something where the technological protection measure is installed and you in some way bypass it, which I know is another word in the statute, and that it doesn't necessarily refer to a situation in which you don't install it in the first place. But that's my first impression on that, and I'm pretty sure there hasn't been any definitive interpretation of it, but that would be my first impression on that.

LEGAL ADVISOR KASUNIC: Okay. Does anyone else have any thoughts on that?

MR. PERZANOWSKI: Whether or not the protection measure is actually installed, the code does exist on the CD. The code that instructs the computer to install the device driver upon the CDs insertion into the computer exists. It's there on the disk, so, if you take some step to prevent it from operating, it seems to me that it's very likely that it's a violation of the anti-circumvention provision.

LEGAL ADVISOR KASUNIC: Okay. Mr.

Metalitz, in your comment, you said the uninstallation of software alone does not constitute circumvention of access control within the meaning of the DMCA. What if that software that you are removing is part of a process or system within the work that's being distributed or joined together? If you remove software that is working together, I guess, essentially, what if the technological protection measure is a computer program, is software itself, and you're removing that? Wouldn't that actually negate the point you were making?

MR. METALITZ: No. I think it --

LEGAL ADVISOR KASUNIC: Can you remove software if it's a technological protection measure?

MR. METALITZ: Pardon me?

LEGAL ADVISOR KASUNIC: Can you remove software without violating 1201(a)(1) if the software is the technological protection measure?

MR. METALITZ: Let me see if I understand your question. The technological protection measure may consist of a computer program within the definition of Section 101 of the Act. Are you asking if you remove that is that a violation of 1201(a)(1)?

LEGAL ADVISOR KASUNIC: Right.

MR. METALITZ: Not necessarily because

1201(a)(1) doesn't prevent you from deleting any copyrighted material that you have. I mean, I could decide to delete the music I've downloaded from a web site. I could decide to throw away my CD. I could decide to do anything that would mean I would no longer be able to use or run that program. If you're talking about a computer program, I could throw away the disk and never install it, or I could uninstall it.

LEGAL ADVISOR KASUNIC: I think we're talking about two different things. You're saying that you could delete the sound recording, right?

MR. METALITZ: You could. I understand your question is whether deleting the computer program is an act of circumvention. It certainly isn't as to the computer program.

LEGAL ADVISOR KASUNIC: Even if that computer program is the technological protection measure --

MR. METALITZ: It may be an act of circumvention of a technological protection measure that protects the underlying work, yes. But it's not an act of circumvention of a measure that protects the technological protection measure itself. You're just getting rid of it.

LEGAL ADVISOR KASUNIC: Right. Okay. So if it was protecting the sound recording, if you have a computer program protecting the sound recording and you deleted the computer program that was acting as a technological protection measure that was protecting the sound recording, that would violate 1201(a)(1)?

MR. METALITZ: That could violate 1201(a)(1)(A) depending on whether any exception applied and so forth.

LEGAL ADVISOR KASUNIC: Okay.

MR. METALITZ: If as a result of that you obtained access to the underlying work.

LEGAL ADVISOR KASUNIC: Let me go back to what we were talking about with, in particular, Section 1201(j), and to what extent is this limited to accessing -- security testing means accessing a computer, computer system, computer network solely for the purpose of good faith testing, investigating, or correcting a security flaw or vulnerability with the authorization of the owner or operator. In the case of Mark Russinovich or Ed Felten, did they do anything that you can see that is outside the scope of Section 1201(j), Mr. Metalitz?

MR. METALITZ: Well, I hesitate to characterize everything they've done because I don't

know everything they've done and I haven't read Mr. Russinovich's blog. But all I can is from what I know of what they've done, it seems to map quite well with what is set out in 1201(j)(1). They accessed a computer, etcetera, for the purpose of good faith testing, investigating, or correcting a security flaw or vulnerability. Obviously, there could be an issue there if there are other facts I don't know about. I do know that that appears to have been one of their purposes. And they did this with the authorization of the owner or operator of the computer, if it was their own computer or if it was somebody else's computer. I assume that, you know, they had the authorization.

LEGAL ADVISOR KASUNIC: Now, solely, when we introduce that word in the factors under (j)(3)(A), that is in relation to in regard to the security testing generally whether it was solely to promote security, right? So this does not concern, although the focus of this and the legislative history does seem to indicate that what Congress had in mind at the time was firewalls and things like that, as Mr. Tepp and Mr. Carson mentioned. What about the plain language here? Doesn't that seem to encompass, in terms of the activity that's going on, that the purpose of this is correcting, is investigating.

First of all, finding out on your own system what the problem, if there is a problem, and, if one is found, correcting that problem.

MR. PERZANOWSKI: My reading of Section 1201(j), in light of the fact that the anti-circumvention provisions, in general, their purpose is to prevent circumvention of protection measures that restrict access. And I think 1201(j) answers the question of access to what. The access that the protection measure is meant to control is access to the computer, the computer system, or the computer network, not the copyrighted works that are on removable media.

MR. METALITZ: Well, I assume that Professor Felten didn't access this computer because he wanted to get access to the music, which would have been the situation he's talking about. I assume he accessed the computer because he wanted to test, investigate, and, if he found one, correct a security flaw or vulnerability. Now, the solely issue enters in there, but, from all I know, I don't know that he had other motivations.

MR. SCHRUERS: May I just add on to Mr. Perzanowski's comment, which does highlight a troubling ambiguity here that access a computer, a

computer system, or computer network does not make it clear whether that also permits accessing the underlying work or, you know, that we're talking about here, to the extent that that poses a risk.

LEGAL ADVISOR KASUNIC: Well, but doesn't, the way the statute is framed, although we have some idea anyway of what the purpose of Section 1201 was generally, we have a specific statutory exemption that deals with a specific area, and that's security testing. And when we get to we have a definition of security testing, that if you are doing these testing, investigating, correcting vulnerabilities that you're allowed to do that. And then, in two, what the permissible acts are and, just generally, states that if you're engaging in those purposes, then 1201(a)(1)(A) doesn't apply. So it would seem that it would cover accessing a work that is protected. Otherwise, (a)(1)(A) wouldn't even be relevant, would it?

MR. SCHRUERS: Well, I would certainly hope that a court would interpret 1201(j)(3) in such a way, although it I think was highlighted in the Reimerdes case the interpretation was rather literalist. So these literalist interpretations cast long shadows for people who are evaluating risk.

MR. FELTEN: It may be relevant that, in investigating these technologies, we did not start out on day one looking for security vulnerabilities. We set out in the beginning to characterize and understand this technology, to learn what we could about its functioning. And it was only in the process of that investigation that we stumbled across security vulnerabilities, which led to then our research taking a different direction.

LEGAL ADVISOR KASUNIC: So in that context, the argument really is that 1201(g), for encryption research, is insufficient because Congress dealt with research differently than it dealt with security testing. And it also didn't deal with security research, which, be that as it may, that's what Congress did. So are you looking for a broadening of Section 1201(j) to include security research in the scope of this exemption or claiming that Section 1201(g) is insufficient in that it's only related to encryption?

MR. PERZANOWSKI: Certainly, Section 1201(g) just doesn't apply here. There's no question about that. I think what we're asking for is an exemption for security research, which is an activity that Congress simply created no legislation to cover.

So I don't think we're necessarily asking for a broadening of either 1201(g) or 1201(j). I think we're asking for an exemption that's completely distinct from those two.

LEGAL ADVISOR KASUNIC: Now, in terms of the national problem of this and governmental potential security flaws, what about 1201(e) and the fact that that provides an exemption for governmental entities, state, local, federal, and also includes that that can be with acting pursuant to a contract with the United States estate or political subdivision of a state? And it specifically mentions information security within that. How might that help?

MR. PERZANOWSKI: Well, I haven't paid careful attention to the text of Section 1201(e), so I'm reluctant to state my definitive position on the issue. But I think, clearly, that even if 1201(e) does apply to certain government networks or certain military networks, that's a really small piece of the problem here. I think the potential overlap with Section 1201(j), with Section 1201(i), with Section 1201(e) only indicates the fact that this is a major problem that implicates all sorts of uses. So I don't think 1201(e) certainly is sufficient on its own to remedy the problem for private citizens who have no

connection whatsoever to the government or government networks.

MR. FELTEN: With respect to 1201(e), even if we were to postulate that every single federal computer were cleaned of this security risk, which seems far-fetched in any case, there would still be a significant issue because there would still be hundreds of thousands of end-user computers which were potentially vulnerable to infection, to being taken over by a hostile actor. And that many computers, even scattered in the living rooms and offices of America, under hostile control is a big problem. That's enough to take down major providers. It's enough to take down eBay. It's enough to take Amazon. If it's enough attackers, enough flow of traffic could b generated from those machines to block access to significant portions of the U.S. government computer systems, as well. There's very strong interdependence between the security of user computers and those of government computers.

MS. CARNEY: Yes, that's just what I was about to say. If you have 200,000 personal computers that can be taken over and used in a denial of service attack, it doesn't matter if all the government computers are clean. Your network is still

vulnerable.

MR. PERZANOWSKI: And I think it's also important to point out that not all of the harms that could be visited by these security vulnerabilities are necessarily national or global in scale. Some of them are very specific to individuals. My credit card information is something that I would prefer not be able to be accessed by malicious code that is installed on my machine. That doesn't implicate government networks, but it is, nonetheless, a significant security vulnerability.

LEGAL ADVISOR KASUNIC: That's all I have for now.

GENERAL COUNSEL CARSON: Well, as Mr. Sulzberger said, we're copyright lawyers, and forgive me if the questions I'm about to ask betray total ignorance or that I didn't understand the answer that was already given to the question I'm about to ask, but I'm not a technologist. I'm still trying to focus on what the access controls are and what the acts of circumvention are because that seems to me to be central to what we're doing here. If we don't understand what the access control is or we don't know what the act of circumvention is, then there's no way on earth we're going to figure out whether an

exemption applies.

So if I understood Professor Felten's testimony, and maybe this is over simplistic, you can break down the access controls we're aware of, at least, in the three cases that happened last year in the three categories. There is something that installs a device driver. There is a music player that is bundled by the label. And there is the rootkit.

So let's start with the device driver. Is that a technological measure that controls access to a copyrighted work?

MR. FELTEN: The way I would think about this is you have those three pieces which are installed together and which act together toward the purpose of controlling access.

GENERAL COUNSEL CARSON: Okay. And I think that's a fair proposition, and I don't want to remove that from the table. But I would like to try to break it down first of all. Maybe it's a meaningless exercise at the end of the day, but it would sort of help me at least in sorting out my thoughts. So can anyone tell me whether just the part of the program that installs the device driver in itself is controlling access to the work?

MR. PERZANOWSKI: If you supposedly have a situation where, say, the only thing that happens is the device driver is installed, I think that that's definitively an access control.

GENERAL COUNSEL CARSON: In what respect?

MR. PERZANOWSKI: Well, I think Professor Felten could probably explain the functionality of these device drivers a bit better than I can but, primarily, what they do is disable the ability of your computer to read the content on the disk without use of the player that it specifies. Is that a fair assessment?

MR. FELTEN: Yes.

GENERAL COUNSEL CARSON: So it's controlling access in that it is forcing you to get access in a particular way?

MR. PERZANOWSKI: Well, if there were only the device driver, it would be forcing you to get access in a particular way that you have no means of using because you don't have the player. That sort of demonstrates how closely connected those two components are.

MR. FELTEN: When the device driver is installed, assuming it's operating as designed, only that player program would be able to access the disk

usefully.

GENERAL COUNSEL CARSON: So if you install only the device driver and not the player, then you would be prohibiting access obviously. I get that. Okay. Let's take the second part then, the player itself. The player that is installed and the device driver is directing you to, is the player itself an access control?

MR. PERZANOWSKI: I think it depends on the characteristics of the particular player. I think I'm not familiar enough with the way that these particular players work to say for sure, but you can certainly think of circumstances where the player does, in fact, restrict access in certain means. It may not let you play the tracks out of order. It may not let you do any number of things that you would normally do in accessing the work as a means of controlling the access that you have.

GENERAL COUNSEL CARSON: Okay. But I gather none of you are of any ways in which the players that we're aware of that have installed as part of these three different systems last year would control access?

MR. FELTEN: I have to admit that, as a non-lawyer, I sometimes have trouble understanding

this distinction between access controls and copy controls.

GENERAL COUNSEL CARSON: As a lawyer, I do, too.

MS. CARNEY: If I remember correctly, and I'd like Professor Felten to confirm this, the Sony player wouldn't let you rip to MP3 so you could, say, put it on your iPod, right? And that would be controlling access to some extent.

GENERAL COUNSEL CARSON: All right. Let's finally move on to the -- sorry.

MR. PERZANOWSKI: I do think it's important to realize that copy controls and access controls often overlap, and I think that's a really good example of the circumstance in which it is directly regulating copying but that copying has downstream effects on access. If I can't, I don't carry a stereo around with me, I carry an iPod. And last quarter, I think 50 million other people bought them, so it's a significant means of accessing copyrighted works. And if you can't make that intermediate copy that's necessary to put that content on your iPod, you're left without access.

GENERAL COUNSEL CARSON: So a copy control is, at the very least, an access control in so far as

it prohibits access to the copy that you weren't able to make?

MR. PERZANOWSKI: Exactly.

GENERAL COUNSEL CARSON: Okay. Finally, the software that frustrates removal of the other technological measures, the rootkit for example, is that a technological measure that controls access to a copyrighted work?

MR. PERZANOWSKI: The rootkit is an integral part of the entire protection measure at issue here. The fact is that once you have installed the player software and the device driver, someone with relatively basic knowledge of the way that these systems work could easily go in and delete the device driver and delete the player software and be able to access that content.

The function of the rootkit is to reinforce the system that is in place by hiding those files to make certain that users that have that knowledge can't go in and delete them. So on its own, a rootkit by itself without those other components is not an access control I would say. But in conjunction with those other components, the rootkit reinforces and is an integral part of the protection measure.

GENERAL COUNSEL CARSON: Okay. Now let's

go back -- I'm sorry, yes, go ahead.

MR. SCHRUERS: May I disagree slightly? I'm thinking slightly beyond the scope of the facts here. It is conceivable that insofar as the files cloaked by a rootkit are the underlying work, you could have a rootkit functioning as an access control. So in this particular circumstance, yes. But if the rootkit were cloaking the work, because that's how the access control functions, you can't see it until you pay or license whatever, then that might be an access control, and a court could so find.

GENERAL COUNSEL CARSON: Okay. Now let's get back to really to the basics, I guess, because I want to make sure I understand why we're all here. The problem with these three particular measures that were deployed last year, could you restate to me what the problem was? Why is this something we should care about? What do these measures do that we should be concerned about?

MR. FELTEN: The problem is that the measures were implemented in a way that had security flaws, security bugs, errors by the developer, which would expose a user who listened to this content and, in the course of doing so installed this software, to be subject to security vulnerabilities. The rootkit

in itself, as designed, exposed users to security vulnerability. The other vulnerabilities associated with these technologies were inadvertent.

GENERAL COUNSEL CARSON: So were the security vulnerabilities caused exclusively by the rootkit, or were they caused, in some cases, by other aspects of the system?

MR. FELTEN: By the rootkit and by other aspects as well.

GENERAL COUNSEL CARSON: Okay. And forgive me again if I'm being simplistic, in some cases the part of the program that installs the device driver was creating difficulties?

MR. FELTEN: Yes. So to give you an example, the MediaMax technology did not have a rootkit, and yet it still had security vulnerabilities. For example, the way it installed itself left openings by which a malicious person could seize control of the computer.

GENERAL COUNSEL CARSON: Okay. Don't let me put words in your mouth. Tell me, and I'm sure you've already said it, but I just want to have it fresh in my mind, what is the purpose for which you want people to be able to circumvent this entire system that, in one way or another or maybe in many

ways, functions as an access control?

MR. FELTEN: Well, the purpose is to enable users to remove this software from their computer so as to be able to safely access the music, to be able to safely listen to the music on their personal computers.

MR. PERZANOWSKI: That's certainly one of the most important non-infringing uses. The other non-infringing use that I think we're interested in enabling is the very act of research that's necessary to find out about these problems to begin with. When Professor Felten has a new protection measure on his system, in order to find out how it functions and in order to assess the way in which it operates and in order to assess the potential security vulnerabilities, as I understand his research, he has to go about a process of removing and disabling the protection measure. Therefore, the research itself could constitute a violation.

MR. FELTEN: The analogy might be to dissecting, the way a biologist might dissect a dead creature to understand how its bodily systems work. We take this apart, we pick it apart with tweezers, etcetera, to understand what we can about how it works.

GENERAL COUNSEL CARSON: All right. Mr. Metalitz, putting aside the statutory exemptions in Section 1201, when Professor Felten engages in this research and does what he's doing, is he violating Section 1201(a)(1)?

MR. METALITZ: Well, I'm not sure that he is. I think you have kind of parsed out the three strands here. We have one strand, the rootkit, that is not an access control, except in the limited circumstance that Mr. Schruers described, and that doesn't apply here. And, yet, it is, I believe, it's fair to say the source of many, although apparently not all, of the security vulnerabilities that have really given rise to this. I was surprised to hear that the purpose, by the way, for which this exemption is needed was to play music because I certainly got the impression from what I've heard over the last three hours was that the purpose was to protect computer security and protect the nation's infrastructure.

GENERAL COUNSEL CARSON: Let me stop you right there, and we'll get back to you, but I was surprised, too. So I'd just like to ask any of the three of you down there that was my impression, too, so are you rephrasing what your purpose was, are you

re-characterizing it, or how does that fit into what you say the purpose is?

MR. PERZANOWSKI: I think our initial comment makes clear that we're concerned about a number of uses, some of which apply directly and solely to computer researchers, some of which apply to consumers and customers who buy these CDs more generally. So I think we're concerned with more than one non-infringing use here. One of them is certainly enabling research. One of them is also making sure that consumers are able to access the music that they pay for without having to open themselves up to these security risks. And I think it's perfectly legitimate for our proposal to address more than one non-infringing use.

GENERAL COUNSEL CARSON: Okay, sorry. You can go ahead.

MR. METALITZ: Okay. I would just say they did address four non-infringing uses in their submission, and it didn't include protecting computer security, except through research, and I'll get to research in just a minute. But I think the fact remains that much of the problem that they lay at the door of XCP could be resolved by removing the rootkit or, perhaps, and I would certainly stand corrected on

this, perhaps by uncloaking this so that the problem, as I understand it, that the rootkit introduces as a security matter is that people could then be putting other programs onto your hard driver. Other people that have access to your hard drive can be putting other programs on there, and you wouldn't even know about it, and they could be malicious programs, and your anti-virus software, your other protective software would have more difficulty finding them, and that could create problems.

But all those vulnerabilities, as I understand it, could be eliminated if you were to get rid of the rootkit. And what we've already heard is, except in the very limited circumstance that Mr. Schruers describes, which is not present here, that's not an access control. So to me --

GENERAL COUNSEL CARSON: Did we really hear that? I thought I just heard the opposite from Professor Felten, but maybe I'm misunderstood.

MR. FELTEN: You did hear the opposite. It's not correct that removing the rootkit solves the problem, even for XCP. MediaMax has no rootkit. The issue there is not at all the rootkit. But even for XCP, there are other security problems.

MR. METALITZ: I understand that he's

saying it doesn't solve all the problems, and if I said it solved all the problems I stand corrected because I know he says it doesn't. But certainly many of the problems that have been described that are attributable to the rootkit can be resolved by removing the rootkit, which is not an access control. So that, to me, takes this outside of 1201 altogether.

Now, your question, Mr. Carson, was whether the research that Mr. FElten did, if 1201(j) didn't exist, would that violate 1201(a)(1). I'm really not sure, but the way he describes it I suspect not because he describes dissecting the program and trying to figure out how it works. I don't know. That might involve gaining access to the underlying work, it might not. If it didn't, then it's kind of hard to see how it would violate 1201(a)(1). If it did, then perhaps it did, but I think 1201(j) is really the operative provision.

GENERAL COUNSEL CARSON: Okay. Let's ask the three of you at that end. What's your concern about the possibility that Professor Felten's research would be construed as a violation of 1201(a)(1)? Why should he be concerned and, therefore, why should we be concerned about it?

MR. PERZANOWSKI: Well, the reason we're

concerned about it is because his research entails disabling, removing, and uninstalling access controls and thereby gaining access to the underlying copyrighted work, which I think is a pretty clear example of a prima facie violation of Section 1201(a)(1). And he can explain a little bit more about how the research actually proceeds and the steps that he takes.

One thing before he begins, though, that I'd like to say is I think, you know, we're talking about potential of eliminating the rootkit and, therefore, solving some but not all the security issues that we're concerned about. I think that it's probably a conceptual mistake to think of the rootkit itself as somehow a completely separate and distinct piece of code that is somehow not integrated with the protection measure more generally. I think it's more valuable if we understand those things as working on conjunction and really forming together, all three of those components, the protection measure issue.

MR. FELTEN: In the course of our research, we do obtain access to the content. One of the methods that we use, for example, is to reach into the inner workings of the technology and turn off individual pieces of it selectively and then try to

diagnose what happens. It's one of the ways to learn. If you think about tinkering with an engine, for example, you might ask what if I turn this part off, what happens? Does it still work? Does it work differently? And so on. Certainly, one of the tools we use, and, in the course of doing that, we do at times get access to the content. That's the only way we can really fully characterize how the technology works and how it works, how it doesn't work, and what its failure modes are.

GENERAL COUNSEL CARSON: All right. So Mr. Metalitz, given that explanation and assuming 1201(j) is off the table, has Professor Felten described a circumvention of an access control in violation of Section 1201(a)(1)?

MR. METALITZ: He may have if it's done without the authority of the copyright owner.

GENERAL COUNSEL CARSON: Can't we stipulate to that?

MR. METALITZ: Well, no, in fact, right now, if he were doing it, it probably would be with the authority of the copyright owner.

GENERAL COUNSEL CARSON: Okay. But back in early fall, I suppose it wasn't; isn't that true? And the next time around, heaven forbid, it may not be

with the authority of the copyright owner, as well?

MR. METALITZ: Well, I would take exception to that to some extent. If you look at the terms of the settlement that Sony BMG is proposed to enter into, so at least as far as their works for their products for the time period of that settlement, I wouldn't assume that it's without the authorization of the copyright owner.

GENERAL COUNSEL CARSON: Thanks for referring to that settlement because I did mean to ask you could you please submit that to us so we have that in our records?

MR. METALITZ: I'd be glad to. I would say it's a proposed settlement. It has to be approved by the court in May, I think.

GENERAL COUNSEL CARSON: Professor Felten, you wanted to say more.

MR. PERZANOWSKI: On the issue of authorization, I think as I stated earlier, we've contacted Sony. We've asked Sony for a very clear written statement that they would not bring a suit against Professor FElten or Mr. Halderman for their research. As of yet, they've been completely unwilling to do so and have not responded to our requests. I would assume that Mr. Metalitz has better

relations with the people at Sony than we do. Maybe he could get us a guarantee of that sort.

But as it stands, Sony has not provided us any guarantee. And Sony, as we've talked before, is probably not the actor that we're really worried about in the future. There are other record companies at issue here. EMI, for example, has distributed several million CDs with these copy protection or these access protection measures installed on them. So it's not so simple as to say that we have authorization. I think if you would ask Professor Felten if he had authorization from any copyright holders it would come as a shock to him.

MR. METALITZ: Well, just to make sure the record is complete on this, I will put in the record a letter which we reference in the footnote of our Joint Reply Comments dated November 18th from Jeff Kinnard at DeBeboise & Plimpton to Robert S. Green, which states, "Sony BMG will not assert claims under Title 17 of the United States Code or similar statutes in other countries against legitimate security researchers who have been, are, or will be working to identify," I should say, "have been, are, or will be working to identify security problems with copy protection technologies used on Sony BMG compact

disks." I think it's also probably fair to say that copy protection technologies in this case includes the XCP, and the rest of the letter is about XCP.

GENERAL COUNSEL CARSON: Who's Robert S. Green?

MR. METALITZ: He was counsel to the, he's one of the counsel to EFF.

GENERAL COUNSEL CARSON: Okay, okay. And does Professor Felten fall into that class of researchers who were described in that letter?

MR. METALITZ: It sounds to me as though if what he's doing, if he's a legitimate security researcher, which I don't dispute, and that he's working to identify security problems with copy protection technology used on Sony BMG compact disks, then I think he is covered.

GENERAL COUNSEL CARSON: Are you speaking for Sony?

MR. METALITZ: On whether he's a legitimate security researcher?

GENERAL COUNSEL CARSON: Sure. I'm trying for you, Professor Felten.

MS. MULLIGAN: To be clear, I don't think that Sony intends to sue Ed, right, for this particular research. What we've been unable to obtain

is a statement that Ed and Alex will not be sued for their research. And frankly, it goes far beyond potential liability under the DMCA. You all are intellectual property attorneys. I'm sure you can imagine the vast number and kinds and sophisticated claims that one could bring against these two folks for their research.

But the fact of the matter is that we haven't been able to get letters that we could use in court in defense. We have a general statement. It's been very, very difficult, despite numerous efforts, to get statements that say we will not sue them for this kind of research done on these kinds of technical protection measures today or in the future. And I find that, you know, quite depressing.

And we're not here because we want to spend a lot of time with you, you know. Ed and Alex have spent way too much time in my office and on the phone with me, and this is probably their least favorite way to use their time. And so, you know, if we thought that when we were faced with a court action that we would have a good defense, and we would certainly argue extremely arduously, we wouldn't be here. But their research has been slowed down, has been put at risk. They have to deal with their

general counsel far more than any other researchers I know, and I know a lot of researchers. You know, it's a burdensome way to go about creating good computer security.

MR. PERZANOWSKI: And it's probably worth noting, and I'm sure most of us are aware of this, that both Professor Felten and Mr. Halderman have faced potential litigation in the past for their research activities.

MS. MULLIGAN: Where they were authorized.

MR. PERZANOWSKI: Certainly. So I think their past experience points to the fact that this is not sort of a hypothetical threat of litigation in the future. Sony, I'm sure, would not be willing to take on the public relations risk of suing two legitimate researchers like these, but there are many other copyright holders and there are many other companies that create technological protection measures that could file suit.

GENERAL COUNSEL CARSON: All right. Now let me clear an inconsistency on either what I heard or what I thought I heard. I thought I'd heard from Professor Felten that the rootkit actually is an access control, but maybe I didn't hear correctly. Mr. Metalitz was saying that it wasn't. Is the

confusion mine, or is there a difference of opinion?

MS. CARNEY: It can be, but it isn't in this specific Sony case.

MS. MULLIGAN: Right. In this specific deployment, it wasn't functioning as an access control. But, you know, cookies could be, right. You can think of lots of different technologies that can be deployed --

GENERAL COUNSEL CARSON: Okay. Right now I'm focusing on what we know has happened. You will have your chance, Mr. Sulzberger. I'm trying to get focused questions right now.

MR. SULZBERGER: There's a parsing going on right now that is implicitly mistaken, and I think every programmer here would agree. A rootkit can operate in many different ways. One way would be to sense the substitute behind every system call on the kernel or the kernel side of it and not the user side, substitute your own stuff. Now, that is exactly what happens. That's the so-called, what were you calling it? The driver. That's a substitution of a driver. A driver is something that, actually the idea is it connects to a peripheral, etcetera. But there are other kinds of drivers, too.

In general, a rootkit is that which cloaks

the machine. In other words, to actually use a machine, you have a stack of programs. You touch things on the machine and move them around, and then those signals get sent down, down, down, down to something often called the kernel that actually touches the hardware. Sometimes it uses drivers they say, etcetera. And then the information comes back, and it's displayed to you or you listen to Alicia Keys on the thing or you hear a scratching noise or whatever.

And there is not, in this case they're using the word rootkit to mean something it disables DIR in a specific narrow way, an unacceptable way but it's narrow. It doesn't control it in that sense.

But the part of the thing that substitutes the driver, that's one of the techniques of a rootkit. All DRM, it's interpenetrated. You have to give a defensible, robust perimeter that prevents the owner of the machine from control of the machine. Otherwise, you don't have an effective rootkit. That is not an effective rootkit because you can press the shift.

But it's just the word rootkit has many shades of meaning, but its central meaning is it stops you where you once had control of the machine. If it

gets installed or if it's installed at the factory you never have control of the machine. And so one should be a little careful. It's a caveat. It's a narrow technical caveat.

A rootkit is not necessarily just this tiny little simple thing that disables DIR, if I've understood what it is and I might be wrong. The rootkit could be the substitution of all the system calls or enough of the system calls to give another party control of your machine.

GENERAL COUNSEL CARSON: Okay. Now, Mr. Metalitz, so we've been talking about -- no, no, I'm sorry, I want to go through this, and I want to get back to you. We've been talking about Professor Felten's research. So I guess my final question on that line is, Mr. Metalitz, is there any reason to doubt that what he is doing in this research is a non-infringing use of the copyrighted works that are protected?

MR. METALITZ: That what he is doing is a non-infringing use?

GENERAL COUNSEL CARSON: Yes.

MR. METALITZ: Yes. I don't think that, as he's described it, it doesn't infringe copyright.

GENERAL COUNSEL CARSON: Okay. Now let's

take the other purpose, and there may be, I'm going to collapse maybe two purposes into one, but I think it's --

MR. METALITZ: Could I just add to that? That is also a condition for the applicability of the 1201(j) exception. If it is infringing activity then you're not eligible.

GENERAL COUNSEL CARSON: Okay. Now, the other purpose or combination of purposes, depending on how you want to parse it, that I heard was to allow people to play their music without creating all sorts of vulnerabilities or dangerous things happening to their computers, is that a non-infringing use?

MR. METALITZ: Yes. Allowing them to play, yes.

GENERAL COUNSEL CARSON: Okay. And do you have any problem with people disabling the particular kinds of access controls we've been talking about here that were deployed last year so that they can listen to music without harming their computers?

MR. METALITZ: They have no need to do so.

GENERAL COUNSEL CARSON: Because?

MR. METALITZ: Because there are many other ways that they could get the music and play it on that same device. And once they have copied the

music to their hard drive, they can then install the entire program, the entire XCP, and, as I understand it, I think it was testified before they have access to the music.

GENERAL COUNSEL CARSON: So if in the future, a record company -- okay, go ahead, Mr. Felten.

MR. FELTEN: I believe that's incorrect. These technologies would allow the user to copy the music to their hard drive only in limited ways, which are unlikely to allow playing without the disk in the future if the software is uninstalled.

MS. MULLIGAN: And suggesting that there are alternative means of accessing doesn't state that circumventing for the purpose of accessing without introducing security vulnerabilities is not infringing, which I think --

GENERAL COUNSEL CARSON: That's what I wanted to ask Mr. Metalitz. Are you telling --

MR. METALITZ: Non-infringing. But the issue here, of course, is whether the inhibition that people are experiencing in making non-infringing uses of works justifies an exemption for circumvention. And as we lay out in our reply comment, there are many other ways that people can listen to their CDs without

ever installing this software in the first place. And I would submit that I take the point that Professor Felten just made, but my understanding is that, in fact, they can continue to play this music after they've uninstalled it on that machine.

But even if that were not true, there are many other ways they can play it on other devices, and there are even ways they can play it on that machine and transfer it to portable devices through downloading this exact same music.

MR. PERZANOWSKI: And paying for it again, which seems to violate the reasonable expectations that consumers have when they purchase a CD. When I buy a CD, I expect it to work not only in my stereo at home, not only in my car, but on my computer, and I expect to be able to transfer it to my iPod. All of those things, you know, listening to it on the computer and transferring it to a portable device of my choice are things that you can't do with these protection measures in place. And I think it's sort of unreasonable to expect people to go out and buy a CD and then when they get home realize that they can't use the CD in the way they expected and then buy the content again from iTunes, for example.

MR. METALITZ: Well, the Register and the

Copyright Office and Librarian has already been all over this ground three years ago. The issue that was presented then was whether an exemption should be allowed in circumstances in which it was claimed there were difficulties in playing CDs on particular types of devices.

GENERAL COUNSEL CARSON: Aren't we hearing something a little different this time? Aren't we hearing that what was deployed was something that not only may make it difficult for you to play things but it might do real damage to you and your computer. Isn't that a little different?

MR. METALITZ: It is different in terms of the allegation that was made or the impact of this particular device. But in terms of 1201, where you're talking about non-infringing use, this is why I think the question of whether the non-infringing use is protecting the computer networks of the world or whether it's listing may be relevant. For the purposes of 1201, this really is no different then the situation last time, at least the issues that are involved in terms of people's ability to make the non-infringing use, listening to their CDs, that they wish to make have increased since 2003 rather than decreased. So if you can't, for whatever reason, play

the CD on your computer hard drive or on your computer drive, first of all, if it involves XCP, you can get your money back and you can get a free copy and you can get a lot of other product for free. But let's assume that that settlement doesn't take effect for some reason, you still have many other ways of gaining exactly the same access to this material for exactly the same non-infringing use. And the new big factor here that wasn't present or was only present to a very limited extent in 2003 is legal downloads.

GENERAL COUNSEL CARSON: Okay. So basically you're telling us that if record companies were to continue in the future to deploy the same technologies that were deployed last year and just basically say, "Look, you don't like the fact that we're wreaking havoc on your computer, you can go get a download," that people shouldn't be able to circumvent those access controls in order to un-do the damage.

MR. METALITZ: Circumvent in order to solve the security problem that is involved in this case.

GENERAL COUNSEL CARSON: Because they should know better than what you're trying to sell them?

MR. METALITZ: Pardon me?

GENERAL COUNSEL CARSON: Because they should know better than to buy what you're trying to sell them?

MR. METALITZ: No. Because, as I think we've explained, the action that they would take to eliminate or minimize the security risk is not, in our view, an act of circumvention. But from the standpoint of the non-infringing uses that they wish to make, I think the situation is the same as or in fact better for consumers than it was three years ago because there are so many other alternatives.

MS. MULLIGAN: So I just want to be clear. So you're saying that Ed's activity, which involves circumventing the same access control mechanism, would not be circumvention, but that a consumer's identical behavior in order to avoid these security vulnerabilities would be?

MR. METALITZ: No. If --

MS. MULLIGAN: Well, that they should get the music get some place else.

MR. METALITZ: Well, they can get the music some place else. Again, I don't think his main motivation was to listen to the music. I think the --

MS. MULLIGAN: No, no, no. Set aside the

motivation. Assume that both motivations are considered non-infringing.

MR. METALITZ: Well, yes. You're talking about the identical activity, and I think we have two answers to that. One, we don't believe that this activity is circumvention. And, secondly, if it is circumvention, then what he is doing and what a consumer is doing when they access their computer in order to investigate whether there's a security vulnerability and to remove it is covered by 1201(j).

GENERAL COUNSEL CARSON: It's not circumvention. Now, we have -- are you telling us that there are no access controls involved here?

MR. METALITZ: What I'm telling you that, as we just heard with the rootkit, that removing the software that is causing or is alleged to cause the security problem is not circumvention of an access control. There is an access control here, or at least I think we should proceed on that assumption that the Register found three years ago that, although as you saw in this letter from DeBeboise & Plimpton, people commonly refer to this as copy control. But in terms of 1201, it may qualify as an access control, too.

But as I think your questioning pointed out, the access control feature is not the same

feature as the one that is alleged to cause at least a good deal of the security problems. Now, I stand corrected, and I didn't mean to say that there was no security vulnerability. I'm not sure I understand it as well for the non-rootkit area as I do for the rootkit area what the security vulnerability is. But to a great extent and the fact that, at this point, Sony BMG is making available to anyone who wants it, and they don't even have to use the telephone, which was the concern that Ms. Carney had earlier, they don't even have to call, there are ways that they can get an uninstaller, and Professor Felten has provided them with an uninstaller. So they can go ahead and uninstall this entire software program, and that, as I understand it, eliminates the security vulnerability that they had experienced. If I'm wrong about that, then I would stand corrected.

MS. MULLIGAN: I think we'd be willing to concede that once Ed and Alex and other researchers published information about the security vulnerabilities and Sony issues an uninstaller that probably authorization exists to use that particular uninstaller, which we've established does not actually address all of the security problems. But I think that doesn't answer the underlying question as to

whether or not this was or was not circumvention and whether or not it was infringing.

MR. FELTEN: With respect to this question of whether someone could just buy the music on iTunes instead, for our purposes of doing research on the XPC and MediaMax technologies, of course buying the music on iTunes is utterly pointless. That's a separate research project.

REGISTER PETERS: I think we have exhausted the questions. Yes.

LEGAL ADVISOR TEPP: I want to go back to the rootkit because, as Professor Felten's very last quip demonstrates and seems to have evolved, it's not about getting to the music or the other visual works as much as it is getting to the driver and the player and either deactivating or removing those to deal with security functions. So I want to focus in on whether or not the rootkit, which where it exists can be a cloaking device over the driver and the player, constitutes, for 1201(a)(1) purposes, an access control because I don't think there's a lot of debate that we could have about whether or not the driver and the player are copyrightable computer programs. It seems clear that they are.

We've sort of heard different answers as

to whether or not the rootkits that we've seen, granted one of the three technologies that we've described didn't have a rootkit; I understand that. But for the two that did, I asked you, Professor Felten, earlier could you disable or remove the other technologies without first disabling the cloaking aspect of the rootkit. And your answer, as I recall, was that if you can you haven't been able to figure it out yet.

MR. FELTEN: Correct.

LEGAL ADVISOR TEPP: So my question at this point is is the rootkit designed by its proprietors to have a deactivation aspect, or is it a permanent cloak that's never designed to be removed by anyone?

MR. FELTEN: As the product initially shipped, it was designed to stay there for as long as it could. There was not an authorized way to uninstall it.

LEGAL ADVISOR TEPP: Even by Sony?

MR. FELTEN: Sony did not initially provide a way to remove it.

LEGAL ADVISOR TEPP: But could Sony have done it themselves? Here's what I'm getting at --

MS. MULLIGAN: Could Sony have used it a

DRM that didn't contain a rootkit?

LEGAL ADVISOR TEPP: No, no. Could Sony have taken their own rootkit and turned it off?

MS. MULLIGAN: Remotely?

LEGAL ADVISOR TEPP: By many means.

MR. PERZANOWSKI: They certainly could have shipped a protection measure that didn't include a rootkit. It's hard for me to imagine that once the CDs are pressed up and the code is already on the disk and we send them out in the world and people put them in their machines that Sony has, at that point, any control left over how these protections function.

LEGAL ADVISOR TEPP: Let me bring it back to the statutory language and, perhaps, be less cryptic. The definition of 1201(a)(1) of a technological measure that effectively controls access to a work is a measure in the ordinary course of its operation requires the application of information or a process or a treatment with the authority of the copyright owner to gain access to the work. And I'm trying to explore whether or not a rootkit that cloaks the driver and the player actually has no, in the ordinary course of its operation, application of information, process, or treatment that would allow access to the driver and the player and, therefore, it

may not actually be, for 1201(a)(1) purposes, an effective, a technology that effectively controls access to a work.

Would an uninstaller, in your opinion, Professor Mulligan, constitute a treatment, I guess it would be?

MS. MULLIGAN: I guess the reason that we're all sitting here kind of trying to bend our minds is that it's hard to kind of pull this technological protection system, which consists of these three discrete technical functions apart. So if you want to think about the rootkit is certainly trying to mask and prevent access to the uninstaller and to the files that restrict access to the underlying work. So you could say, perhaps, and Ed can correct me if I'm wrong, perhaps one could argue that removing the rootkit would be avoiding or disabling a technical protection measure that is preventing access to the device driver. And then removing the device driver would be removing a technological protection that would be protecting access to the underlying copyrighted musical work. We can frame it that way if you'd like but --

LEGAL ADVISOR TEPP: Well, what I'm getting at is I'm not sure, and, in fact, I think I

may have heard the opposite, that the trio of technologies that we're talking about may very well not be an access control protecting access to the underlying musical work, not necessarily from you. I understand that you're making the argument it is. I'm not sure that that's been demonstrated, and I think I heard from Mr. Metalitz that it very well may not be.

MS. MULLIGAN: I'm not sure, in what way do you think it is not limiting access to the work?

LEGAL ADVISOR TEPP: Well, I guess it goes back to the question I asked earlier, and that Mr. Kasunic followed up on, which is can I hear the music on my Windows PC, putting aside the availability of other devices and so on and so forth, even though this technology is on the CD? And it sounded to me like, but for the EULA, the answer is yes, either because I accept this technology and granted the security problems that come along with it or because I either disable the installation of the technology at the beginning or uninstall it and use other players to play the music. So you tell me, you know, where in that thought have I gone wrong? And, Ms. Carney, I'd like you to respond as well.

MS. CARNEY: I don't think that it's fair to argue for or against this exemption based on this

Sony XCP technology alone. I think we have to consider the case when a music company will release a CD that can only be played with their player and that player introduces security vulnerabilities. Are we really going to tell consumers that you can either agree to return your music that you lawfully purchased or you can accept the security vulnerabilities that come with it. I mean, it's true in the Sony case that the problems may be resolved at this point, but I don't think that argues against the exemption.

LEGAL ADVISOR TEPP: It's not an unfair point to make that this is the only way the technology could be configured. But when I asked earlier what evidence is there, beyond the purely theoretical, that anything could happen in the future, that this is more likely than not to occur in the next three years, which is the standard we've got to apply, I'm not sure I heard a lot of tangible evidence.

MR. FELTEN: The MediaMax disks are still out there, and it's certain, virtually certain that they will still be out there in quantity within the next three years and still posing this issue with respect to the MediaMax technology.

LEGAL ADVISOR TEPP: Right. And that goes to the question of the reinfection and the brief

exchange that we had earlier. I'm not sure -- well --

MR. PERZANOWSKI: So if I could, your question is how is access controlled. Because if you sort of follow along with the process, at the end of the day you're able to listen to your CD, right? That's essentially your question. Well, I think access is limited in two ways. First, the device driver by itself, if the device driver were the only thing there, you would have absolutely no means of listening to the music whatsoever. So what the protection measure does is block all access. And then it says, "You know what? We'll give you a little bit of access back. You can use this particular approved player, but you can't use any other number of players that you may choose to use." And even more importantly, the way that these protection measures limit access is by forcing consumers to accept unreasonable risks in order to enjoy that access. So you can have a little bit of access to your copyrighted work that you paid for but only if you're willing to put up with these intolerable security vulnerabilities.

LEGAL ADVISOR TEPP: Okay. Mr. Schruers, and then I want to move on because we're re-treading ground we've already tread, and we've already spent a

lot of time on this.

MR. SCHRUERS: I'll be quick. I apologize. I hope I've misunderstood, but to the extent that the Office is saying that because you can follow some course of processes here to gain access to the protected work that it doesn't effectively control access to the protected work under 1201(a)(1)(A) would suggest that nothing would effectively control access to anything because anything that is controlled through some means of processes somebody would be able to gain access to.

LEGAL ADVISOR TEPP: Let me be very clear. The Office isn't saying anything. I'm not even saying anything. I'm asking questions.

MR. SCHRUERS: I understand. But I guess what I'm saying is is that definition would seem to sort of disenvow 1201(a)(1)(A), at least with respect to a broad class of users. And perhaps, I hope I've misunderstood because it seems --

LEGAL ADVISOR TEPP: The very first question I asked this morning was do we all agree that 1201(a)(1) prohibits the circumvention of access controls which prevent access to a copyrightable work, and I think we've all agreed on that. So I'm just asking how does this fact pattern or any other fact

pattern for which there's some evidence that it's more likely than not to happen in the next three years fit in to that prohibition? That's my question.

MR. PERZANOWSKI: I think the point is well taken that eventually all access controls have to result in access. You know, otherwise, the copyrighted work would never be accessible to anyone. So the fact that there's a process that you can go through in order to obtain access doesn't mean that access is not controlled.

MS. MULLIGAN: Controlling access doesn't mean prohibiting access, it means structuring access, right? It could certainly mean prohibiting, but I think the way in which you're setting it up it can only mean prohibiting. And what most access controls do is structure the way in which access occurs. People rarely put into the market something for which access is impossible.

LEGAL ADVISOR TEPP: My last question. Mr. Metalitz, taking what we've heard from some of the other panelists, if we have a rootkit which is designed to and, in fact, does cloak the underlying driver and player, and someone wants to disable and perhaps delete the driver and the player, and in order to do that they need to deactivate the rootkit, in

deactivating that rootkit have they violated Section 1201(a)(1), in your opinion?

MR. METALITZ: I think you're proceeding on the theory that the protected work, the work to which access is being controlled here is the driver and the player. I'm not sure the answer to that because that's certainly not the class that's proposed here, and so we haven't really focused on access controls for those types of computer software in this context.

LEGAL ADVISOR TEPP: You're a smart guy. What do you think?

MR. METALITZ: I think I'd probably rather think about it a little bit before I answer you.

MR. SULZBERGER: Let me point out that suggested amendment to the Mulligan/Felten proposal deals precisely with what you're talking about. That is our amendment, and that was our suggestion three years ago, too. You've hit the nail on the head, and this is why it goes all the way through and why it's going to be hard for you to avoid facing the things that Professor Mulligan has suggested are not within your commission because you're facing them now.

LEGAL ADVISOR TEPP: Okay, thank you.

REGISTER PETERS: Okay. Rob, you had one

more question.

LEGAL ADVISOR KASUNIC: I just have one quick technical question just to make sure it's in the record. If the autorun feature is disabled, does that mean that the device driver or the player and the rootkit will not be installed?

MR. PERZANOWSKI: It does not mean that they will not necessarily be installed. It means they will not be installed until the user clicks through the EULA.

MR. FELTEN: It means they will not be installed automatically.

MR. PERZANOWSKI: Right. But they will may be installed if the user, as most users do, simply click the buttons that come up on their screen or if they really want that access to the bonus content that they can't otherwise access.

REGISTER PETERS: Thank you. I want to thank all of you. This has gone an hour and a half beyond its scheduled time. It was mentally challenging for those of us up here, and we'll work through it. I believe we probably will have questions, follow-up questions. But I thank all of you for your testimony here today. And we will be back at 2:30 to talk about dongles.

(Whereupon, the foregoing matter went off the record at 1:09 p.m. and went back on the record at 2:40 p.m.)

REGISTER PETERS: This is a continuation of our hearing and the panel this afternoon is focusing on an exception proposed for computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. And the witnesses are Joseph Montero and Steve Metalitz. Why don't we start with you, Mr. Montero, since you're the proponent of the exemption. If you would, the beginning, what we'll do is you'll present your testimony, Steve will present his, we'll ask the questions, and then you have any questions of each other you can ask questions.

MR. MONTERO: Good afternoon, Ms. Peters and members of the Board. Thank you for providing me the opportunity to speak before you today, this being my third time in six years.

We in the triennial rulemaking have grown together. When I first came here in 2000, my little girl, Gabrielle, was only six years old. Now in two weeks, she'll be a teenager, and I want to thank her

first for being such a great daughter and also for helping me organize my papers for this hearing. And Gabby is behind us, and thanks a lot, girl.

Just a week ago, Gabrielle invited me to a poetry reading at her school, but she also said that, "It's okay, Dad, if you can't make it." Puzzled, I asked, "Why?" and she said, "Well, sometimes you make me nervous when you're in the room and watching me." I told her not to worry because I was just invited to Washington to testify at the Copyright Office, and she'll have a chance to watch me and make me nervous if she'd like to come. So, Gab, yes, I am a little nervous, too. Thanks.

Just like my little girl, technologies continue to grow and mature. Computers have become faster. Operating systems have changed. Now we have 64 bit Windows and dual core processors. Floppies have been replaced by CDs and memory cards. What was once known as the printer port, has given way to the USB port. Companies continue to get bought and sold, such as Rainbow Technologies, one of the dongle manufacturers.

Now, change does not have to be good or bad. But it does bring about certain problems, and that's why I'm here before you today.

Some of us would like a new car every few years. We love those new gadgets, while others are quite comfortable driving the same old car for years. It gets us where we want to go, we know what it does, and have no need to change or spend the money for something else.

Computer software and hardware is often like that. Some of us would like to stay with what we have, and others would like the latest and greatest. Manufacturers design products to become obsolete, or products become obsolete because other technologies arrive.

There are certain dongle devices with a battery built in that will only last a certain number of years before it fails, and one of these is here. Microsoft operating systems are phased out and replaced every few years. If you remember DOS, Windows 3.0, Windows 95, 98, Millennium, and 2000, all of those at the moment now are unsupported operating systems. Microsoft only got forced to continue supporting 2000 because so many corporations were involved with that already and didn't want to upgrade to another system. But is it really necessary and shouldn't we have a way to continue to use older products we have paid for?

Certain computer programs are access controlled by either a floppy key disk or putting a hidden file or files on a computer. This is explained in more detail and document for the initial comments by Brewster Kahle of the Internet Archive. The current dongle exemption has permitted dongle programs to be archived. I am familiar with the products and problems he discusses and have seen this in my field as well, and I'll speak to that in a moment.

I support his proposed classes of works, computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, and computer programs and video games distributed in formats that require obsolete operating systems or obsolete hardware as a condition of access.

What I have in front of me is called the dongle, and that would be these. While one may seem innocent enough, often end users must chain multiples of these together to run different packages on the same computer. And as you can see, it's not very practical. These devices have been around since the 1980s, and millions of them have been sold. It is an access control device that presents one from accessing a computer program that has been legally purchased.

Unless the device is attached to the printer port, the program will not run. Consumers are also finding that after upgrading their computer, many newer systems do not come with a printer port, and they have no way to plug in their access control device and run their software, a non-infringing activity.

In 2000 and 2003, the Librarian of Congress decided that one of the classes of works that should be exempt was computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. The exemption has had a positive effect providing relief to those end users that have experienced problems with these access control devices.

In September of 2003, I received an inquiry from a previous client. This was a large organization with amazing people resources. They had two software programs that used an old printer port dongle and, incredibly enough, no one in their vast organization had the technical expertise to replace these control mechanisms. They had used my dongle replacement software for both programs in the past on a Windows 95 and a Windows 98 operating system. Now, on their new Windows XP machines, my software and the dongle devices were not able to grant access to their

programs. Neither of the software programs are supported any longer, and one company had gone out of business and the other would not support an older product. That former client was the United States Department of Defense. The division involved was the Naval Surface Warfare Center.

While preparing for this hearing, I sent an e-mail to my contact there and asked him to describe what he did with the software and if its continued operation was valuable to his job. He responded, "I can't give specific examples of what I use the software for since it's all classified. However, both applications are circuit simulators. The establishment here is the Department of Defense Laboratory doing research, development, tests, and evaluation work for the Navy. My work involves doing a considerable amount of circuit analysis and simulation. Simply put, I couldn't do my job without them. I do analysis and simulations with them in minutes to hours that would take days to weeks of laborious computation to do otherwise."

If you recall a few years ago, the example that I presented to you was for the Department of Justice and the Immigration and Naturalization Service ran programs with lock devices that they had

previously gone bad, and they were down to a single lock device, and if that device had failed they would have been unable to continue using the passport system and providing passports.

So happily, we were able to provide a solution to the Department of Defense, just as we were to the Department of Justice a few years earlier. This rulemaking proceeding is directly responsible for helping those agencies, and I thank you for your rulings.

Over the years, companies get bought and sold. They may go out of business, or they may simply want an end user to upgrade to a new higher-priced package when the current software they're using suits them just fine. The company that purchased Rainbow Technologies is SafeNet, Incorporated. Only three dongles from the Rainbow Sentinel Line continue to be sold for the PC: the Sentinel LM, the Superpro, and the more recent Ultrapro.

Products that have been in the marketplace for years, such as the Pro, the C, the Scribe, and the Scout, will not be able to be replaced any longer. They are obsolete. Hundreds of thousands, if not more, consumers will find the thousands of dollars they paid for their software will be worthless at some

point in the near future.

I have once again numerous unsolicited e-mails sent to me regarding dongle problems, and I'd like to read some of them into the record. They are all after the date of my last testimony. I believe these would be considered privileged communications, and I have copies for this Board. However, I would ask these not go into the public record.

GENERAL COUNSEL CARSON: That can't happen, Mr. Montero.

MR. MONTERO: Oh, is that correct?

GENERAL COUNSEL CARSON: Yes.

MR. MONTERO: I thought we did that the last time. We read my testimony in.

GENERAL COUNSEL CARSON: We'll have to take that under advisement, but I think it's highly unlikely we would accept anything that can't be made part of the public record.

MR. MONTERO: Then I have no objection to it being part of the record. One client, Wayne, uses a software package called Scenario, which is no longer supported. The power generating company he works for, for safety reasons, cannot wait for a working dongle to fail. Scott has seen the software program sold several times. It is called Breakware. He received

permission from the latest company that owns it to have the program recompiled without the dongle access checks. However, as is often the case, those source code files were not kept properly, and they were not able to recompile the program.

An e-mail from Dennis has a program that was about five years old. It stopped working all of a sudden. The company wanted him to upgrade to a current product for $1250.

Robby writes of a Scanvec program that ran and crashed on Windows 98. They want it to run under Windows XP. However, the company is out of business, and they cannot find drivers to upgrade to the new operating system.

Neil has 16 years of CAD drawings on his computer, and, because of the dongle, he cannot run the software on anything more than a Windows 98 computer, which is no longer a supported operating system by Microsoft.

Lee has a DOS version of Cabinet Vision that is no longer supported but works with the key for now. However, as we all know, DOS is not a supported operating system any longer by Microsoft, and he will end up losing access to all his data if he cannot bypass the key.

As I mentioned earlier, millions of printer port dongles have sold since the 1980s. Now more and more computers and laptops are being sold without the printer port. Most often, manufacturers will not simply exchange dongles, a printer port one for a USB type. Rather, they want the customer to upgrade to their latest and greatest version for thousands of dollars, which the end user may not need.

Being able to run software that was legally purchased on a new laptop or rackmount server, whether it was dongle protected or key disk protected, increases the availability of copyrighted works and permits the works to be archived and preserved.

Lee says of his Inframetrics software that his new notebook computer only has USB ports, and the company wants $7,000 to upgrade to their new software. Mr. Larson from Denmark writes of a problem when he bought a new laptop without a parallel port. His Oceanographics software is not supported any longer. JP is implementing rackmount servers and, more and more, he says they are no longer coming with parallel ports, so he has to keep an old machine around just to use his dongle.

Nick is from the UK. He's having a problem getting his PADS software to run on Windows XP

64 bit systems. He cannot get drivers for it.

Sergio has a laptop that does not have a parallel port and, even with a port replicator, he cannot get his software to recognize the dongle. The program developer has gone out of business, and he's out of options.

Bernd in Germany has purchased a new Acer laptop without a printer port. And even with a port replicator, the dongle is still not recognized.

End users are not the only ones that are aware of the problems with dongle devices. A simple search on Google will produce hundreds of results. I've attached numerous pages printed from company web sites describing problems and incompatibilities. It's not always the lock the device itself that is causing a problem. Beginning with Windows NT, hardware and software programs could no longer directly talk to the dongle. They had to use what was called the device driver to handle the communications between the dongle, the operating system, and the application software.

Sometimes, drivers for different operating systems are not available for some time, such as 64 bit Windows operating system. The company that bought Rainbow Technologies, Safenet, does not support

printer port devices under 64 bit Windows XP. Safenet only provides a USB interlock support for 64 bit Windows XP operating system.

The chart below is from the Safenet web site and shows only two dongles, both USB, one for AMD, one for Intel, that support the Windows XP Pro 64 bit system. Since we've already established Microsoft phases out operating systems over time, none of the printer port dongles will be functional in years to come. This ensures a nice revenue stream for the new company, Safenet, and forces people to upgrade to a USB key for a cost, if they want to be able to continue to run their software on the current operating system.

Provided, of course, the software company is still in business, many companies require you to upgrade to a new version of the software. You cannot simply upgrade your key. Where would be the profit in that?

At times, the software driver interface is released into the market with known problems. In the Rainbow Technologies version 6.3 release notes for the Sentinel Superpro dongle, they list over a dozen known problems with the release. Among them, a protected application loses its license when the system goes

into hibernation or standby mode, which means it will not work. And the Superpro service loses its database of licenses and the related information when the system returns back from the paused state. So, once again, if a computer would go into a hibernation mode or a sleep mode the problem that we would have is the dongle would no longer remember the license information, and the program would not operate.

MCL Technologies note that if a user is logged in remotely the program will not recognize the dongle. They also say that other software, like Norton Internet Security 2005 can prevent the Sentinel driver from installing. And Norton, of course, is one of the most popular software programs out there with an anti-virus and firewall. Intel notes that there have been cases where third party packages have not detected their own parallel port dongle when a USB key is present.

This isn't as bad as the first time when I think I drank an entire pitcher when I testified.

I am part of the Microsoft Developers Network, and when Microsoft releases service packs and hot fixes, software developers are not given previews of that software. When Windows XP Service Pack 2 rolled out, it caused problems for many end users.

There are known issues with XP Service Pack 2, as well as other recent updates, not only for Windows XP. It may cause problems with hardware locks. No harm to the industry and continued industry growth.

The 2000 and 2003 rulemaking has had no negative effects on companies such as those that produce these dongle devices. Attached, please find the financial highlights from Aladdin Security showing their quarterly total revenue increased nicely from quarter one of 2003 through quarter four of 2005. Also attached are the results of the company Safenet. For the fourth quarter of 2005 and the 2005 annual revenue, and the reason that's included is because it was the end of 2004 is when the Rainbow Technologies company was incorporated when they bought them out.

Their financial results show that in the fourth quarter of 2005, revenue grew 21 percent. And for the year ended, it grew 31 percent. Earnings per share grew 60 percent.

The problems we have discussed over the last three rulemakings over a six-year period have not gone away or been resolved. They will only continue, since this industry does not remain stagnate but is ever-changing. The exemptions granted regarding dongles have served the purpose intended. They have

provided relief for consumers and government alike and increased the availability and use of copyrighted works. No evidence has ever been presented to the contrary.

I foresee over the next ten years an exemption that needs to be a bit broader. With changing hardware and operating systems, the lack of support for printer port devices and the consolidation of the Sentinel dongle product line, consumers need your protection now more than ever. I would respectfully suggest a new class of works. Computer programs protected by dongles that prevent access due to malfunction or damage or hardware or software incompatibilities or require obsolete operating systems or obsolete hardware as a condition of access. Again, I thank you for inviting me and look forward to your questions.

REGISTER PETERS: Thank you. Mr. Metalitz.

MR. METALITZ: Thank you very much, and I appreciate the opportunity to provide the perspectives of the 14 organizations joining together as the Joint Reply Commenters in this proceeding.

I think our position can be stated quite succinctly. We're not taking position in opposition

of the existing exemption per se. We are simply, would simply urge the Office in its recommendation and the Librarian in his action to follow the standards drawn from the statute and that were spelled out quite clearly in the 2003 recommendation and the 2005 Notice of Inquiry regarding existing exemptions. And, briefly, these are that all the exemptions are reviewed de novo, and so an exemption should expire, unless there's sufficient new evidence that the prohibition has or is likely to have an adverse effect on non-infringing uses.

I think it's fair to say that until we sat down here about 30 minutes ago there was virtually no evidence in the record that would indicate that the prohibition has or is likely to have an adverse effect on non-infringing use in the next three years, but Mr. Montero has brought in a wealth of documentation here, which, of course, we really haven't had a chance to look at. And, obviously, you haven't had a chance to look at either, but when you do so I would urge you to apply the standards that are well settled in this proceeding about the burden that has to be met.

I would say that some of what he is suggesting in the expanded class on the last page of his written testimony that he recommends. First of

all, I'm not clear whether he's recommending that now or at some point in the future perhaps. But assuming that he's recommending that you expand the exemption now, I think we would have some concerns about that. The recommendation in 2003 I think gives a good explanation of what is meant by the concept of a dongle that prevents access due to malfunction or damage and is obsolete, and I think obsolete is defined in terms of whether there's a replacement or repair reasonably available on the market. That may not be the exact wording, but something to that effect.

I think that standard is an objective one and one that's easy to apply. And also the requirement that there be a malfunction or damage to the dongle. In other words, this only applies if the dongle isn't working. I think that's also certainly an objective standard rather than standard that Mr. Montero asked for three years ago and that I think some of his testimony today would support, which is a dongle that may fail in the future. And I think the recommendation from three years ago explains well why that's not the appropriate standard.

He's also grafted in here some of the provisions of one of the exemptions that the Internet

Archive asked for, and, of course, we had the hearing on that last week in California, and I'm not sure I can add much to what I said there. But to the extent that it's relevant to this proposal and, again, to the extent that this proposal is for now and not for ten years from now, I would simply ask the Office to review the remarks that I made then and the concerns we raised in response to Mr. Kahle's proposal originally.

I'm not sure that there is much else that I can say because it's hard to comment on all this new material that's been brought here, but I would just close by asking the Office and, ultimately, the Librarian to follow the standards set out in the Notice of Inquiry and not recognize this exemption, unless there's an adequate record showing a likelihood in the next three years or a strong track record in the past three years about the inability to make non-infringing uses of software. Thank you.

REGISTER PETERS: Okay. Thank you.

GENERAL COUNSEL CARSON: Let me start with a question to Mr. Metalitz. In light of what we just received today, how would you suggest we deal with this?

MR. METALITZ: Well, I'm not sure. I

think there is some, just from flipping through it, I think there's some overlap in some of the issues. I don't know if there is in the actual exhibits, but there's some overlap in some of the issues from what was submitted last time. Again, there is some indication that there's, I think you recognized in your recommendation last time that you had evidence that people were concerned their dongles might fail in the future, and you considered that and found that was not sufficient to justify an exemption in that situation. And I don't know of any reason why that should have changed.

So I think that, to the extent that it's the ground you've already plowed, that might be one way to approach this. I don't know if there's new arguments here or new data here, both chronologically and in terms of a new argument. So I'm not sure if that's responsive to your question, but perhaps going through it with an eye toward the arguments that have already been raised and you've already considered, obviously you're free, of course you're free to come to a different conclusion on them, but I think it should be recognized that some of these are the same arguments recycled from last time.

GENERAL COUNSEL CARSON: Now, would you

like some time to give us some response in writing to this?

MR. METALITZ: We would certainly that opportunity, yes.

GENERAL COUNSEL CARSON: Okay. That's something we're going to need to grapple with. We obviously can't decide that right now. Mr. Montero, I think when Mr. Metalitz said that, up until now, the record showed not much of a record of a problem. I think that was an overstatement. I think the record before you walked in today showed absolutely nothing. And I realize you're not an opportunity, but let me just suggest to you this is not the way to present your case, and if you try to do it three years from now there won't be an exemption for sure because this is what a lawyer would say is sandbagging.

MR. MONTERO: I'm sorry, sir. How so?

GENERAL COUNSEL CARSON: We had a comment period, and people were supposed to present proposals and facts. We had a reply comment when others in support of a proposal were supposed to present arguments and facts.

MR. MONTERO: Yes, sir.

GENERAL COUNSEL CARSON: We came here to the hearing today to have witnesses to elaborate and

explain and clarify, not to, for the first time in the entire proceeding, give us their evidence because, let me make it clear, when you walked in the door today we didn't have a shred of evidence of any problem within the past three years. To ask us now to have to deal with this, to ask Mr. Metalitz now to have to deal with this, and to ask the general public which has an interest in this to have to deal with this and ask us to set up some mechanism whereby we can get comment on this is rather an extraordinary task, which, at the very least, totally sets back the timetable for this thing. This should have been done long ago.

So whether we're going to even consider what is in here is something we're going to have to deliberate on after the fact. And we may well decide we will, and we may well decide to give Mr. Metalitz and his clients an opportunity to respond. We may, I hate to even think about it, we may decide we have to make this available on our web site or something and give people another chance to submit comments because the whole point of this is to get public comment. It's, at the very least, creating great difficulties for us in our decision-making process. It's not the way to do it.

Now, let me ask you the facts that you've

set forth here, the incidents where you describe problems people have had, are these all within the past three years?

MR. MONTERO: Yes, sir.

GENERAL COUNSEL CARSON: Are these all new?

MR. MONTERO: That's correct.

GENERAL COUNSEL CARSON: All right.

MR. MONTERO: But if I may, sir, the record that I built from 2000 and 2003 remains the same.

GENERAL COUNSEL CARSON: It's irrelevant.

MR. MONTERO: It's already been established.

GENERAL COUNSEL CARSON: It's irrelevant. It's irrelevant, Mr. Montero. I'll make that quite clear. If you read the Notice of Inquiry, we do this de novo. We do not consider facts from the past as being terribly relevant today. We consider our analysis of the problems in the past. So if you came forward to us with evidence showing exactly the same problem that existed in 2003 and in 2001 it's still a problem, then there's a record on that. There's a record on the way we analyze this. But you've got to come with us and you've got to show us, yes, this is

the problem now, not this was a problem three years ago, this is a problem now. And the time to do that is when you're submitting comments, not now.

We're not equipped to address anything here at this moment. You've got to understand that.

MR. MONTERO: I believe that's the way we presented the evidence last time, in --

GENERAL COUNSEL CARSON: Well, and maybe we should have reacted a little more strongly that time.

MR. MONTERO: Absolutely.

GENERAL COUNSEL CARSON: Because it was pretty difficult for us last time to deal with, and pretty difficult for Mr. Metalitz.

MR. MONTERO: Absolutely. I would have made sure that it was presented in a timely fashion at that time. Sure, of course.

GENERAL COUNSEL CARSON: But, I mean, the point of the hearing is for us to explore this, to get explanations, to ask you questions about this. We can't begin because we don't know what's in here, and there's no way we're going to know what's in here in the scope of this hearing today.

So I don't have any questions at all because I'm not in a position to ask any questions.

But there's a big question for all of us in just how we deal with this, and I want to state, no matter what we do here, in no certain terms, next time do it right.

MR. MONTERO: Absolutely, sir.

REGISTER PETERS: Can we get a clarification, though, with regard to there's a question that you asked, Mr. Metalitz, with regard to what you say that there will be a problem in the next ten years, and then you have a language for an expanded exemption. Is that for now or for ten years from now?

MR. MONTERO: It's for now, ma'am, because the problems have occurred. And what's really different, and Mr. Metalitz brought it up, is that we've made a very strong case from 2000 forward. The difference now is that with the buy out of Rainbow Technologies by the new company Safenet, products that were in the market place for years, hundreds of thousands of these devices that have been sold are not going to be supported because the new company chose not to continue that product line.

Now, that's the drastic change in turn of events. That distinguishes this from the previous hearing, and why the modification, why the expansion

of the exemption I believe is really required.

REGISTER PETERS: First question, Steve.

LEGAL ADVISOR TEPP: I'm not sure. I did, in just flipping through this packet of documents at random literally, I thought I noticed some dated earlier than 2003.

MR. MONTERO: I don't think anything I have submitted as far as exhibits go that are numbered and the only thing that was dated before that were two articles, I believe. One of them was by Ed Foster, and the other one by Jim Seymour. I believe everything else was current.

LEGAL ADVISOR TEPP: Well, yes.

MR. MONTERO: It certainly was current since my testimony during the previous hearing.

LEGAL ADVISOR TEPP: Okay.

MR. MONTERO: During the previous rulemaking.

LEGAL ADVISOR TEPP: Well, I don't want to belabor the point that Mr. Carson has made quite emphatically. I'm not going to try and ask questions about the specifics of anything in here, having not looked at it carefully. I just do have, I guess, one question in relation to the recast exemption that you've discussed here today. Is there a reason that

you didn't put that forward in an initial comment or in the reply comment that you did submit? Has something transpired between now and then?

MR. MONTERO: No. The reply comment was essentially, I made the reply comment, but as we did in the 2003 hearing, there was such an amount of information that I felt, as we did before, to submit everything as I did now. But I didn't realize that Mr. Carson had wanted the record, you know, built before that, and, of course, that won't ever happen again.

LEGAL ADVISOR TEPP: Okay. And I think the only other question I have at this point is the proposal you're making harkens back to the original 2000 exemption, which we narrowed slightly by changing the "or" to an "and" in front of obsolete. Do you have any information, and, if it's in the packet of information, just refer to that. We'll deal with that however we deal with it. Do you have any information to suggest that the exemption as crafted in 2003 was less useful than the exemption as crafted in 2000?

MR. MONTERO: I believe so. I think the difference now is that with the devices we're talking about, even though the physical, one of these is a good example, even though if one of these devices

still may be technically functional, the problem is that it doesn't operate alone. It operates through the software and through the software operating system through a device driver. And if the device driver cannot operate on the Windows operating system, then it becomes an obsolete and non-functional device because, in all practical terms, you can't use the software program to run your program. And that's even more important now, as Microsoft goes into their newer operating systems, which was Longhorn, and now it's called Vista, but with 64 bit Windows out there, it's really a concern.

LEGAL ADVISOR TEPP: Well, there's a mention of software compatibility in what you've discussed today that was not back in 2000 or, of course, in 2003. So aside from that, I'm just trying to compare the 2000 articulation of the exception with the 2003. Putting aside additional issues that you've introduced here, just comparing the 2000 and 2003, do you have information showing that the changing the "or" to an "and" in front of "obsolete" was a significant change in the usefulness of the exception?

MR. MONTERO: I don't know exactly the way the exemption was crafted. Is the device obsolete if it can't be used on a computer essentially is the

question. If that's the case, if it's the software operating system that the device won't run on, then the device is also malfunctioning and it's obsolete because we're not able to work with the software that we intend to. So I don't know if the difference in the language has had any effect, and the problems persist.

LEGAL ADVISOR TEPP: Okay. I think that's all I've got at this point.

ASSOC. REGISTER SIGALL: Mr. Montero, I've listened carefully to your examples you described in your oral testimony of post-2003 problems. I did not hear in any of those examples involved a situation where someone wanted to use the software on the same hardware and software configuration for which they purchased the software. They all seem to involve situations where someone had migrated to either a new computer system hardware or a new operating system.

Do you have any examples of post-2003 situations where a user was unable to use software on the original hardware and software platforms for which the software was purchased due to an obsolete or broken dongle?

MR. MONTERO: Yes, sir, yes. A number of the things that I discuss in my papers, those are

people that have had problems on the same operating system. For example, the Windows XP Service Pack 2. They were running the program they wanted to run on an XP machine. When the software by Microsoft was updated to Service Pack 2, the incompatibility started to occur again in that software package. So that would be one example.

ASSOC. REGISTER SIGALL: Okay. But do you have examples of where there wasn't an upgrade or change to the underlying operating system in the software?

MR. MONTERO: Yes, sir. The example I gave with the Norton Internet Security, where somebody was using a software program but was having difficulty trying to install the software with a dongle device driver because Norton Internet Security was to blame for that.

ASSOC. REGISTER SIGALL: Okay. And in all of these cases, the problem is not the dongle is malfunctioning, the problem is either the upgrade of the software or an additionally software program that they'd like to run has created an incompatibility with the dongle or with the software that requires a dongle to operate; is that right?

MR. MONTERO: Yes, correct, or the

operating system itself, yes.

ASSOC. REGISTER SIGALL: Okay. Is it your experience in the software industry that when someone purchases a piece of software to run on a particular operating system there's no guarantee that that software application will run on future operating systems that are created that the person might choose to deploy?

MR. MONTERO: No guarantee from the software manufacturer selling their product to someone else, yes. Correct.

ASSOC. REGISTER SIGALL: There's no guarantee that, you know, if a new version of the operating system is out and they choose to employ that that that existing application that they've purchased will run on that new software or the new hardware that they've purchased?

MR. MONTERO: There's no guarantee from the manufacturer, I believe. Correct.

ASSOC. REGISTER SIGALL: Okay. Can you see how allowing an exemption that would allow people to essentially migrate software -- before I get to that question, is it also your experience that that's a major way that software developers help monetize or earn revenue for their products because they create

new versions of new operating systems and new computers that come down the line?

MR. MONTERO: Partly, yes. Partly.

ASSOC. REGISTER SIGALL: Do you think the ability for people to migrate software from one operating system to a new operating system would have any effect on the developers of the operating system or other programs in their ability to monetize that in some way?

MR. MONTERO: Speaking as a developer, I don't see any -- I think it's important that people be able to continue operating their machines, their software, but the software should certainly be able to run on another operating system and not make the software program they bought last year obsolete next year.

ASSOC. REGISTER SIGALL: Okay. But I guess my question is isn't that a fact of life in the software industry? And the question is should efforts by software developers be undermined by creating an exemption, if that's the way they choose to try to provide their software to the public?

MR. MONTERO: I don't think it should be. The software, the people that are using software are not just end users or people. Usually, these are

corporations that use software protected by these devices. In the Department of Defense example, this software is extremely important. Budget concerns usually take precedent, and there is not the budget to continue to upgrade to other software packages over and over again through the years when they've made a significant investment. And, typically, the software that we're talking about ranges in price from $3,000 to $25,000 to $100,000.

ASSOC. REGISTER SIGALL: I guess, stated another way, isn't there the expectation, though, that people who purchase software, what they're purchasing is the ability to use it on the operating systems and the hardware that is present and for which the software is defined and designed? And there's no necessarily obligation on the part of the operating system manufacturer or the software provider to include in the price, that original purchase price, the ability to upgrade to new operating systems or new software, just as a matter of course, but that's something that gets sorted out in the marketplace as to whether you have to pay more when you migrate to different systems; isn't that right?

MR. MONTERO: I don't think a consumer should not expect his software that they legally

purchased to not function another year from now when a new operating system comes out.

ASSOC. REGISTER SIGALL: I'm done.

REGISTER PETERS: Rob?

LEGAL ADVISOR KASUNIC: Okay. Mr. Montero, the only way consumers are achieving the ability to circumvent is primarily through your services, at least the people who have written in; is that correct?

MR. MONTERO: Me in particular, sir; or other people that do what do; or just in general?

LEGAL ADVISOR KASUNIC: Right. Through your or similar services or companies who provide those services.

MR. MONTERO: Yes, correct.

LEGAL ADVISOR KASUNIC: And so to that extent, the existing exemption is covering their individual acts, but it's not extending to the activity that your services are providing. How do you make these programs work when the dongle is obsolete or when you're trying to make a particular program interoperate with a new operating system? Is that a hardware or a software fix?

MR. MONTERO: It's a software operation.

LEGAL ADVISOR KASUNIC: Well, let me turn

to the only lawyer on the panel, Mr. Metalitz. Have you thought about how Section 1201(f), reverse engineering, might apply to this situation?

MR. METALITZ: Well, I thought in the last few minutes that it might apply, but I haven't gone through the examples that were just provided to us. But with the proposed expansion of this to cover, in effect, migration to new operating systems, I think that's a good example of the kind of activity that 1201(f) was directed to, which was facilitating the interoperability of two independently created computer programs. And, of course, there are certain requirements and prerequisites before you could take advantage of that exception, but I think that is probably very relevant to these situations, and it's also relevant to the fact that Mr. Montero is offering a service to others to do this because there is some provision in 1201(f) to allow sharing of the tools that are developed or that are used to facilitate interoperability. And, of course, the exemption that's before you doesn't extend that far.

LEGAL ADVISOR KASUNIC: And although I know you haven't had a chance to really think about this, do you think that, you mentioned in relation to the new aspects that Mr. Montero was mentioning, but

might it not also apply to the obsolete dongle situation or the malfunctioning dongle situation where someone has a lawful copy of a computer program and there is an independently-created computer program being created by someone else to achieve that interoperability with whatever operating system that the person is using?

MR. METALITZ: I think that's correct. At least some of these situations would involve that type of interoperability.

LEGAL ADVISOR KASUNIC: Okay. And, Mr. Montero, I think that you may have mentioned this three years ago, but let's refresh ourselves. How do you ensure that users of your software fixes are utilizing the services, utilizing that software only for non-infringing uses?

MR. MONTERO: Speaking only for myself and my company, we request a person to come in that wants to buy our software, they would have to first of all submit proof of purchase, a copy of an invoice from a manufacturer to show they are, indeed, a licensed user of the software. On the order form that we provide, it says that they've exhausted essentially all possibilities and that they request our services and help.

What we also do is the software that I do put out is also in a way copy protected so that it can't be run multiple times and, therefore, create infringements on their software where they would be able to run unlimited software versions of that program.

LEGAL ADVISOR KASUNIC: So is the software that you're returning limited to one machine?

MR. MONTERO: Yes, sir, correct.

LEGAL ADVISOR KASUNIC: Okay. That's all I have.

REGISTER PETERS: I don't have any questions either at this point. Mr. Metalitz, do you have any questions of Mr. Montero, or, Mr. Montero, do you have any questions of Mr. Metalitz?

MR. MONTERO: No. My main concern and my main point is that the situation, the environment has changed with the purchase of Rainbow Technologies by Safenet. Products that were available for manufacturers at some point to purchase additionally lock devices for an end user, for a consumer, don't exist any longer. So the software that's out there essentially is going to become useless.

MR. METALITZ: I have no questions to pose. Thank you.

ASSOC. REGISTER SIGALL: Mr. Montero, a general question about the use of dongles. In your experience in this industry, the impression that I have is that the use of dongles as a means to protect software is sort of an old thing. It's something that was done more prevalently in the 90s than it is today and that it isn't proceeding in the future with any great increase. Is that correct that using dongles on pieces of software that are developed now is a thing of the past generally?

MR. MONTERO: I wish that were the case. It's not what I've seen in the marketplace. And, typically, what I've found is that the software that would use a device like that is something that would be important. For example, just like the Department of Defense example, the gentleman cannot use, he couldn't complete his calculations and simulations without software that would do something like that, even though it was an older product. There's newer products out there, but they would have the same protection method, as well.

ASSOC. REGISTER SIGALL: But if computers these days are fewer and fewer having parallel ports and things that fit those kinds of dongles, what kinds of dongles are being used today and what kind of

ports, which ports do they work off with respect to the newer systems being developed?

MR. MONTERO: What I spoke to about the USB ports and the incompatibilities of the hardware, these devices attach to a printer port. There's other devices that are newer that would attach to a USB port. The problem is that I think the manufacturers now are not going to support these older devices on future operating systems, so that's really one of the major concerns. And even with the USB device going to a different port, there's still the inter operating system incompatibilities using the device driver that must talk between the operating system, the software, and the dongle itself.

GENERAL COUNSEL CARSON: I did have a question of Mr. Montero about what you said with respect to some of the material here that you didn't want to be part of the public record, and I just want to get some clarification on that. First of all, I'm reasonably certain that anything you gave us least time became part of the public record in that it was part of our files, it was part of what we considered, and anyone on earth who wants to come in and look at it is free to do so. Were you speaking of the public record in that respect, or are you speaking in terms

of what we put up on the web site? I just want to make sure I understand what it is you're asking us to do or not do with some of this.

MR. MONTERO: I think what did in 2003 was, because some of these were communications to my company and were marked as confidential, that they wouldn't be put on the web site, and I think that's how we did it last year.

GENERAL COUNSEL CARSON: All right. Well, depending on what we decide to do with this, one thing we may have to put to you is we may well decide we need to put whatever submission you given to us up on the web site if we decided we need to reopen this for public comment because people who might want to comment upon what you've said need to know what you've said. And I'll just speak for myself, in my view, this is really, you've just started building your case today and not earlier on in this process, so there's at least an issue with respect to fairness of the whole process as to whether this has to be put up in a publically-accessible way so that people may express support or opposition to it.

So I suppose probably the best way to do this is once we've made the determination whether we'll consider this at all, we may have to go back to

you and say, "All right, you need to tell us, if we decide we need to post this, you need to tell us what can and can't be posted," and the consequence may be that if there are parts of this that you tell us can't be posted, that just may not be considered by us at all. This is not a ruling by any means. It's just sort of giving you a sense of the issue we're going to need to address and the questions we may be coming back to you with in order to determine how to deal with it.

REGISTER PETERS: Do you have a time frame?

GENERAL COUNSEL CARSON: I have no time frame at this point, no. I think we need to sit down and figure out what we're doing.

MR. MONTERO: I have no objection. I'm sorry, no objections to Carson whatsoever. And I'm not an attorney. I think the important things, my concern was when I get something that's from the Department of Defense, from a Naval surface warfare unit, I have a little concern about making that available to the public. Most of the e-mails are not anything highly confidential, secret, top secret. You know, other than that, I have no problem with that.

GENERAL COUNSEL CARSON: You may have to

go back to some of these people if you think it's their call rather than yours. That may be what we end up doing.

MR. MONTERO: Sure. Thank you.

REGISTER PETERS: Okay. With that, we're going to conclude this hearing a little bit short of what we thought. But in any case, I want to thank both of you for testifying. We do have an open question, and we will have to get back to you. So thank you.

(Whereupon, the foregoing matter was concluded at 3:33 p.m.)