Loyola of Los Angeles
Entertainment Law Review

Volume 25
Number 1 *Symposia—At the Crossroads of Law & Technology: Fifth Annual Conference, Alternative Methods for Protecting Digital Content and Gamer Technology Conference*

Article 2

1-1-2005

# Oral Argument Before the United States District Court for the Western Districtof California in the Matter of United States v. Baltimore: A Prosecution under the DMCA

Karl Manheim

Ed McCaffery

Brad Hunt

Seth David Schoen

# AT THE CROSSROADS OF LAW & TECHNOLOGY FIFTH ANNUAL CONFERENCE

## *UNITED STATES V. BALTIMORE*[†]

## A PROSECUTION UNDER THE DMCA

*Karl Manheim,*[*] *Moderator*
*Ed McCaffery*[**]
*Brad Hunt*[***]
*Seth David Schoen*[****]

*The Honorable Ronald S.W. Lew*[§]

**MR. MANHEIM**: I'm Karl Manheim. I'm the Loyola Director of the Program for Law and Technology. And I'd like to welcome you again to the fifth annual *At the Crossroads Conference and Mock Trial.* As with all of our prior mock trials, the litigation teams consist of Caltech and Loyola students and they have been admitted *pro hoc vice* for this proceeding in the District Court for the Western District of California. For those of you who are unfamiliar of the complexities of our legal system, the Western District of California is a fictitious district. I'll introduce you to the case at issue, *United States v. Baltimore.*

(APPLAUSE)

**MR. MANHEIM**: Today's trial is actually a motion to dismiss the indictment brought by the defendants in this case. And they have two arguments as to why the case ought to be dismissed. The first is that the

---

[†] The following is an edited transcript of a panel discussion held on May 21, 2004, in conjunction with the Fifth Annual At the Crossroads of Law and Technology Program sponsored by Loyola Law School of Los Angeles. This panel is based on a hypothetical case, *United States v. Baltimore* (W.D. Cal. 2004) (No. MHP-04-9999). For an introduction to the facts of this case, see the Background section of the mock Supreme Court opinion published within this issue.

* Professor of Law, Loyola of Los Angeles Law School, and the Loyola Director of the Program for Law & Technology at the California Institute of Technology and Loyola Law School.

** Steering Committee Co-Chair, Caltech.

*** Senior Vice President & Chief Technology Officer, Motion Picture Association of America.

**** Staff Technologist, Electronic Frontier Foundation.

§ Judge of the United States District Court, Central District of California.

technological protection measures used in the Five C encryption that we heard about earlier today do not effectively control access to the underlying content, and therefore, it is not protected by the DMCA.[1] Their second argument is even if the technology is effective, the DMCA cannot constitutionally be used to stifle research and discussion in an academic environment. And therefore, they will ask that charges against Professor Law, President Baltimore and Caltech be dismissed. Since this is a hearing on defendants' motion to dismiss, they will go first. So the order of the sequence of events that are about to unfold is first, opening statements by the defense and then the prosecution, focusing on the effectiveness issue. And then, each side will present its witness and cross-examine the other side's witness. That will be followed by closing arguments, focusing principally on the constitutional issues. We are very fortunate to have presiding today Judge Ronald S.W. Lew of the Central District, a real court here in California. Bailiff, I now turn the case over to you.

**BAILIFF**: Will everyone please rise? The United States District Court for the Western District of California is now in session. The Honorable Ronald S.W. Lew presiding.

**JUDGE LEW**: Please take your seats. There's a law and motion matter on the calendar in the case of the *United States of America v. Baltimore*. And for this motion to dismiss, you have your marching order with regard to the procedure of this Court. I wish that you will abide by it. We will begin promptly by having the movant, the defendants, first make their opening statement. As you come forth, please identify yourself and then proceed into your duties of whatever it is you're calling. For opening statement, please proceed.

**MR. YOAKUM**: May it please the Court. I am Graham Yoakum from Caltech, here with my colleagues, representing John Johnson, Sundance Law, [Caltech] President [David] Baltimore, and Caltech. We're moving to dismiss the charges against the defendants on the ground that the Digital Transmission Content Protection ["DTCP"] system does not effectively control access under the Digital Millennium Copyright Act and on First Amendment grounds. I will be discussing the effectiveness issues and Ben Shapiro will answer the First Amendment question later.

The DMCA protections of effective technological controls are found in §§ 1201(a)(1), (a)(2), and (b). Section 1201(a)(3) defines that "a technological measure 'effectively controls access to a work' if the 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

1. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2000).

owner, to gain access to the work."[2] Note here that the protection must be effective under the statute for a crime to exist. The presence of the word is very important.

Congressional history reveals that there was a desire to separate effective technologies from any technology that would be applied. For example, the DMCA is based on Article 11 of the WIPO [World Intellectual Property Organization] Copyright Treaty.[3] Article 11's language evolved during its creation to become milder, refining the article to address effective technological measures, as the DMCA does. Congress has made it clear in the legislative histories that there should be some sort of restraint on how the DMCA is applied here. DTCP, the Digital Transmission Content Protection system, is not effective within these boundaries.

There is a clear history of using distributed computing attacks, much like Johnson did, to break 56-bit systems. Johnson recognized this precedent, and established his program, and it worked quickly and effectively. This is a basic design issue that's a flaw of DTCP. A larger key size would be much more appropriate and a reasonable system design should address this issue immediately. It's not something that's tricky to figure out; it's not subtle. It's an obvious point. Anyone should recognize it, and therefore, it should be the first thing that's dealt with. To not address this issue shows negligence in design that would prevent it from being considered truly effective. If you want to protect your content and make sure that no one else gets it, you use every available security measure you can. If there's an obvious way to improve security, then you should use it.

What's currently happening here is that the DTCP is hiding behind the umbrella of law, rather than evaluating new methods and creating better security systems. What's being done is there's a lackluster security system and then [plaintiffs] try to use the law to protect content, rather than looking for technological solutions. Looking for a better technological solution would improve the overall state of the art, and actually keep the information more secure than it would otherwise be. The expert witness, Seth Schoen, will elaborate more on this issue. He has a background in mathematics and computer science; he has familiarity with the technology. He can address the history of the subject, and his knowledge of design and security of encryption systems will provide valuable insight into the effectiveness, or lack thereof, of DTCP.

2. 17 U.S.C. §1201 (a)(3)(B) (2000).

3. Codified in 17 U.S.C. § 104(b)(1).

I think it is useful to note that other courts have previously accepted an overly broad interpretation of the Digital Millennium Copyright Act, using it to protect any technological measure, regardless of how well it actually performs. I would note here that this district has no precedent of this sort, and that the technologies being used here are different. Distributed computing was not an issue in previous cases, so it's very reasonable that the issues that it brings up would not have been addressed in determining effectiveness. Even if the Court decides to take this broad interpretation and look at the visual statement of the law, the case *Holy Trinity Church v. United States*,[4] from 1892, noted that the court can substitute the congressional intent for the literal wording of a case if the literal wording were to produce an absurd result. So in this case, we can look at the congressional intent of effectiveness, rather than what is actually stated. But the real issue at heart here is that John Johnson was doing an assignment for a course and he was doing it well. He did what he was assigned to do by a professor who was interested in increasing his knowledge and understanding. The government will try to depict that the defendants are some sort of digital pirates—

**JUDGE LEW**: Before you go into what the government says, let me be clear to understand what your argument is. In your opening statement, you're setting the parameters to say that you're attacking the narrowness of the application of the statute, rather than attacking the vagueness of the statute to declare it unconstitutional, is that correct?

**MR. YOAKUM**: Yes.

**JUDGE LEW**: Alright. Continue on.

**MR. YOAKUM**: The government will try to suggest that the defendants are fearsome, bold rascals and rogues. This isn't the case. They're scientists, scholars and innocent.

**JUDGE LEW**: You're saying he's not a rascal?

**MR. YOAKUM**: Well—

**JUDGE LEW**: Alright. Be careful with your adjectives. That's all.

**MR. YOAKUM**: Noted, your Honor. But we would do well to try to learn from the points that are raised in studies like this, rather than simply dismiss them and punish those who would seek to understand more and find new solutions to problems.

**JUDGE LEW**: Is that the extent of your opening statement?

**MR. YOAKUM**: Yes, your Honor.

**JUDGE LEW**: Alright. Let me hear from the other side, then. Who

4. Holy Trinity Church v. United States, 143 U.S. 457, 460 (1892).

is to proceed with the opponent's opening statement?

**MS. FU**: May it please the Court. I am Meng-Meng Fu from Caltech, co-counsel for the prosecution. I, along with co-counsel Iram Parveen Bilal, also from Caltech, and John Egley and Michael Matoba, both from Loyola Law School, along with advisors Arif Alikhan and Jim Spertus, represent the United States of America. The defense has filed a motion to dismiss. However, the law is very clear on this case. The defendants violated the DMCA, or the Digital Millennium Copyright Act. The current Five C content encryption technology is effective within the DMCA. It is used to protect the copyrighted digital content of HDTV [High-Definition Television]. Companies are able to regulate the distribution and usage of their copyrighted information because only those users with the correct decryption devices are able to view the digital information. The DMCA provides protection of such technology in this way. It prohibits the circumvention of a technical measure that effectively controls access to a work. In this case, Johnson devised a system to undermine digital content encryption. The defendants then knowingly developed specialized tools and coordinated circumvention attacks that anyone on the Internet could join. The defendants will try to argue that since Caltech is an educational institution, they are exempt under the DMCA for encryption research purposes. However, this is not supported by the facts. The defendants were notified that their actions were illegal under the DMCA. However, they refused to remove the illegal decrypting program. Furthermore, the defendants never tried to contact or—

**JUDGE LEW**: When you say "they," I'm going to start considering the differences between each of the defendants before the Court. When you say "they," are you saying that this argument applies to each and every defendant in the same way?

**MS. FU**: The argument of refusing to remove the illegal decrypting programs?

**JUDGE LEW**: Any of your arguments. There are many defendants here, so are you going to say that the argument that you're giving to the Court at this time is to be weighed equally as to each defendant? Not only as to that issue, but all the issues involved?

**MS. FU**: Apparently, only the defendants Caltech, Dr. Baltimore and Professor Law have filed the petition to dismiss on terms of First Amendment rights and vicarious liability. And so then, the student, John Johnson, is in direct violation of the DMCA. But as my co-counsel will show in closing arguments, all of the defendants are still liable and have criminal liability.

**JUDGE LEW**: Continue with your opening so I can understand

where you are at.

**MS. FU**: Thank you, your Honor. Furthermore, the defendants never tried to contact or involve the owners of the protected content. During this trial, you will hear expert testimony from Brad Hunt, Senior Vice President and Chief Technology Officer of the Motion Picture Association of America. Mr. Hunt has been working in the motion picture and television industry for over twenty-five years. He helped establish one of the earliest DVD pre-mastering and MPEG compression companies, and in addition, he is currently involved in the legal, technical, and commercial aspects of copyright protection of digital media. Mr. Hunt will tell you about the Five C technology. And based on his testimony, it will become very clear that the current Five C technology is effective within the definitions of the DMCA, for three main reasons. First, the current Five C is effective—

**JUDGE LEW**: How are you making that argument when the term is not clearly defined in the statute?

**MS. FU**: The effectiveness statute?

**JUDGE LEW**: Yes. How are you going to argue that?

**MS. FU**: Our interpretation of the effectiveness statute is that the Five C technology was issued to prevent ordinary users from circumventing the technology. It is not foreseen that any person in the average home would try to link a connection of networks—composed of tens of thousands of computers—to try to hack the 56-bit encryption.

**JUDGE LEW**: That is your argument. I accept your argument, but you're referring to the statute itself with the definition of effectiveness. You're not trying to imply that there is a definitive term within the statute, are you?

**MS. FU**: No, your Honor.

**JUDGE LEW**: Continue, please.

**MS. FU**: Thank you. First, the current Five C is effective because it has been designed to prevent people with ordinary technical skills and computing power from breaking the encryption. The Five C protection technology does not contain any inherent weaknesses that would allow circumvention with a specific algorithm or code. Furthermore, prior to this case, the Five C technology has never been successfully broken. Johnson was only able to decrypt that information using a brute force attack. A brute force attack involves a massive network that links the distributed computing power of tens of thousands of computers. That is, his program coordinated these linked computers to try every possible encryption key until it found the right one. A central coordinator, in this case the defendant's, is essential for such a network to work. The ordinary user would neither be able to devise nor access such a network without the

central coordinator.

Second, the current Five C content protection is a robust technology, since it is further fortified by the fact that content encryption keys change at least every two minutes. Thus, to circumvent the copyright protection of a typical movie file, dozens of decryption keys would have to be discovered.

Third, Five C uses 56-bit encryption, which translates to over seventy-two quadrillion possible keys. Seventy-two quadrillion is "72" followed by many, many zeroes.[5] The defense has suggested that this 56-bit encryption is insufficient and insecure, and they have suggested increasing the number of bits in this encryption. However, this would result in cost increases to both the consumer and the industry. In addition, this would render current lawful decryption devices, such as those currently in use inside HDTVs, useless, since interoperability problems would emerge between new and old devices.

For all of these reasons, the current Five C is an effective technological measure under the DMCA because it prevents ordinary users from illegally accessing copyrighted digital content. And thus, we believe, it is protected under the DMCA. And by circumventing this technology, the defendants are in blatant violation of the DMCA. Your Honor, by the end of this trial, my co-counsel John Egley and Michael Matoba will explain why this case can not be dismissed for the following three reasons: one, that the First Amendment is not an obstacle to the enforcement of the DMCA; two, that the Five C technology is effective within the DMCA; and three, that criminal liability can be attached to all of the defendants. Thank you.

**JUDGE LEW**: You made the conclusion, but you never support the argument about the First Amendment not being applicable.

**MS. FU**: Your Honor, those arguments will be addressed in our closing statement, since opening is only regarding the effectiveness of the technology.

**JUDGE LEW**: I will patiently await that then.

**MS. FU**: Thank you.

**JUDGE LEW**: Thank you very much. The parameters for the case have been set forth in the opening statements by both sides. Let's look at the technologies to be presented by each side to support your arguments. I will ask that the movant proceed first by calling your first witness.

**MS. FU**: Go to the stand. Your Honor, may I approach the witness?

**BAILIFF**: Do you affirm that everything you say here today will be

5. "... [A] quadrillion is equal to one with fifteen zeros, namely: 1,000,000,000,000,000 ($10^{15}$)." WIKIPEDIA.ORG, at http://en.wikipedia.org/wiki/Quadrillion (last visited Oct. 16, 2004).

the truth or a close facsimile thereof?

**MR. SCHOEN**: I do.

**JUDGE LEW**: What is the purpose of your approach?

**MS. FU**: I would like to show him the curriculum vitae that I am about to speak of.

**JUDGE LEW**: Is it his?

**MS. FU**: Yes.

**JUDGE LEW**: I think he'd know instantly.

**MS. FU**: Okay. This curriculum vitae that I have, the one that you have given to us, do you affirm that it is accurate?

**MR. SCHOEN**: The last time I saw it, it was accurate.

**MS. FU**: Well, let's just go over a couple of the important points of that. How did you become an expert in the field of cryptography and cryptoanalysis?

**MR. SCHOEN**: I've been interested in computer security for quite some time. I had an unprofessional, or a non-professional perhaps would be better, interest in computer security for many years. And in recent years, I've had a professional interest in computer security in the course of my employment at the Electronic Frontier Foundation.[6]

**MS. FU**: Now, what is that?

**MR. SCHOEN**: The Electronic Frontier Foundation is a not-for-profit organization based in San Francisco that performs advocacy and legal services to advocate free expression and other freedoms in the online environment. And in the course of that employment, I've attended a number of conferences. I've read a number of technical articles and magazine articles, and participated in online forums to keep current in the field of computer security.

**MS. FU**: Could you please describe your educational background?

**MR. SCHOEN**: I have a high school diploma from Northfield Mount Herman School in Northfield, Massachusetts, and I attended UC Berkeley, studying computer science and mathematics. I then left Berkeley to pursue professional opportunities in the field of computing.

**MS. FU**: Could you please describe how your current employment is keeping you up to date with new developments in these fields?

**MR. SCHOEN**: I write technical reports, technical white papers, and perform research to support our attorneys in the performance of their legal duties. I attend conferences and events and give presentations at those events. About once a month, I have the pleasure of seeing the prosecution's

6. The Electronic Frontier Foundation can be found at http://www.eff.org.

expert, Mr. Hunt, at the Copy Protection Technical Working Group,[7] here in the Los Angeles area. I think those are a few examples.

**MS. FU**: In your own words, how does encryption work?

**MR. SCHOEN**: Encryption is a part of the science of cryptography. And encryption refers to a set of mathematical techniques for transforming information mathematically, in order to scramble it by the use of a key. The intent is that when the information has been scrambled in this way, it will be unintelligible, except to those who are in possession of the appropriate decryption key.

**MS. FU**: So specifically, how does this Five C technology encryption work?

**MR. SCHOEN**: Five C is a fairly large topic, but I will give it an attempt. Five C is the Digital Transmission Content Protection system developed by five companies, hence the Five C. This is a system that attempts to enforce policies against end-users related to the use of audiovisual works that the end-users have obtained. And it used encryption, among other technologies, in furtherance of this objective. So, a DTCP device typically will have received a license from a licensing entity. And the DTCP device will work by encrypting audiovisual works within the device. Although there are copy restrictions and other restrictions enforced by DTCP, it may sometimes be possible to send audiovisual works from one DTCP device, or one Five C device, called a source device, into another device, called the sync device. This depends on the policies that the publishers of the work have set. In that case, the DTCP devices use encryption in a way known as link encryption, so that no one who records the conversation between the source device and the sync device would, they hope, be able to understand the substance of it or to obtain a usable copy of the work.

**MS. FU**: Can you describe how Mr. Johnson was able to successfully mount an attack on the system?

**MR. SCHOEN**: Well, I would first emphasize that to my knowledge, and to my understanding, Mr. Johnson did not actually intend to attack the DTCP. He intended, specifically, to attack a different system that was not commercially deployed, not commercially used, that was developed by his colleague, Mr. Skylor. It seems that the technology that he developed for this purpose was applicable to DTCP as well, and, in my understanding, that technology is a so-called distributed computing system that helps people who want to participate in performing what's known as a brute force attack. That is to say, it is an attack that proceeds by trying

7. Copy Protection Technical Working Group can be found at http://www.cptwg.org

every possible key, one key after another. In my understanding, Mr. Johnson's program is a distributed computing program that was used by other people, not by Mr. Johnson himself, to successfully decrypt a movie that had been encrypted with DTCP. Presumably, the movie was sent from one device to another device in encrypted form, and presumably someone recorded the conversation between the two devices. The publishers might hope that the conversation would be in scrambles and unintelligible. But it seems that people with the aid of Mr. Johnson's program were able to find a key that made it make sense again.

**MS. FU**: You were talking about distributed computing. Can you give some examples of its uses in other fields, perhaps?

**MR. SCHOEN**: Probably the most familiar example of distributed computing to the public is a project called *SETI@home.*[8] *SETI@home* was developed by the UC Berkeley Space Sciences Laboratory as a way of allowing the general public to participate in the search for extraterrestrial intelligence. The scientists take radio waves from outer space, they record them, and they send them out. They distribute them—hence distributed computing—to members of the public who donate their computing resources to work together on the difficult computational problems of looking for statistical anomalies that might indicate some kind of communication from another civilization. So that's probably the most familiar. There's also a project that's made a lot of progress in number theory in mathematics: finding large prime numbers of a type called Merced Primes. For many years now, the largest prime number known to humanity has been discovered through distributed computing efforts, where people from around the world pooled their resources to work together on a problem. So I want to suggest that distributed computing has led to a lot of scientific progress and scientific advance, within computer science in terms of exploring how distributed computing works, and how it can be made better, and in terms of attacking problems. I also know that it has commercial uses in drug discovery and even in petroleum exploration for oil companies.

**MS. FU**: Would you describe the Five C encryption as an effective means of controlling access to a technology?

**MR. SCHOEN**: Well, it seems that in this case, it was defeated. So it doesn't seem that it was very effective. I recognize that there is a great deal of controversy over the legal meaning of the word "effective." I am

8. SETI is an acronym for Search for Extraterrestrial Intelligence. J.A. SIMPSON & E.S.C. WEINER, THE OXFORD ENGLISH DICTIONARY (Oxford University Press), *at* http://dictionary.oed.com (Dec. 2002).

not a lawyer, and I am not here as a legal expert, so I don't know what exactly to make of the legal controversy over the word "effective." I would emphasize the technology did not, in fact, survive this attack. It was defeated. More than that, I would emphasize that this successful attack could have been anticipated by the developers of this technology. I believe that there are clear technical reasons why people who develop technology, like DTCP, would have known that DTCP would successfully be attacked in this way.

**MS. FU**: Does that involve this 56-bit key?

**MR. SCHOEN**: That's correct. One of the components of the DTCP system is the use of an encryption system, or a cipher, that uses a key of 56-bits. That's seven bytes. I recall that the attorney for the United States emphasized that 56-bit encryption leads to a large number of possibilities. I believe she said seventy-two quintillion,[9] which is certainly a larger number than I've ever counted to. At the same time, computers are not like us. They're very stupid, but they think very quickly. To a computer, I think seventy-two quintillion is not such a daunting number as it might appear to a person. The capabilities of computers and the capabilities of people are on separate scales. Computers really can perform mathematical operations with remarkable speed that has been getting faster all the time. And so with regard to 56-bit ciphers, as I said in my expert statement, during the 1990s, several people, including the Electronic Frontier Foundation, where I am now employed, actually publicly demonstrated the capability to mount a brute force attack that was successful against 56-bit ciphers. So, not only had it been conjectured in the academic literature that probably this wasn't enough against a knowledgeable attacker, but in fact, it was demonstrated several times in the 90s, that these attacks could be successful and could be mounted. It was not merely conjectural.

**MS. FU**: Can you explain, then, why industries like the movie industry have continued to use the 56-bit encryption system?

**MR. SCHOEN**: Well, obviously more effective technologies certainly are available to them. The United States National Institute of Standards and Technology,[10] for example, has issued a national standard. I can talk more about that if you'd like. That's a system that starts at 128 bits, which is substantially stronger. And technologies like that are available, certainly. And so, it seems that there are other reasons. I'm

9. One quintillion is "the number equal to $10^{18}$, written as '1' followed by eighteen zeros." MSN Encarta, *Dictionary*, *at* http://encarta.msn.com/encnet/refpages/search.aspx?q=quintillion (last visited January 1, 2005).

10. The National Institute of Standards and Technology can be found at http://www.nist.gov (last visited Oct. 23, 2004).

aware of two; there may be others. I'm aware that some device manufacturers were concerned about power consumption. They said, if we use state-of-the-art encryption like 128-bit encryption, it will burn more power in our player devices. The batteries won't last as long, and so consumers will be disappointed, because their batteries will run out. The battery companies will be happy, but the consumers won't. So that was one reason. They felt that if they used what I would characterize as obsolete, 56-bit key length, it would produce devices that consumed less power. And as far as I know, that is correct. It has no bearing on the ease with which someone could defeat it, but it is a reason. The other reason is that in the past, and perhaps at present, some governments have imposed restrictions on the availability of certain cryptographic devices. To my knowledge, United States law—and I'm not a legal expert—never significantly restricted the use of encryption technologies in digital rights management applications. But it seems that there are other countries where these technologies may be restricted. And it's possible that device manufacturers wanted to expedite the process of selling their devices in such countries.

**MS. FU**: But what is really the—

**JUDGE LEW**: Are you moving into another area?

**MS. FU**: Okay—

**JUDGE LEW**: Are you moving to another area?

**MS. FU**: We have a couple of questions about—

**JUDGE LEW**: Let me follow up. What is the national standard that you referenced?

**MR. SCHOEN**: The national standard is called the Advanced Encryptions Standard ["AES"],[11] your Honor.

**JUDGE LEW**: But what is that for?

**MR. SCHOEN**: It's an encryption system that can be used for any application that requires a symmetric key encryption system.

**JUDGE LEW**: But when you're talking about any application, does it make reference to digital?

**MR. SCHOEN**: To this kind of application, your Honor?

**JUDGE LEW**: This particular kind of application.

**MR. SCHOEN**: The National Institute of Standards and Technology operates at a very high level of abstraction. So they didn't really spell out specifically what this technology was meant for; they said it was encryption

11. *See* The National Institute of Standards and Technology, *at* http://www.nist.gov/aes/ (last visited Oct. 23, 2004).

of a certain type. And they left it to the experts to decide.

**JUDGE LEW**: If you're the expert in this area, why do you leave such a big opening gap to refer to a national standard, when the standard itself is vague in its own application?

**MR. SCHOEN**: I'm sorry. I didn't understand that question, your Honor.

**JUDGE LEW**: Well, you're saying the national standard doesn't make reference to the digital application in the movie rights area, correct?

**MR. SCHOEN**: That's correct. I think that's because the people who would be implementing that technology, being experts themselves, are qualified to determine what the technology is good for. So, for example, if the National Institute of Standards and Technology says that a meter is a certain size, they don't say for use in measuring bridges, or they don't say for use in measuring construction materials. They simply say, we're issuing a standard which is technically useful to any expert who finds an application for it. And, your Honor, I think that's what happened in the case of the AES system.

**JUDGE LEW**: Your next question.

**MS. FU**: How much more secure is the 128-bit system versus the 56-bit system?

**MR. SCHOEN**: Well, if you just look at those two numbers you might think that it's something like twice as secure, because 128 sounds about twice as big as fifty-six. But the great thing about bits is that each time you add one bit, you double the number of possibilities, so that's actually a very significant increase. My arithmetic skills are not up to calculating the exact factor, but it's essentially an unimaginably large number, because each added bit is going to double the number of possibilities. So for example, since it's more than double, it's going to be more than quintillions of times as many possibilities.

**MS. FU**: And what are the added costs of the 128-bit system versus the 56-bit system, in your opinion?

**MR. SCHOEN**: If you were implementing it into a computer—

**JUDGE LEW**: That's a vague question, why don't you narrow it down: Costs to the manufacturer? Costs to the end user? What are you talking about?

**MS. FU**: Cost to the manufacturer, in his expert testimony, Mr. Brad Hunt was referring to.

**MR. SCHOEN**: Well, if you were implementing it into a computer, for example, I think the costs on a modern computer system would be virtually negligible. If you were implementing it in hardware, it would

require additional hardware and it would be more expensive. I am not an electrical engineering expert, but I believe it would be on the order of cents per device to increase the encryption strength that way.

**MS. FU**: In Mr. Brad Hunt's pre-filed expert witness testimony, he claims that Five C technology is an effective means of controlling access because the key is changed every two minutes. Do you agree?

**MR. SCHOEN**: Well, earlier I said that seventy-two quintillion is not a human-scale number. On the other hand, a number like two minutes is a human-scale number. So to be more precise, if the key is going to change every two minutes in a movie that's one hour long, that's going to be thirty different keys. And so you're going to have to recover thirty different keys in order to successfully decrypt that entire movie. Now, thirty is a very human-scale number. So, for example, if you had an attack that worked in one day, and now you have these thirty keys to break instead of one, your attack is going to take a month, which is a long time, but not longer than people's capacity to wait. Also, there's this phenomenon known as Moore's law,[12] which predicts computer power increases. At least in the short term, regular predictable way, the general consensus is that available computer power roughly doubles every eighteen months. That's the way they put it in the industry. That would mean that in order to make it as easy to break thirty keys as it is now, you would just have to wait for five doublings, because that's a factor of thirty-two. And so that would be some time in the next five to ten years. At that time you would expect it to be just as easy to attack thirty keys as it is to attack one now. And that's what I mean by a human-scale number; things that people can actually deal with that will be realistic in the short term.

**MS. FU**: And according to Moore's law, how long would it take for the doubling to reach the 128-bit level?

**MR. SCHOEN**: My calculation earlier is that if Moore's law continues—and there is a good deal of doubt about that—and doesn't run into any fundamental physical limits, we would expect that it would take about a century to make up, in computer power, the difference between a 56-bit key and a 128-bit key. And I think that the technologies here are intended to last, say, five to ten years. They're just being deployed now, but are not necessarily intended to last a century. So I do think it makes a

12. J.A. SIMPSON & E.S.C. WEINER, THE OXFORD ENGLISH DICTIONARY (Oxford University Press), *at* http://dictionary.oed.com (Dec. 2002) ("[a] broad principle relating to the rate at which the density of transistors in integrated circuits, and hence the power and miniaturization of computers, is expected to increase with advances in microchip technology, originally predicted by Moore as approximately doubling every year now modified to approximately every two years.").

concrete difference.

**MS. FU**: Really quickly, what are the consequences of using the legal standard that the government would like us to use?

**MR. SCHOEN**: Well, I'm concerned that if anything at all is considered effective and receives legal protection, then there's the issue about the incentive of people to deploy systems that are actually secure. In other words, if they're going to deploy systems that the consensus of the cryptographic community is against, that security people say are predictably and expectably subject to attack, that's a real problem for the development of technology and the incentives to improve technology. I think in every other area of computer security, people are concerned about improving their security using the state of the art technologies. And it seems in the DRM[13] world, because of the breadth with which, perhaps other courts have interpreted "effective", people have felt that almost anything goes; that you can just deploy something and you made an effort, and you can just keep using it. So I'm concerned about that.

**MS. FU**: Thank you, your Honor. No further questions.

**JUDGE LEW**: Alright then, cross examination?

**MS. WADA**: Good afternoon.

**MR. SCHOEN**: Good afternoon.

**MS. WADA**: You mentioned earlier that seventy-two quadrillion is really not that large of a number for computers, correct?

**MR. SCHOEN**: Yes, I did.

**MS. WADA**: And a 128-bit system is several times larger. So on the same note, it's really not that large for a computer either, is it?

**MR. SCHOEN**: Well, I guess it all depends on what you mean by large for a computer. I guess it's the difference between whether a computer could count up that high in a couple of days, or whether a computer could count up that high in longer than the edge of the universe. So, I mean, to a computer, all numbers are numbers and there's no such thing as big or small. But computers actually deal with objects that are on the range of 56-bits of possibility. They actually manipulate them and do useful work on them. I'm not sure in the cryptographic context if the same thing is true of 128.

**MS. WADA**: Okay. And in the numbers of combinations, specifically in the Five C technology, about how many different

13. Digital Rights Management systems "use encryption technology to securely protect digital content and to bind the set of digital usage rights associated with the content." See Summary of Expert Statement of C. Bradley Hunt, MHP 04-999, *available at* http://techlaw.lls.edu/events/atc2004/Prosecution_Expert.pdf (last visited Oct. 23, 2004).

combinations are there?

**MR. SCHOEN**: Well, it's precisely true to the fifty-sixth power, which I believe we were saying was seventy quintillion, which accords with my memory. The number is in my testimony.

**MS. WADA**: Okay. And how many zeroes is that?

**MR. SCHOEN**: Quintillion. I'm going to have to count on my fingers. Would you like that?

**MS. WADA**: An approximation—

**MR. SCHOEN:** Well, just to know the number of zeroes, quintillion is eighteen zeroes.

**MS. WADA**: Okay. Thank you. So, in order for one computer, say a computer that someone were to pick up from Best Buy, and they were to work in a brute force attack on the seventy-two quadrillion different combinations, how long would it take this one computer to figure this out?

**MR. SCHOEN**: I don't have the current statistics about the speed of current computers. I'm certain that for one computer, it's an extremely long time, and certainly many years, even with current technology.

**MS. WADA**: So would you say that it's maybe in the decades?

**MR. SCHOEN**: I would easily believe that it was longer than that, yes. So the distributed aspect of this is clearly very significant. You clearly gain a major advantage by being able to take advantage of the contributions of many people, not just one computer.

**MS. WADA**: Okay. Well, turning to that aspect, then, you need a certain level of skill and technology to coordinate such a vast endeavor, correct?

**MR. SCHOEN**: At least the technology to coordinate such an endeavor has to be invented by someone with some skill. It's not necessarily an original invention, but it is a substantial technical problem that you would have to solve. Obviously, inventing the technology and actually coordinating it, as we can see in this case, are not necessarily things that were obviously done by the same person. But I would agree with the suggestion that inventing the means of coordinating such an attack does require a significant level of technical skill.

**MS. WADA**: Well, in this case here, they were able to accomplish this, I guess, seventy-two quadrillion in a day. How many computers would be involved in this endeavor?

**MR. SCHOEN**: I really don't have any data that would allow me to calculate that. We haven't been given key rate estimates, or learned how optimized the search code was, or anything of that nature. So I'm afraid I really can't calculate it.

**MS. WADA**: Can you give an estimation of how many computers it would take?

**MR. SCHOEN**: My expertise in that is really not so current, but I would suggest on the order of thousands of computers. If I had a calculator I might be able to make it more precise.

**MS. WADA**: Okay, so thousands. Maybe tens of thousands?

**MR. SCHOEN**: I think that's also possible.

**MS. WADA**: So let me get this straight, just to kind of sum up what we've gone over so far. In order for one computer to figure this combination out, this key combination, it would take several decades. So, an ordinary person who would attempt to break this with their home PC might not even be alive when the computer finishes this calculation.

**MR. SCHOEN**: In fact, I once attempted to break a different 56-bit cipher with my own home PC. I did receive an estimate of when it would finish, and I would certainly not have been alive. Now, computers have gotten a lot faster, so it would be gratifying to learn if I could actually survive to see that happen. But I think distributed computing is really the wave of the future in this area.

**JUDGE LEW**: Do you recall the question?

**MR. SCHOEN**: So the question was whether one person would even be alive, and I was trying to suggest—I'm sorry, your Honor—that the person would probably not be alive.

**MS. WADA**: So, you mentioned that 128 is, you said, a better method of decryption. But it's not perfect, is it?

**MR. SCHOEN**: I suggested in my testimony that there's only one kind of perfect encryption, called the one-time pad. And by definition, all other kinds of encryption are not perfect. So, yes, that's correct. It's not perfect.

**JUDGE LEW**: So are you going to imply by your answer that the movie industry should only use that?

**MR. SCHOEN**: Well, I think there is a meaningful difference. And I don't mean to speculate about the legal standard, your Honor—

**JUDGE LEW**: Well, by your own standard. You're admittedly not able to speak on the legal standard, but you were making many comments with regard to your standard in your industry.

**MR. SCHOEN**: Well, I think what I'm suggesting is that people in computer security traditionally would be concerned about what kinds of attacks are foreseeable. And so, I believe that the current consensus is that a purely brute force attack against a 128-bit system is not foreseeable, and an attack of that nature against a 56-bit system is foreseeable. It's not

foreseeable by one individual at home, but it's foreseeable in terms of people actually doing such things. They've publicly demonstrated that they do such things.

**MS. WADA**: You mentioned earlier that the 56-bit system is not effective because someone broke it. So are you saying that when a person puts a lock on their home and a robber breaks in, the lock was ineffective?

**MR. SCHOEN**: I guess it depends on whether the lock provided some other benefit to them that they cared about. Well, for example, in security, people talk about a lock in terms of how it increases the chances of a burglar being caught. So it might be effective in that way even if, perhaps the burglar can actually break it. It's a difficult question. It seems like a somewhat subjective question. Do you want to try to ask it a different way?

**MS. WADA**: Well, it seems that a lock keeps most people out of a home, and it's very effective at doing that. Just because a few people get in, doesn't mean that the lock has become inefficient to the entire society, does it?

**MR. SCHOEN**: I guess there's a difference between effective. I don't want to suggest that systems that have known successful attacks against them were necessarily useless. I want to suggest that if you learn about a capability of breaking something, depending on what kinds of attacks you're concerned about, it's likely to be worth your while to try to upgrade the security.

**MS. WADA**: And you mentioned about EFF's attempt to do a brute force attack in the past, correct?

**MR. SCHOEN**: Yes.

**MS. WADA**: And didn't they invest over $200,000 in a specific computer to try and specifically crack this code?

**MR. SCHOEN**: That's correct.

**MS. WADA**: So, this type of technology isn't available to the general public, is it?

**MR. SCHOEN**: Well, EFF published a book, which I have over there at the defense table, describing exactly how to build such a machine. So that will knock something off the cost. That approach is still cost-prohibitive for the average person. It's not cost prohibitive for some people who would have a real-world incentive to hack. So, a lot of it comes down to what kind of attacker you're concerned about. We published a book that says, here is how to build a machine that will successfully attack, and very quickly. In 1998, that machine cost nearly $200,000 to construct. Because of Moore's law, the cost has been falling. It's still not something that I

could afford. I don't think it's something that many people in this room could afford to buy at home. I don't think this means that it doesn't contribute to our understanding of the insecurity. But I'll never have one at home, I'm afraid.

**MS. WADA**: So, after going through one computer working decades on this, and then I guess breaking it after decades, ultimately they would only get two minutes of content. Wouldn't they?

**MR. SCHOEN**: I think that's correct. But someone needs to consider some version of this scenario so plausible that they're willing to try to send people to jail to prevent it from occurring in the real world. So, someone is afraid of something.

**JUDGE LEW**: You're not the jury here. Let's answer the question so that we can complete your examination, and you can keep the opinions to yourself, unless it's a part of the answer. Your next question?

**MS. WADA**: Thank you, your Honor. So, an average person, who goes to Best Buy and picks up a standard computer, would not be able to break into the Five C technology in a reasonable amount of time. Is that correct?

**MR. SCHOEN**: Not using a pure brute force attack.

**MS. WADA**: May I have a moment, your Honor? So, ultimately, what you're saying is that for the average person, it's not very plausible that they would be able to break into this Five C technology?

**MR. SCHOEN**: Certainly not acting alone with no other resources.

**MS. WADA**: So isn't that effective? Effectively keeping most people out?

**MR. SCHOEN**: I guess I want to distinguish between effectively keeping most people out and effective.

**MS. WADA**: What's the difference? If most people are kept out, then a security system has served its purpose. There are always going to be a few people who have the knowledge to go way beyond and break any system, aren't there?

**MR. SCHOEN**: I never met anyone who had the knowledge to launch a successful pure brute force attack against a 128-bit cipher. If I knew of such a person, or believed in such a person, I would use very different technology to protect my own e-mail, for example. I currently entrust my own e-mail to a 128-bit cipher.

**MS. WADA**: And until this trial, there hasn't been a breach of the Five C technology, 56-bit technology has there?

**MR. SCHOEN**: Certainly not by anyone who wanted to publish or publicize it.

**MS. WADA**: Okay. Thank you. No further questions.

**JUDGE LEW**: I may have missed it, but would you enlighten me? I'll ask you a direct question. How long has the Five C technology been in place?

**MR. SCHOEN**: I believe that the early versions of the Five C technology were developed around 1999. I think I have a precise year in my direct—

**JUDGE LEW**: Okay. It was approximately in 1999?

**MR. SCHOEN**: But I don't think products that incorporated it went on sale until just about a year ago, or two years ago. Perhaps Mr. Hunt has more specific information about that.

**JUDGE LEW**: Well, I think they'll remind me at their closing argument.

**MS. WADA**: Your Honor, could I ask one follow-up question, if I may?

**JUDGE LEW**: Sure, you may.

**MS. WADA**: Thank you. Five C technology, you mentioned a national advanced encryption system. That's not nationally used though, is it?

**MR. SCHOEN**: It's used by the U.S. government. The federal law requires that the U.S. government, for certain applications, employ technologies that are better known as Federal Information Processing Standards.[14] And the advanced encryption system is a Federal Information Processing Standard, so portions of the U.S. government are required to use it and do use it.

**MS. WADA**: But most people use 56-bit encryption, don't they?

**MR. SCHOEN**: I have no basis at all for saying what sort of encryption most people use. I know many people, including EFF, published recommendations advocating for security considerations against the use of 56-bit encryption. But, I have no way to know how effective those suggestions, those recommendations were.

**MS. WADA**: Thank you, your Honor. No further questions.

**JUDGE LEW**: You may step down.

**MR. SCHOEN**: Thank you.

**MS. BILAL**: Your Honor, may it please the Court. I'm Iram Parveen Bilal from Caltech, co-counsel for the prosecution. The United States of America calls Mr. Hunt.

---

14. Federal Information Processing Standards can be found at http://www.itl.nist.gov/fipspubs.

**BAILIFF**: Do you affirm to tell the truth today, or a close facsimile thereof?

**MS. BILAL**: Good afternoon, Mr. Hunt.

**MR. HUNT**: Hello.

**MS. BILAL**: Would you please introduce yourself to the Court and please tell them what you do for a living?

**MR. HUNT**: Yes. My name is Brad Hunt. I'm the Chief Technology Officer for the Motion Picture Association of America ["MPAA"],[15] which is a trade association made up of the seven major motion picture studios in Los Angeles. And I provide guidance, information, and policy-making facilitation to our member companies on a number of technical-related topics, such as copy protection, anti-piracy and Internet security issues.

**MS. BILAL**: How long have you been with the MPAA?

**MR. HUNT**: I've been here about five years.

**MS. BILAL**: Thank you. What did you do before you became the chief technology officer?

**MR. HUNT**: Well, I've been involved in the motion picture and television industry for over twenty-five years. I started in research and development in motion picture film products. I've been involved in digital imaging. I'm sort of a computer audio-video hobbyist and that moved my career, really, into the areas of digital technology. And again, I joined the MPAA in 1999.

**MS. BILAL**: Does that more or less outline most of what you did before you became the chief technology officer?

**MR. HUNT**: I've been involved in the digital post-production field. I was chief technology officer for a post house in Los Angeles and helped establish one of the first DVD pre-mastering and MPEG2 compression facilities. So, I was one of the lucky individuals at the beginning of the DVD marketplace offering DVDs for the marketplace.

**MS. BILAL**: Your Honor, we're going to go by our claims as we talked about in our witness statement. So, claim one, the effectiveness of the Five C Digital Transmissions Content Protection technology within the DMCA. My first question to you is: how do we create digital content?

**MR. HUNT**: Well, digital content starts with an analog signal that's sampled. Each sample is measured, and the measurement is quantized into a number that's converted into binary digit bits, which can be easily stored and processed by a digital computing device. So, that's how we digitize

15. Motion Picture Association of America can be found at http://www.mpaa.org.

information, and that's how we create digital content, digital movies.

**MS. BILAL**: What are the benefits of storing content in digital form?

**MR. HUNT**: Well, having content in a digital form is one benefit. It can be transmitted and conveyed in a lossless manner, so that there's no degradation of the signal of the content. Two, you can make perfect copies of the content to deliver so that each copy is identical to the original. So, there are some quality benefits and delivery benefits, in terms of getting content in a digital form.

**MS. BILAL**: Alright. So, bringing this to more specifics, the Five C Digital Transmission Content Protection technology exists in order to prevent such copying. How exactly does it work?

**MR. HUNT**: Well, the Five C technology is a link encryption technology. It allows for two devices, a digital source device that has the digital content and wants to transmit it across a digital interconnect, to a digital sync device that may render and display the content, or may make a copy of the content. So the way the Five C technology works is that a manufacturer that wants to build a device with the Five C link encryption technology signs a license, which dictates how it will build the product and how it will handle this copyrighted or protected content. The Five C also allows the manufacturer to gain access from the license or the technology to the digital certificates that allow the devices to authenticate and establish a trust between the two devices and the digital key material. This allows the processing of the encryption keys to be able to encrypt the content so that it moves across the connection, and then can be decrypted by the same device to be able to gain access, to render, or make a copy of the content.

**MS. BILAL**: So, unless you have a device that is licensed to get the data from the original, whatever encrypted content you're doing, it is considerably hard to obtain the data, right?

**MR. HUNT**: Yes. If there is an unlicensed device that does not have the digital certificate to validate its trust from the source, the Five C source device that is sending, transmitting the protected digital content cannot authenticate itself and get the content encryption key to be able to decrypt the content. So, in fact it has no ability to access the content in a usable form.

**MS. BILAL**: Right. In your expert opinion, would you please outline the exact need to have digital content protection technology?

**MR. HUNT**: Well, digital content protection technology is very important because of the great harm that can occur from lossless copying and redistribution of the content. It is important to be able to protect the content and associate it with rights that a content owner may want to

convey. The DVD video format is a good example. Content owners would never be able to sell DVD movies for less than $20 a copy if every copy of this movie on DVD could be easily copied and distributed over the Internet. There would be quite a different price. So, from an economic standpoint, one can think about digital content protection technology as a tool that facilitates the most cost-effective transaction between a content producer and a content consumer.

**MS. BILAL**: Right. So, you're asserting that in addition to protecting the content from a legal perspective, it's also an economically beneficial system?

**MR. HUNT**: Certainly, there are many benefits to digitally delivering and distributing content. For example, for consumers, the high quality that can be conveyed by digital content provides many benefits to consumers. But in fact, there has to be protection for content owners to prevent unauthorized access, unauthorized copying, and unauthorized redistribution, including over the Internet.

**MS. BILAL**: Coming back to Five C DTCP technology, how familiar are you with it?

**MR. HUNT**: Very familiar.

**MS. BILAL**: And how?

**MR. HUNT**: Having worked at the MPAA very closely with our member companies, I dealt with the Five C companies on the technical aspects of the DTCP technology, and I also helped facilitate the negotiation of the non-economic terms of the DTCP license. This occurred during the late 1990s into the 2000 time period.

**MS. BILAL**: So, in your expert opinion, does the Five C DTCP technology prevent illegal access, usage, and duplication by individuals?

**MR. HUNT**: Yes, it does.

**MS. BILAL**: And how? Why do you say that?

**MR. HUNT**: Well, it's an effective technological measure that's being deployed in probably over 100 different products these days. It's been in the marketplace for about three years. Just recently, in the FCC ruling on the digital cable plug-and-play, the cable industry approved the Five C technology as a protective digital output for new digital cable-ready products that will be hitting the marketplace within the next couple of months. It's being used in the DVD audio space for protecting high-resolution digital audio outputs. So, there's a number of areas. And even the satellite broadcasters now are incorporating Five C protective digital

outputs on their set-top box receivers. Echostar[16] has just introduced a device with Five C protected digital output. So, we're seeing marketplace adoption. Products have been in the marketplace for over three years now and their use is growing.

**MS. BILAL**: Now, I'm moving to claim two, your Honor, which is the circumvention of the Five C DTCP prior to Johnson's case—

**JUDGE LEW**: You're finished with the effectiveness issue?

**MS. BILAL**: With the first claim, yes.

**JUDGE LEW**: Can I ask you one question? With regard to where we are today, someone has cracked the Five C and used this on the Internet. Do you still continue to believe that the Five C code is effective?

**MR. HUNT**: Yes, I believe that the Five C technology is still an effective measure because the attack that has been mounted is a very sophisticated attack that has a centralized figure, Mr. Johnson, who has created a very sophisticated tool to be able to deploy this distributed computing attack by harnessing hundreds, tens of thousands, of computers. And it's very important to recognize that this is not a normal attack of the Five C system. It's a very sophisticated attack which requires a very sophisticated tool to be developed. So, it is not the ordinary type of attack that a content protection technology would defend against if it was being incorporated into a consumer product that has very high price sensitivity.

**JUDGE LEW**: How about the implication of Moore's law? Now that you have distributed computing, with Moore's law, you can see that during the duration of the copyright the technology may not hold up as well.

**MR. HUNT**: Right. I think there are a couple of points to be made here. One is that distributed computing is not a broad, widespread functionality that every Windows operating system is deployed with. In fact, the program that Johnson developed is a very specialized computing attack. One must understand that to basically exploit and orchestrate this sophisticated attack, where you're decrypting certain keys, not only does this centralized sophisticated program have to allocate which keys will be tried by computers attached to the distributed network, but you also have to provide in that software an ability to assess that the decryption of the test key actually creates video content, versus just another bunch of scrambled bits that are meaningless. And so, Mr. Johnson's program has been developed to actually try this key, decrypt it, look at the bits, and say, "Does this look like video or not?" That's a very specific attack that Mr.

16. Echostar can be found at http://www.echostar.com. Echostar offers digital video, data and audio channels of programming including local networks and HDTV.

Johnson has put together and that the defendants have facilitated on their site. That's why we don't believe that this is a typical type of attack and that Five C is still an effective technological protection measure.

**JUDGE LEW**: Okay. I can ask many more questions, but let me not take more of your time. Continue please.

**MS. BILAL**: Thank you, your Honor. A lot of what you just said is going to be re-mentioned in the following questions, but I will still ask. Claim two is the circumvention of the Five C Digital Transmission Content Protection technology. Prior to Johnson's case, prior to this case, has the Five C DTCP technology ever been successfully broken?

**MR. HUNT**: I'm not aware of it ever being broken.

**MS. BILAL**: But then how did Johnson manage to do this?

**MR. HUNT**: Well, as I just mentioned, it was a very sophisticated attack. Mr. Johnson developed, posted on his website, and harnessed the power of tens of thousands of computer users to use their spare computing time to basically process Mr. Johnson's circumvention tool.

**MS. BILAL**: So as you said, is it very necessary for a central party or entity to coordinate this brute force attack?

**MR. HUNT**: Absolutely. The central party needs to coordinate the assignment and the range of keys that will be tested by each computer that's attached to the distributed network. The program also has to give guidance on how it knows that it has the correct key. By scanning the content, these digital bits that are produced after decryption have to look like this, i.e., they have to look like video. So, Mr. Johnson, being a very smart individual, has put together a very powerful circumvention tool.

**MS. BILAL**: So, now coming to the details of the brute force attack, would a brute force attack like this, that only discovers one key at a time, damage the effectiveness claim of the Five C DTCP?

**MR. HUNT**: Well, the Five C technology developers understood the possibility of brute force attacks, about the possibility of eavesdropping and actually designed their system to change the content encryption key every two minutes to, again, defend against this type of attack.

**MS. BILAL**: Would the five companies, the Five C, have anticipated that this would be a normal attack to prevent?

**MR. HUNT**: The brute force attack?

**MS. BILAL**: Yes.

**MR. HUNT**: They would have seen this, but probably would not have designed an encryption or content protection system that would be incorporated in the consumer products to defend against this, because it would have increased the cost of the products.

**MS. BILAL**: So, you're saying that the Five C did not, when they did a cost-benefit analysis of this, it was not in favor of the (inaudible).

**MR. HUNT**: Yes. That's correct.

**JUDGE LEW**: My understanding is that a brute force attack is a system that has always been in place. It's just that it was not used with computers. It's an approach.

**MR. HUNT**: Yes. That's correct. It's always been available. But I think the distributed computing approach for the brute force is something new. It's something that we're aware of but again, to defend against it can be quite expensive.

**MS. BILAL**: So, considering that it has always been in existence, the brute force attack of 56-bit versus a 128-bit, you would still be able to ultimately crack the 128-bit.

**MR. HUNT**: That's correct.

**MS. BILAL**: Can one circumvent—I think this has been mentioned by Mr. Schoen, too, but I'd like you to reiterate—can one circumvent the Five C DTCP technology with an ordinary home computer?

**MR. HUNT**: No, you can not.

**MS. BILAL**: This moves me to my third and last claim, your Honor, which is the cost-benefit analysis of the Five C DTCP technology versus possible alternatives. In your opinion, is the Five C DTCP technology effective with the respect to its cost—here, I mean cost of manufacture, cost of implementation?

**MR. HUNT**: Yes, it is. And my rationale behind this is when the Five C companies met with content owners, they talked to them about the security requirements: What level of protection would make you comfortable with putting your content out? These companies were consumer electronic and computer companies, that had in mind interest in terms of controlling the cost of the technology because this had to be implemented in consumer products. And through the negotiation between content owners and their own interests in terms of building products that would incorporate it, they found the right balance in terms of the technology that has been implemented using a 56-bit cipher.

**MS. BILAL**: Given that this specialized distributed computer attack has occurred, and the defendant's claim that the Five C DTCP technology is no longer effective, are there any other steps that can be taken to address the issue? And if so, are they cost effective?

**MR. HUNT**: Well, there could be some possible steps that could be taken. One possibility that has been offered up by the defense is the idea of changing the length of the encryption keys. There are some problems

associated with that. First off, if Five C moved to a longer key length, it would require more processing power, so the implementation and consumer product's cost would be higher because you would need silicon chips with larger gate counts to be able to process in real time. This is an important aspect of Five C. The content comes in real time, encrypted. Therefore, the decryption has to occur in real time. So not only in hardware implementations do you have to have more gates—more processing power—so the silicon costs more to manufacture. However, the important aspect of choosing 56-bit encryption was to facilitate the creation of software applications that could then encrypt certified compliant software applications that could decrypt the Five C technology to be able to render and to play content on a personal computer. As the key length becomes larger, you need a more powerful computer, which would prevent some consumers from being able to play the content. They'd have to buy a new computer versus buying a new software package. The second problem with changing the bit length is interoperability problems. There are literally thousands of products, tens of thousands, maybe even hundreds of thousands of Five C equipped products now in consumers' hands. If Five C changed the encryption keys in new products, there would be potential compatibility problems where the devices could not communicate, could not authenticate and could not encrypt.

**MS. BILAL**: Is there any other step for the number of keys per session?

**MR. HUNT**: Well, another approach would be to change the frequency of the session key. It would require a greater brute force attack because now, instead of requiring, for example, sixty keys to encrypt a two-hour movie, you could increase it and now it would require 120 keys. But again, we get into the same problem of the processing required to now manage rapid key changes of the encryption. So again, there are costs associated with that.

**MS. BILAL**: With the current Five C DTPC technology, what is the time for a key? What's the session length for a key? How long is one key valid?

**MR. HUNT**: The informational spec that is available on a non-confidential basis states that the content encryption key can not be changed any more frequently than every thirty seconds, but it has to be changed at least every 120 seconds. That is the spec that is in the informational specification.

**MS. BILAL**: This leads to my last question, your Honor. Given that there are a lot of capable hackers in the world who, if given ample time and money, might be able to attack the latest technology using brute force, do

you think it is wise to solely rely on investing more money into complicating the existing technology, or do you think that we should rely on law enforcement as well?

**MR. HUNT**: Well, I think the marketplace negotiations between content owners who require a certain level of security and the consumer electronics and computer manufacturers who make products that would implement that technology have found the right balance between the costs of the technology associated with the Five C technology. They made that negotiation based on the idea that any technology can be broken, but what you're balancing is the cost of the technology versus the cost of enforcement. If we had no technology, enforcement costs would be very high because everybody would be copying. We could build Fort Knox security into it and have a low enforcement cost, but there would be a very high price to pay for these consumer products. I think in the marketplace negotiations between the technology developers, the Five C companies, and the content owners, they found the right balance. In fact, you need a balance between enforcement and the cost of technology to really get the right balance for a digital world to develop.

**MS. BILAL**: Thank you, your Honor. Thank you, Mr. Hunt. No further questions.

**JUDGE LEW**: Thank you very much. And for the cross-examination?

**MS. WADA**: Your Honor, my name is Emily Wada. I'm from Loyola Law School. May I proceed?

**JUDGE LEW**: You may proceed.

**MS. WADA**: Mr. Hunt, I understand that you are not here in your official capacity. But, is it true that you work for the Motion Picture Association of America?

**MR. HUNT**: I do.

**MS. WADA**: And isn't it true that the MPAA referred this case to the Department of Justice?

**MR. HUNT**: Yes, we did.

**MS. WADA**: Mr. Hunt, isn't it true that your bachelor's degree is in chemical engineering?

**MR. HUNT**: Yes, it is.

**MS. WADA**: And that you have a master's degree, but it's in business administration?

**MR. HUNT**: Yes.

**MS. WADA**: Sir, let's review the highlights of the qualifications that you placed on your resume. Over the past twenty-five years, you gained

experience and contacts in the motion picture and television industry worldwide. Is that correct?

**MR. HUNT**: Yes. That's correct.

**MS. WADA**: Sir, you didn't refer to your experience as a cryptographer or a mathematician, is that correct?

**MR. HUNT**: No, I'm not a cryptographer or a mathematician.

**MS. WADA**: And you referred to your skills in identifying and developing new high-technology business opportunities, is that correct?

**MR. HUNT**: Yes, I did.

**MS. WADA**: Not as to digital protection technologies, correct?

**MR. HUNT**: Correct.

**MS. WADA**: And you also referred to your experience in managing international partnerships and alliances with multinational corporations, is that correct?

**MR. HUNT**: Correct.

**MS. WADA**: Sir, doesn't that suggest to the Court that you're more of a businessman rather than a cryptologist or a mathematician?

**MR. HUNT**: Well, I have a unique background, in that I have both a business and a technical background, as well as combined with my hobby interest in computers, home video and home audio products.

**MS. WADA**: So, do you know what the Data Encryption Standard ["DES"] is?

**MR. HUNT**: Yes, I do.

**MS. WADA**: Are you aware that DES was a standard adopted by the federal government in 1977?

**MR. HUNT**: Yes, I did.

**MS. WADA**: And isn't it true that DES uses 56-bit encryption?

**MR. HUNT**: Yes, it does.

**MS. WADA**: And isn't it true that the DTCP encryption in this instance also has 56-bits?

**MR. HUNT**: That's correct.

**MS. WADA**: And isn't it true that the federal government has now adopted a new standard?

**MR. HUNT**: Yes, they have.

**MS. WADA**: Sir, isn't it true that participating in a distributed computing project is easy, as simple as clicking on a link for the ordinary user?

**MR. HUNT**: It's easy for the ordinary user to join a distributed computing project.

**MS. WADA**: Are you aware that such projects are well-known and widely publicized today?

**MR. HUNT**: Yes.

**MS. WADA**: Are you aware that in your sworn declaration you speak of effectiveness in terms of the ordinary user, rather than in terms of the technology?

**MR. HUNT**: Yes.

**MS. WADA**: But isn't it true that the DMCA defines effectiveness in terms of the technology and not the ordinary user?

**MR. HUNT**: Well, I'm not a lawyer, so I can't tell you exactly what the DMCA says.

**MS. WADA**: Let me inform you. The DMCA, § 1201(a)(3)(B), sets forth "a technological measure 'effectively controls access to a work' if [the 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."[17] That refers to the technology and not the user, correct?

**MR. HUNT**: Yes.

**MS. WADA**: And sir, isn't it true that in the modern computer landscape, distributed computing and brute force attacks are to be expected in the ordinary course of an encryption operation?

**MR. HUNT**: Well, when we talk about an encryption operation, it really depends on whether we're talking about military secrets, multi-million dollar banking transactions, or whether we're talking about protecting movies.

**MS. WADA**: But, you are aware that distributed computing projects and brute force attacks are widely used and publicized today, correct?

**MR. HUNT**: I'm not sure I would use the term "widely." Distributed computing is not a prevalent activity that most users get involved with. If you look at the software that's provided for computers, I don't think I've ever seen software that's been sold that allows for distributed computing projects and activity. So I wouldn't call it widespread. And brute force attacks are a very unique field of cryptography research that has been orchestrated by companies like RSA in special contests. But I would not use the term "widely."

**MS. WADA**: But, you do recognize that they have been in the news, and that they have been publicized and that, I think several minutes ago, I asked you whether or not you were aware that they were widely publicized

17. Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(3)(B) (2000).

for over a decade now?

**MR. HUNT**: There has been some publicity for distributed computing and brute force attacks, yes.

**MS. WADA**: And they are not uncommon, is that correct?

**MR. HUNT**: I don't think they're common.

**MS. WADA**: Sir, in your sworn statement to this Court, you also spoke of your cost-benefit analysis at paragraphs fourteen and fifteen of your declaration. Isn't it true that you put forward a cost-benefit analysis that it is unfair to put the burden of the cost on the industry and the users?

**MR. HUNT**: Well, I think the idea is that the industry must find the right balance between the technology and the cost of enforcement, so there's a marketplace balancing that occurs.

**MS. WADA**: So, isn't it true, then, that the industry's choice to rely on 56-bit encryption relies on non-security reasons?

**MR. HUNT**: No, I think the idea of where the use of 56-bit encryption comes out is from the marketplace negotiations between digital content protection, technology developers and content owners, to find the right match between the level of security that content owners are comfortable with and the costs providing that level of security, and then finding the cryptographic tools that would balance all of those.

**MS. WADA**: So, would it be correct to say, then, that copyright owners were comfortable using an encryption scheme that has been abandoned by the federal government over five years ago, and has publicized attacks?

**MR. HUNT**: Well, I think it's important to understand that there's a difference between how the government might use an encryption technology and what they might endorse as a new, improved, advanced technology. Also recognize that, again, the design of a consumer content protection system is quite different than the design of a content protection or a message encryption system that protects military secrets or multi-billion dollar financial transactions.

**MS. WADA**: But in this instance, with distributed computing projects, ordinary users are able to overcome 56-bit encryption successfully. Is that correct?

**MR. HUNT**: Well, the only way a distributed computing attack can work is when there is a centralized figure using sophisticated tools and facilitating the deployment of those tools with tens of thousands of computers. And so, there is a point in time where a balancing must occur between what technology you would use to defend against, for example, a very sophisticated distributed computing brute force attack, and when you

would use enforcement to basically defend against that.

**MS. WADA**: So, in your opinion, Mr. Hunt, how long would it take, given Mr. Johnson's set-up, to overcome, with brute force, 128-bit encryption?

**MR. HUNT**: I don't think I've done the calculations, so I can't really give you an answer on that.

**MS. WADA**: Could you give the Court an estimate? An educated guess?

**MR. HUNT**: I would say it would take a lot longer than using a 56-bit key, but I have not done the calculations.

**MS. WADA**: Let's turn back to your cost-benefit analysis. So in paragraphs fourteen and fifteen of your declaration, you set forth your cost-benefit analysis. Is that correct?

**MR. HUNT**: Yes, I think so.

**MS. WADA**: However, you suggest that the cost would be passed to the end user if the industry were to increase the relative security of the encryption being used, is that correct?

**MR. HUNT**: The consumer products that would implement a higher level of security, the costs would be transferred in the price of those consumer products.

**MS. WADA**: However, you don't set forth any estimates, any numbers, or any evidence of that, is that correct?

**MR. HUNT**: I'm not in the business of manufacturing consumer products, so I can't give you an answer on that.

**MS. WADA**: But you are a businessman, is that correct?

**MR. HUNT**: I have an MBA and I'm dangerous.

(LAUGHTER)

**MS. WADA**: And isn't it true that rather than increase the cost to the end user, maybe your employers at the MPAA could make a little less money and put out a product with more protection?

**MR. HUNT**: I'm not sure I understand the question.

**MS. WADA**: No further questions, your Honor.

**JUDGE LEW**: Alright. Again, I would have a lot of questions to ask; however, you've completed your examination and I want to keep on schedule. Why don't you step down then, and we'll go into the closing arguments, first beginning with the movant.

**MR. SHAPIRO**: May it please the Court, Benjamin Shapiro for the defendants. The second of our motions today is to have all charges against defendants Law, Baltimore, and Caltech dismissed. First of all, for Caltech, § 1204(b) of the DMCA specifically exempts educational

institutions, such as Caltech, from any criminal liability.[18] Therefore, all charges against Caltech should be dropped. Secondly, under any theory of liability, charges against Professor Law and President Baltimore also must be dismissed. Neither is directly liable. Under § 1204(a), criminal liability requires that the defendants act "willfully and for the purposes of commercial advantage or private financial gain."[19] Nothing the government has presented to this point proves that either of these acts has taken place. There is no evidence to suggest that, either. These defendants have not aided and abetted anyone else in the commission of a crime. According to the Ninth Circuit jury instructions for aiding and abetting, the government must prove, first, that the crime was even committed. It hasn't been committed. They haven't proven that yet. Second, they have to prove that these two defendants knowingly and intentionally aided or counseled or commanded the defendant, presumably John Johnson in this situation, to commit the crime. Third, they have to prove that the defendants, Law and Baltimore, acted in their capacity before the crime was committed. Fourth, it's not enough that they were merely associated with the defendant or that they were notified about the possibility that there might have been a crime at some point and afterwards.

**JUDGE LEW**: Does it have to be before the crime was committed?

**MR. SHAPIRO**: According to the Ninth Circuit jury instructions under the *United States v. Avila-Macias*,[20] defendants had to contribute some action before the crime was committed.

**JUDGE LEW**: And if we continued to advise and pursue him to leave the code on the Internet?

**MR. SHAPIRO**: Are you referring to the Department of Justice request that they take down the website?

**JUDGE LEW**: Yes, that's where it would apply.

**MR. SHAPIRO**: Any attempt to construe that as giving them criminal liability would be a violation of their First Amendment rights. The First Amendment free speech provision has been—

**JUDGE LEW**: No, just speaking on the issue of aiding and abetting. You can argue First Amendment later.

**MR. SHAPIRO**: Under any theory of liability, a president of a university or a professor at a university liable for not changing the curriculum of the course as the government requested—

**JUDGE LEW**: Not the curriculum, allowing it to be on the Internet.

---

18. Digital Millennium Copyright Act, 17 U.S.C. 1204(b) (2000).

19. *Id.* § 1204(a).

20. United States v. Avila-Macias, 577 F.2d 1384, 1390 n.4 (9th Cir. 1978).

**MR. SHAPIRO**: The website, which is the class website, where a student posted the answer to a homework question on the class website, is part of the curriculum. Any attempt by the government to compel the professor or the president to remove or change those materials would be a prior restraint. Second of all, it would impermissibly affect their First Amendment rights. The Supreme Court has said that the First Amendment protects an educator's right, the freedom of education. That right can not be touched by the government. They cannot compel them to change the curriculum. Now, in our brief, we address what are traditionally civil theories of liability: vicarious liability and contributory liability. We're not arguing here that they apply. In the event that the Court would like to hear whether they would mean anything here, these defendants are not liable under those theories, even if they were to apply in a criminal context. Vicarious liability requires the right and ability to control. Again, they may have technically the right and ability to control the website and the curriculum, but any attempt by the government to compel, would again, burden their First Amendment rights. Secondly, they have to derive some direct financial benefit from the individual acts. There has been no evidence presented to this point by the government that Professor Law or President Baltimore derived any direct financial benefit from any of the actions alleged.

**JUDGE LEW**: Doesn't *Napster*[21] make a statement as to what is to be financially derived and what would satisfy that requirement?

**MR. SHAPIRO**: In the *Napster* case, I believe the court held that the growth of the attractiveness of the venue, the idea that they would bring more users to *Napster* and maybe eventually charge them in the future, was a financial benefit. There has been no evidence presented here that this is attracting more students to Caltech, or that this is providing any financial benefit either now or down the road. Again, *Napster* was a civil case against a corporation. It wasn't against the employees of that corporation, as Professor Law and President Baltimore are here.

**JUDGE LEW**: I'm only bringing it up for the definition of the term. But anyway, continue.

**MR. SHAPIRO**: Also, under the theory of contributory liability, which requires specific knowledge of the defendant's actions as they were happening—the standard that was applied in the civil context in *Napster*—there's no evidence presented by the government here that these two defendants had any specific knowledge of the actions of Mr. Johnson until after the alleged acts took place. Secondly, it requires a material

21. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

contribution by these two defendants to the act. There's no evidence that these two materially contributed to anything. Under all these theories, under any of these theories, charges against these two defendants must be dismissed. In the absence of any further questions from the Court, do you have any further—?

**JUDGE LEW**: On this issue?

**MR. SHAPIRO**: Yes.

**JUDGE LEW**: You have other arguments, don't you?

**MR. SHAPIRO**: I just have this and the First Amendment.

**JUDGE LEW**: Why did I give you twenty minutes?

**MR. SHAPIRO**: Maybe the government needs more time to rebut this.

(LAUGHTER)

**JUDGE LEW**: Counsel, the burden is on you. You're the movant. If you're satisfied—

**MR. SHAPIRO**: I believe I've laid out the elements. In the absence of any further questions, I rest.

**JUDGE LEW**: First of all, with regard to Johnson, the motion is not made with regard to Johnson at all.

**MR. SHAPIRO**: No, it is not.

**JUDGE LEW**: With regard to Caltech, what explicitly is the stated ground for the exemption argument?

**MR. SHAPIRO**: Section 1204(a) of the DMCA is the portion that criminalizes activity under § 1201.[22] Section 1204(b) says that § 1204(a) does not apply to an educational institution.[23] Therefore, Caltech should be exempt.

**JUDGE LEW**: Are you arguing that that argument might extend to Law and Baltimore as well?

**MR. SHAPIRO**: I'd be happy to accept that argument.

**JUDGE LEW**: No, I know that you would. But you never made it.

**MR. SHAPIRO**: I'm not arguing that. I'm arguing that they are themselves outside of liability under the statute for different reasons.

**JUDGE LEW**: Alright. Your argument is based upon the arguments stated. With regard to aiding and abetting again, I think you've stated enough in that regard. But how about your First Amendment argument?

**MR. SHAPIRO**: Yes.

**JUDGE LEW**: What is the basis for the First Amendment

22. Digital Millennium Copyright Act, 17 U.S.C. § 1204(a) (2000).

23. *Id.* § 1204(b).

argument?

**MR. SHAPIRO**: Well, in *Keyishian v. Board of Regents of New York*[24] in 1967, Justice Brennan wrote that academic freedom, the freedom of the teachers to decide what's in their curriculum, to decide what they teach their students—

**JUDGE LEW**: What is the speech here? The code?

**MR. SHAPIRO**: No, the speech is their teaching of the course. The government requested not only that they take down the website, which was part of the class, but to stop teaching this type of decryption and encryption in the future.

**JUDGE LEW**: Okay. I'll accept your teaching for the moment. How about taking down the code off the website?

**MR. SHAPIRO**: I believe that in this day and age, and especially at a university such as Caltech, the class website is integral to the teaching, the same as a textbook was fifty years ago. It is just as integral to the teaching of a class now. And to have them required to take a class website down is a prior restraint.

**JUDGE LEW**: You have authority for that?

**MR. SHAPIRO**: I just have the cases from the Supreme Court saying that academic freedom is of transcendent value, not only to the teachers and the students involved, but to all society.

**JUDGE LEW**: I don't think they have envisioned that argument to be made by the government with the application of the statute here, the criminal statute.

**MR. SHAPIRO**: They may not have. Cases regarding academic freedom have not found their way to the Supreme Court in more than three decades.

**JUDGE LEW**: Don't you think there should be some balance?

**MR. SHAPIRO**: Balance between what, your Honor?

**JUDGE LEW**: Between the criminal statute and the First Amendment right to free speech?

**MR. SHAPIRO**: Actually, yes, I do. I believe that teachers should be able to teach technology without interference from the government. I believe it was unfair for the government to request that the teacher and the president change the curriculum of one of their courses at the university, or else face criminal charges. I believe that's where the imbalance is: to assign criminal liability for failing or refusing to change the curriculum at a university.

24. Keyishian v. Bd. of Regents of the Univ. of the State of N.Y., 385 U.S. 589, 603 (1967).

**JUDGE LEW**: You're not going to sever the factual argument for each Law and Baltimore, are you? Are you going to leave them lumped together?

**MR. SHAPIRO**: I believe in respect to the academic freedom and First Amendment, I believe they share the same rights. However, there may be a slight factual difference between their various involvements in this situation.

**JUDGE LEW**: And you don't care to argue any of that?

**MR. SHAPIRO**: I believe it does not apply to the First Amendment rights.

**JUDGE LEW**: Alright. I'll leave it at that. Thank you very much. And for the closing argument for the opponent?

**MR. EGLEY**: Thank you, your Honor. John Egley from Loyola Law School on behalf of the United States of America.

**JUDGE LEW**: Joe or John?

**MR. EGLEY**: John Egley.

**JUDGE LEW**: Thank you.

**MR. EGLEY**: I will address the First Amendment issues and then deal with the effectiveness of the technology under the DMCA and then I will yield to my colleague, Michael Matoba, to address the criminal liability issues and go one by one through each defendant, which theory applies to the particular defendant in that case.

In its opening statement, the defense began by stating that the companies of the recording industry were hiding behind the law. Yet in its closing statement, the defense revealed who was truly hiding behind the law. Namely, that they are hiding behind this umbrella of academic freedom to cloak criminal actions. This Court cannot tolerate it, and it is not able to do so under the First Amendment. First, the code at issue in this case, your Honor, is not speech. As such, it can not be regulated under the First Amendment. In particular, there is no expressive purpose served by the code in this case. In past cases, where the courts have held that code can be expression, it was when programmers were looking at the code and communicating with each other and serving that kind of communicative purpose. Here, the code serves no such communicative purpose. It's posted on a website, people click on the code, which allows them to engage in a distributive computing force attack, and therefore the computers are communicating, but it is not communication between people. Furthermore, there is no communication going on in the classroom. Initially, the code might be speech, within the protections of the First Amendment, during the initial class discussion. That probably is speech. However, when they

went beyond that classroom discussion, when they went beyond the teaching function at the university and posted it on a website for use by everyone, it lost that speech purpose and became non-speech. As such, the First Amendment should not apply.

However, even if the Court determines that it is speech, although there are cases which hold that computer code is not speech, the government still believes that the First Amendment is not an obstacle to prosecution under the DMCA because we can survive the scrutiny that this Court can apply to it. First, the government contends that intermediate scrutiny is the proper level of review to apply to this regulation because the target here is content neutral. The DMCA does not target the way computer programmers—computer hackers, be it as they may—choose to communicate. Rather, it is serving a content-neutral purpose of preventing criminal acts, preventing the circumvention of technological protection measures. Therefore, all that is needed is an important governmental interest and some connection between the serving of that interest and the regulation at issue. Here, intermediate scrutiny is clearly met. There is an important governmental interest. There is a key governmental interest in preventing the circumvention of technological measures. Without it, there is no point to protecting and being able to distribute digital content and copyrighted works. Furthermore, there is the connection between the regulation and the ability of the DMCA here, because it just targets those people that try to enable others to circumvent technological protection measures, as well as it prevents those who are hacking it themselves from doing so. That is a nice nexus between the regulation of the DMCA and the conduct that it seeks to regulate.

But even if this Court decides to apply the heightened level of strict scrutiny, the government still prevails, and the defendants are guilty. Here, there is a compelling government interest. As I've already mentioned, there is a multi-billion dollar industry at stake. There is intellectual property at stake. There is the ability of companies and individuals to protect their copyrighted material and their protected material at stake. That certainly qualifies as a compelling governmental interest. Furthermore, it is narrowly tailored because it specifically attacks only those individuals that violate it. As such, it is narrowly tailored and can survive any type of First Amendment analysis. But first, before we get to that, it will be important to define the terms used in the DMCA, which has been lacking thus far. In particular, as your Honor mentioned, there is no precise definition for the word "effectiveness." Now, unfortunately, words have no precise and exact meaning, otherwise lawyers would largely be out of business. You know, like if I mention "Jack," I could be referring to my

father-in-law, whose name is Jack. I could be referring to a jack that lifts my car so I can change the tire. But if I told you that "Jack" meant something else, like jump or run, I would be wrong. Here, "effectiveness" means exactly that: effectiveness. We can use that as a jury determination to see whether or not the technological measure is effective within the meaning of the DMCA.

**JUDGE LEW**: It has never been argued by them, but this is a criminal statute. Statutes charging crimes should be clear so that defendants would know what they're charged with. If you put vague terms in a criminal charge in a statute here, it may very well be defective as being too vague. But to the extent the other side is only arguing that it's to be narrowly construed, or to be narrowly viewed in this application, even then, there still is an issue. But it's so vague, even within this narrow sphere. How do you get around that?

**MR. EGLEY**: Unfortunately, it's not, your Honor. In fact, there is a definition provided for the term in the statute itself. Specifically, it is § 1201(a)(3)(B), which states that "a technological measure 'effectively controls access to a work' if the 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, [in order] to gain access to the work."[25] In short, whether or not it keeps ordinary users from accessing protected work, that is the definition.

**JUDGE LEW**: You think that's a clear definition?

**MR. EGLEY**: I do, your Honor. The definition is provided for in the statute. Now, although it's not the height of clarity, it is certainly clear enough to be able to determine whether or not something is effectively controlled or something is not effectively controlled. It provides some standard, and I think a reasonable standard, to assess whether or not something is in violation of the DMCA or not. For instance, there was a case where a technological protection measure could be circumvented by just drawing with a Magic Marker around the edges of the CD.[26] Now, clearly, within this definition that's offered by statute, that doesn't effectively control anything. A little three-year-old could take a little Magic Marker, draw around the edges of a CD and *voila*, they've violated the DMCA. Well, clearly, that's not the case. Furthermore, the defense has argued that there is somehow a basic flaw in the 56-bit technology

25. 17 U.S.C. § 1201(a)(3)(B) (2000).

26. Todd R. Weiss, *Felt-tipped Markers May Threaten CD Copy Protections*, COMPUTER WORLD (May 21, 2002), *at* http://www.computerworld.com/printthis/2002/0,4814,71354,00.html.

because it has always been susceptible to a brute force attack. Unfortunately, the statute here is not overbroad or outrageous as the defense would argue by citing *Church of the Holy Trinity*, because here the standard of proof to be applied is discernible.[27] It does not yield outrageous results. Those who violate the DMCA will be convicted, and the standard set forth for the conviction is those who effectively circumvent a technological measure that's deemed to be effective within the meaning of the DMCA. Here, that standard has been broken by the defendants. In particular, it prevents an ordinary user from gaining access to the protected work. As our expert testified, the ordinary person with an ordinary computer, even Seth Schoen, the defense expert, confessed that even himself as an individual, would not be able to process or have the computing power available to brute force attack a 56-bit device. The only way he would approach that type of attack is when you have tens of thousands of users combined to mount that assault. And to do that type of assault requires one individual who is overseeing and operating all aspects of which computer is going to break which cipher and then move on. And then, even when you only successfully violate that one crypt key, you gain access to two minutes of video content. So you would have to repeat the process all over again. For example, a typical two-hour movie requires the process to be repeated sixty times, again and again and again.

**JUDGE LEW**: By the movie industry standard, 120 seconds for change on the encryption is the outside limit. Why should they use the shorter range? I think it was fifteen seconds or maybe even sixty seconds. Wouldn't that be even more effective?

**MR. EGLEY**: Possibly, your Honor. However, using that type of reduction in the time frame would require additional sophistication on the consumer devices.

**JUDGE LEW**: That would make it more effective. On a consumer device?

**MR. EGLEY**: Well, on the consumer device that has to communicate the encryption code to the authenticating device, they would need to operate at a quick speed because every thirty seconds it would be requesting a new—

**JUDGE LEW**: Are you arguing that it is a known fact to you? Because if it is within the standard, it certainly should be. It wouldn't affect the consumer unit costs.

**MR. EGLEY**: Not the consumer viewing costs, your Honor. It would impact the hardware costs.

---

27. Holy Trinity Church v. United States, 143 U.S. at 457.

**JUDGE LEW**: I'm talking about the hardware.

**MR. EGLEY**: The hardware costs, it would impact, your Honor.

**JUDGE LEW**: It should be the same because it's within the standards. I think you're wrong there, unless you know something I don't know.

**MR. EGLEY**: Well, your Honor, our expert testified to the fact that even though there is a range within which the cipher code would need to be repeated, the result of that changing cipher code could require more computing power on the part of the consumer device. So if the device that's receiving the cipher only has to verify the data every 120 seconds, that's a lot of computing power required. However, if you ratchet that up to every thirty seconds it has to make this calculation. Again, it would require more on the part of a consumer device. But all this is really beside the point, your Honor, because even though it is set at 120 seconds, it is still effective within the meaning of the DMCA because it prevents ordinary users in the ordinary course of business from accessing protected work.

**JUDGE LEW**: Where in the statutes or code does it say "ordinary"?

**MR. EGLEY**: In the definition of whether or not a technological measure effectively controls access, or more specifically 17 U.S.C. § 1201(a)(3)(B) which provides that definition, where something is effective if it keeps people, "ordinary" people, from accessing protective work.[28] And as such, even the 120-second cipher would be effective under that definition.

**JUDGE LEW**: Well, what bothers me in this whole technological area is not the person so much as the hardware technology. The ordinary person can push the button on the computer and say, "Start decrypting." It's not the person so much as the software and the hardware that's available on the market, readily able to be purchased by ordinary people.

**MR. EGLEY**: Well, your Honor, that's why I submit that we are not pursuing the tens of thousands, perhaps hundreds of thousands of individuals who click that button. We're pursuing the person who wrote the program and acted as the hub of this brute force activity. As such, that individual falls within the reach of the DMCA. Not everyone else. If I may use a brief analogy, this is a lot like when you lock your keys in your car. Now I don't expect your Honor to confess to this, but I will be brave enough to confess to such a tragedy. Now, when I locked my keys in my car, I of course felt very embarrassed, and even more embarrassed when the AAA guys showed up. And within twenty seconds, he used that little

28. 17 U.S.C. § 1201(a)(3)(B) (2000).

tool, popped open the car, and I could get in. Well, this analogy has its limits, but it's applicable here because just like the AAA person had his tool, this person had his tool. He had the computer code, which requires a high degree of skill. And speaking of skill, much like the AAA guy who has that special skill of knowing where to put the little device onto the side of your car in order to make the lock work, this person had a special skill that a vast majority of people do not have. It requires a highly sophisticated knowledge of computer programming. And only with that type of sophistication is the person able to circumvent 56-bit encryption. Now just like a car lock, even though it can be jimmied or it can be forced open in a matter of seconds by experienced personnel, it's still effective at preventing a lot of car thefts. If it wasn't effective, we'd have a lot more car thefts in this country than we already do.

**JUDGE LEW**: Sometimes I have a problem in this general area where I have to look at the entire industry as a whole with the technology that you have. If you have something played and you can make an analog copy, that's not illegal. With an analog copy, you can make a digital copy and you can mark it without the code. If that's available already in the industry, why should I give such tremendous weight to this one statute?

**MR. EGLEY**: Unfortunately, your Honor, there are, indeed, a number of gaps within the DMCA which, to me, suggest to Congress that they need to amend the statute and plug those holes. But when someone falls within the confines of the statute as it is written and not within those gaps, I would suggest to your Honor that this Court ought to follow the statute, if it doesn't suffer from any constitutional problems, which it does not here. There are gaps within the statute that suggest amending of the statute, rather than voiding the whole statute or not enforcing the statute as it stands.

Now, moving on to the defense expert witness. We all saw him do a lot of dancing. He's very good at dancing. It's nice to have an expert witness who has an opinion. But no amount of dancing by that witness is going to avoid some key concessions that he made. Number one, he said that a $200,000 computer was required in order to brute force hack a 56-bit encryption. He admitted that cost is prohibitive, and I quote: "It is cost prohibitive for the ordinary person." Since it is prohibitive for the ordinary person within the meaning of the DMCA, specifically whether something is effectively controlled or not by the ordinary person, that is a fatal concession by the defense. Furthermore, Mr. Schoen suggested that we should anticipate future technological advances, and, thus, the DMCA is defective for that reason. Unfortunately for the defense, that's not the language in the DMCA. The language is not that the prosecution or the

technologically effective measure has to anticipate advances in technology, it just has to effectively control access. The defense can't bait and switch and state that the standard is anticipatory, rather than prevent ordinary access. This presents the problem of the 56-bit encryption versus the 128-bit encryption. And that seems to be a common sense approach. You do not need to be a mathematician or an expert in mathematics to understand that using a 56-bit encryption when there's a 128-bit encryption available is not practical. However, there are a number of key considerations that prevent the adoption of such a device. First, a 128-bit encryption would impose a tremendous burden on consumers, the industry and technology as a whole. By adopting the new standard, you would essentially make all existing consumer devices obsolete because the 56-bit encryption would be unable to decrypt the 128-bit encryption. Therefore, everyone that just went out and bought a DVD or a digital TV or what have you, would need to go out and buy another one. That's a tremendous burden. Furthermore, this statute, which focused only on the 56-bit type of encryption, was only able to be brute force attacked by a massive conglomeration of computing power. It took tens of thousands of users to glob together and use their dormant computing capacity in order to brute force attack the system. And the expert conceded that even if 128-bit encryption would be able to be brute force attacked, it might take a little bit longer. Unfortunately, the experts do not say how long, but that's beside the point. Because even though the 128-bit encryption exists and would pose additional costs, the 56-bit itself is still effective. Would the 128-bit be more effective? Arguably so. It's a better encryption device. But that's not required under the DMCA. Again, the defense is seeking to bootstrap the standard of proof. The standard here is not whether or not the technological protection measure is error-proof or is the best available. No, the standard is whether or not it effectively controls access to the ordinary person and prevents them from doing what the defendant did here. Here, the defendant violated that clear statute and he has the special skills to make that available. Finally, your Honor, it is conceded by the defense that one computer, which the ordinary consumer would have access to, would take decades to complete the decryption. The expert even conceded it could take possibly more than decades in order to brute force attack a 56-bit or a 128-bit encryption system. As such, since the ordinary consumer with the ordinary computing power cannot possibly hack a 56-bit encryption within their lifetime, it is effective within the meaning of the DMCA. Now, I would like to yield briefly to my colleague to discuss the vicarious liability issues defendant by defendant.

**JUDGE LEW**: I didn't know it was bifurcated. But that's no

problem. Proceed.

**MR. MATOBA**: May it please the Court, Michael Matoba for the United States of America, a Loyola Law student. The question I'm addressing here is about actual liability. Direct infringement. The question is not whether there is vicarious liability, but whether Dr. Baltimore and the other defendants acted directly in violation of the DMCA. *Napster* brings an interesting point.[29] The defense alluded to *Napster* in the civil context. But what *Napster* also says is that "if a computer system operator learns of a specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."[30] What we're submitting to the Court is that when the government asked Dr. Baltimore and the other defendants to remove this material from their website, their refusal to do so constituted a direct infringement. Subsequently, they should be held accountable for their criminal conduct. Now, the question is, was their conduct willful? And, was there commercial advantage or financial gain? Willful conduct. The government asked them specifically to remove this material and they refused. That conduct is sufficient to meet the willful conduct standard. Commercial advantage. Caltech, being the first university to crack Five C technology, gains a huge amount of prestige as a university. They can draw all sorts of students from across the world because they, specifically, were the first to break Five C technology. It had never been done before this point. And because of this prestige, they gain financial benefits. They gain a huge commercial advantage as an educational institution. They're able to draw in the top students. They're able to draw in research grants from the government and other private entities. And this is a huge advantage for them. And under willful conduct and a commercial advantage, that's sufficient to meet the standard of the DMCA. Furthermore, they trafficked in circumvention technology. They knew the material was on the website, they refused to remove it and they facilitated access to such information. So in a vicarious liability sense, without their participation in this endeavor, it never would have happened. They did not have the capability to use the university website for this purpose. This classroom environment crossed the line. Education is important and the government conceded that education and research are vitally important to our society. But the distinction to be drawn here is the first time that Dr. Law looked and applied it to Five C technology to see if it was appropriate or if the program worked on Five C technology, that was testing out the

29. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

30. *Id.* at 1021.

technology for educational and research purposes. Once he continued to allow that material to be on the Internet and to allow it to be used by anyone in the entire world, that constituted a shift in intent. He's no longer under educational protection, but in fact, he's violated the DMCA. It falls directly under what the DMCA is trying to address and trying to stop. To sum things up, your Honor, the issue here is whether we allow the defendants to circumvent and traffic in digital rights technology. The U.S. government understands the need for education and Congress has specifically provided these exceptions in the statute. Here, the defendants crossed the line. They crossed the line into piracy and continued to allow them to benefit from this method and this action is reprehensible. The defendants can't claim ignorance because they defied a government request to remove the infringing material. Piracy in this form needs to be punished, it needs to be stopped. Otherwise, copyrighted material may never be protected again. Thank you, your Honor.

**JUDGE LEW**: With your argument, I conclude that you concede that Caltech falls under the exception of the statute?

**MR. MATOBA**: No, your Honor.

**JUDGE LEW**: You just argued it.

**MR. MATOBA**: What I argued was that the first time that they used the material, we concede that it was for educational and research purposes. But what happened is it was transferred. It transformed.

**JUDGE LEW**: So your argument is to all defendants.

**MR. MATOBA**: Yes, your Honor.

**JUDGE LEW**: I understand that. Alright. We're right on schedule. We will take a recess now until 5:45, at which time I will return with a verdict.

**BAILIFF**: Please rise.

**MR. MCCAFFERY**: This concludes the session of the United States District Court for the Western District of California.

**MR. MANHEIM**: Thank you Judge Lew. As Judge Lew well knows, there is traditionally an appeal from the trial at the Crossroads Conference, so we hope to see you all back here next year. Again, I want to thank Judge Lew and certainly our prosecution and defense teams for a fabulous job well done. Thank you very much. Please stay tuned on our website, http://www.techlaw.lls.edu, where we will post all the pleadings, the movie, and some excerpts from the video and certainly Judge Lew's ruling when it is issued in a couple of months. Thanks very much for attending.