EDITED & EXCERPTED TRANSCRIPT OF THE SYMPOSIUM ON THE LAW & TECHNOLOGY OF DIGITAL RIGHTS MANAGEMENT

TABLE OF CONTENTS

I. INTRODUCTION 697
II. IMPACTS OF DRM ON INNOVATION, COMPETITION AND SECURITY 697
III. IMPACTS OF DRMS ON FLOWS OF INFORMATION 715
IV. DRM-RELATED LEGAL AND POLICY INITIATIVES IN THE UNITED STATES 735
V. ANTICIRCUMVENTION REGULATIONS IN THE UNITED STATES AND ELSEWHERE 760

I. INTRODUCTION

On February 28 and March 1, 2003, the Berkeley Center for Law and Technology and the *Berkeley Technology Law Journal* presented a symposium on Digital Rights Management. The following are edited versions of the transcripts from several of the conference panel discussions. Full transcripts are available at http://www.law.berkeley.edu/institutes/bclt/drm/transcriptions.html (last visited Apr. 24, 2003).

II. IMPACTS OF DRM ON INNOVATION, COMPETITION AND SECURITY

Panel:

Hal Varian, School of Information Management and Systems, University of California, Berkeley (moderator)

David Farber, Computer Science, University of Pennsylvania

John Manferdelli, Microsoft Corp.

Lucky Green, cypherpunks.to

Alex Alben, RealNetworks, Inc.

VARIAN: John Manferdelli will speak on principles guiding trustworthy computing, kind of lay out some of the technology and some of the principles that should apply. Lucky Green will talk about who the computer should trust. And Dave Farber will talk about some of the privacy and security of the digital rights management issues that arise in the technology. Then I'll chime in and say a few words about some of the economic and business issues, and then [Alex Alben] will wrap up with some discussion of government policies towards DRM.

MANFERDELLI: I'm going to talk about the principles of digital rights management, and I'm actually going to follow up on a theme that Allan [Adler] mentioned, that it's not exactly one size fits all.

We think of rights management as a way to have rights persist with the thing they're trying to protect. That's lots of stuff. It's to protect and to share assets both with customers, vendors, and other employees. It's also to protect personal information, personal photos. So there's a wide range of things not only in the pure commercial space, which I think most of the discussion has focused on today, but in other spaces. And all the attack models you have to think about it in each of the domains carefully that what you are trying to do is very different in all of those domains.

So, one of the areas which most people spend all their time doing, which I think of as classic DRM, is audio-video protection. And that's basically people thinking: "We're going to sell audio files and video files to people over the Internet."

So it is not the purpose of a DRM system to have provided a perfect protection mechanism. In fact, it cannot ever possibly do that. I guess there's some question as to whether any system could possibly do that. But let's look at a very different application. I think last week we announced something we call "enterprise rights management," and that's to protect documents for a corporation. And there, the issues are completely different. Privacy issues are much reduced and what you think of as "fair rights" doesn't come into it. It's roughly the same technology. It's basically a way to authenticate the thing you're granting rights to and authorize it, but it's a very different application domain.

Personal rights management can be two fold. And then finally, privacy rights management, from trying to protect my e-mail or documents to having a conversation with my lawyer or my doctor that's a very different kind of protection that has a very different attack model, and what you're trying to prevent is actually quite a bit different.

People who were clearest about what they wanted and wanted it right now were in the enterprise. So we have done audio-visual video protection systems. Intel has a very clear focus, and the focus is not to restrict what people can use their computers for. We don't want to restrict it in any way. What we want to do is enable new stuff. And we want to enable them to get things on their computer that people would be unwilling to let them have now, or would not risk, in the situation PCs are used in right now.

So I think one sort of key aspect, and I think something nobody is sort of focused on in a very clear way, is whatever the mechanism you use, it cannot impose policy. It's very difficult to anticipate the policy needs of a

DRM system. They change all the time, and they change with application, so whatever the system is, it has to have this sort of 360 degrees of policy. It has to be an "opt in" model. One of the issues with mandated DRM is users don't have the option to decide whether they want it or not. And one of the firm principles is it really ought to be in user control. That is, the user ought to decide whether he is willing to go along with this.

It really ought to benefit both the corporation and the user. I expect it to evolve over time, and I expect that will be a matter of negotiated equilibrium. As a technology provider, I can't be in the middle of that. It just won't work for two reasons: One is it'll take me six months, a year, to get out the next release that does the next thing you want in policy management; and the other reason is that you won't trust me to do it. You have to be able to specify what you want and get that to happen. So, I do think much of what we talk about, as it settles down, is going to be a matter of negotiated equilibrium in the application spaces that the DRM or rights management systems are used.

I think there are some principles that go along with that. Don't censor or disable content. Stuff that works on a PC now, it's a bad idea to go around and try to disable it. That goes against the principle of enabling your stuff, and if you ever blow it, you're in deep trouble. The intention is not to lock out the vendors or format. In fact the whole idea is the DRM layer ought to be interoperable in that 360 degrees of policy dimension. There ought to be a standard to say what you want, and have it both be extensible when you think of new stuff, and have it enforced whether it's your technology or not that's doing the enforcing.

With end user control, one of the common questions is, "Who owns the key?" and the answer is, "Nobody." The machine acts on behalf of the user. If the user allows a certain set of operations to take place protecting a certain set of content, it does that. If the content is the user's content, it acts on behalf of the user. If it's somebody else's content and the user said, "Go ahead and protect it the way I've agreed to," it acts on behalf of the user. But there's no key that's owned by somebody. There ought not be in such an operation.

It won't be perfect. It can't be perfect. Bob [Blakley] is right. There's a sort of famous guy I like a lot at Microsoft called Butler Lampson who, one of his favorite aphorisms is: "the enemy of good security is the demand, not the quest, for perfect security." All these systems are trying to do something. None of them are trying to achieve perfect security. They're trying to provide a benefit, some sort of describable benefit, for the people who use it. In the case of enterprise documents, that's to keep documents from leaking, either accidentally or, in some cases, on purpose. In the case

of video, and for consumers, it's to try to have a reasonable sales model so that people can: (a) use their PCs to do what they want, which sometimes, believe it or not, is to look at videos, and (b) not destroy your entire business model. So it won't be perfect.

I've heard two comments on the "DarkNet" paper, and I do want to correct a couple of almost misimpressions. The purpose of the paper was not to say, "DRM, you should just abandon it"; nor was it to say, "You shouldn't do enforcement on a client machine." There are lots of reasons you want to do that, just for pure computer science reasons. There are a lot of things you do which you may or may not think of as DRM. The purpose of "DarkNet" was not to say that DRM wasn't useful in all these domains; it was to say, "Wake up, be realistic." If you're selling a book, realize that somebody could type the book in. Arguing over whether the system was perfect was a little bit useless because there's already a medium for injecting that content into the Internet, and you don't solve it simply by doing client enforcement. And in fact, the best thing to do is offer customers good legal, reasonable choices, probably with DRM, maybe without it.

So there are a lot of models this enables, and I want to make a slightly arrogant, technical statement and a very humble policy statement: I think we can build systems that give the user control, that let people achieve this negotiated equilibrium, but I don't think, as technology providers, we know the answer to how the policy is going to evolve. That's my key message, and that's the thing I think has driven most of our designs: it's policy neutral. The person it's protecting is the person it's protecting, and it won't do that unless the user says so.

GREEN: I would like today to focus on one aspect of digital rights management and its bigger and somewhat meaner brother, trusted computing. One of the subjects of my talk here is whom do you trust and why should you trust entities that perhaps may not trust you.

Let me tell you a story. In the fall of 2000, I worked at the time for a fairly sizable vendor of security products used throughout the industry and received an invitation from this new association that I'd never heard of called The Trusted Computing Association. It sounded really good. What this invitation said is that, "Hey, we would like you to join us; we've been founded by some of the largest players in the computer industry, and what we would like to offer you is 'secure boot.'" Now "secure boot," as I understood it at the time, would enable my applications that are running on top of an operating system to not just know what operating system they are running on, but also what is running underneath the operating system. For example, has my hardware been compromised given the applications that we did? This seemed quite important.

I attended some of the formative meetings, and at one meeting, one of the founding principles of this Trusted Computing Association, TCPA, after we were discussing secure boot, said that one important thing you need to remember is that they were not building a DRM system. Why was he talking about a DRM system when we were here to talk about secure boot? I let it go for a moment, but a few minutes later, he again said, "It's important to prevent the public from thinking that we are building a DRM system." After two or three such remarks, I started to wonder, "What is going on here; what are these people really up to." During a break, I took aside one of the other founding members of the Trusted Computing Platform Alliance and he told me, "Listen, it's very simple. Our operating system platform, on a general peer purpose PC, currently does not have server content available, such as, for example, high quality streaming video, that our customers demand. The content owners, or I should say the accumulators and distributors, have told us that they will not make this content available until such time that we have these features available on our platform. We don't have much of a choice. We have to solve this problem one way or another." While I understand that the future for digitally released content, certainly in the home environment, is of importance to future business models, it still didn't quite explain to me why some of the largest companies in the business here not only were in the process of implementing new hardware-based digital restrictive management technology, but actually at this point in time really had conspired to keep the public and the customers in the dark about the true purpose, which was DRM. I'd like to address some this today because after a few years, I and some of the others in the industry believe we finally figured out why.

First, however, I need to somewhat definitely define what the word "trust" means when used in the context of "trusted computing." It does not exclusively mean that you as the owner can trust the processes running on your machine. It also, and perhaps for the purposes of our discussion today, more importantly means that third parties can trust that your computer will disobey your wishes. Third parties by means of trusted computing will know that your computer will implement whichever digital rights management system the producer of the content has placed on the content. The analog to this in the analog world, as opposed to the digital world, will be that a book vendor will know that you can read a book only once, and then only with a special light that they will also happily sell you.

However, that is certainly the classic DRM application. There is another side to this. Providers of trusted computing products, especially if they're in a dominant market position, can trust that potential competitors will be prevented from competing in the future ever.

Some of the obvious business objectives of trusted computing and the DRM it implements are, of course, the usual: prevent CD ripping and Divx creation. Something that hasn't been talked about much is the plugging of the analog hole. What's the analog hole? Well, today's computers are high quality. Even with the best digital rights management system, you can still feed the speaker output right back into the sound card and digitize, which will give you a darn good copy, one that will certainly sound fine on the computer speakers on which most people probably listen to their MP3s.

Another issue is enabling flow control, information flow control, which I won't get into today. It allows the application provider to prevent the use of unlicensed software. Now this is something of more interest to application providers, if you're an application provider. It thereby, as this gentleman from this operating system and office productivity company told me, will allow the PC to become the core for home entertainment center, growing a new market. The PC industry fully understands that at the core of your future home entertainment system there will be some device processing data, and that device can either be manufactured in a PlayStation-like fashion by Sony or it come from the usual vendors in the PC industry. The PC industry does not want to lose this market to Sony. They need to compete and this is fairly understandable.

And lastly, it creates new market opportunities in the governmental sectors. Government employees are notorious for leaving laptops with top secret data on buses and in train stations. This is repeatedly being reported in the press. Having hardware security that prevents third parties from getting at this data obviously is a good thing and a clear and very legitimate market for it.

So, let's look at some of the upcoming hardware/software DRM features in office productivity software, and here I would like to quote Bill Gates from Microsoft, "We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains." Why is that? Rather than hoping for a potential market expansion in the home entertainment system market, there certainly is a current clear market for office productivity software—Word documents, e-mail documents, what have you—and there is at least some demand, and certainly some vendors believe there is a massive demand, for this technology. For example, you can't forward this Word document outside the company or, I should say, you can perhaps forward it, but nobody else at the company will be able to open it. Or you have some e-mail that only can be displayed on your screen and by the way, we're disabling screen copy so you can't just dump it to a graphics file. Or a document as was also stated would only be valid for so long, and then will no longer be readable regardless of

what PC you copy it to because you have a secure clock, there's no such thing as setting back the date.

If you are the CEO of Enron, you would just absolutely love this technology, because there would be no evidence left for discovery. So yes, there are clear benefits. It's not clear that these are clear benefits to society.

Question: what does the federal prosecutor call a third party application that is compatible with the proprietary DRM format? An illegal circumvention device. If you build compatible software that can read a DRM wrapped file format, you, at least as long as the software is open, thereby enable third parties to infringe on such digitally rights-managed content. One hypothesis, and certainly my hypothesis and I believe it is the vendor hypothesis, is that this will make it illegal to create interoperable software in the United States, interoperable with software that has DRM features enabled subjecting software authors to substantial penalties. So what are the choices? Don't create interoperable software or spend five years in prison. As a product manager for software, this does not sound very appealing.

Lastly you will hear that DRM is voluntary. That is absolutely true. It will be voluntary. You do not have to turn on your computer; you do not have to power it up; you do not have to read the documents that are DRM wrapped and that will be sent to you, which if it becomes enabled in office productivity software, of course, will be something that you will probably have to do to do your day job; but you don't need to do that. Nobody is forcing you with either the law or physical force. Thank you very much.

FARBER: Let's start with some miscellaneous comments just while I have the microphone. One of the things I think we've suffered incredibly from is having a marvelous religious war and not paying any attention to understanding very clearly and articulating what the technology is capable of doing, what it isn't capable of doing, what its limitations are in a technically valid way, and instead arguing that the world is going to collapse or the world will be sunny. It is real good for some newspaper reporters but it doesn't help at all in understanding really where we are. I recommend strongly we stop having religious discussions for the time being, at least.

The other observation, for those who don't have historical perspective, is rights management is not a new idea. It's been tried ever since I've been in the computer business, and I go back quite a ways. It's always suffered from the fact that, in general, it's been a software product, and software products are easy to break, very easy to break. That means that in fact they've been not very useful things.

A couple of systems have hardware protection. Luckily or unluckily, take your choice, they never quite made market. Certainly when we designed the original Motex system, that was an issue. It wasn't rights management. It was protection of documents, protection of private information.

I was an advisor to TCPA since its beginning. Along with some other people, I have no benefit from it, I haven't even gotten a trip out of it, but I had some interesting discussions in the very early days. Let me make two other comments while I've got the microphone and then I'll get to the meat.

The ARPANET was not built to survive a nuclear attack and I wish people would stop saying that. It would not. And finally, anybody who would like the FCC to be in a regulatory position of new business models deserves what they'll get. I served there for a year and a half, and tomorrow, in fact, we're having a conference down in Stanford, for which the intention is to get the FCC out of the spectrum-regulatory thing.

Let me punch in some stuff. I'm not going to spend a huge amount of time. A lot of what I was going to say has been well said, but I think it is important to push down on the issue of security, and I understand, the lack of perfect security. If we look for perfect security, we'll be here for the next five hundred years. However, an acceptable level of security is getting more and more important in the world we live in. It's important for individuals, it's important for corporations, and it's going to be increasingly important for nations. Things which increase the level of security are very hard to turn down, realizing that of course they're never perfect.

When you have a relatively secure system, I would hold that it is very difficult for you to keep out a rights management system, especially if you don't own the machine down at the gut level.

But in fact if you have anything other that boot privileges, the equivalent which most of us have, it's reasonably hard to not host the rights management system. If you say by law somehow that you can't implement rights management, you are essentially saying by the time you're done that you are not going to be able to build or at least market a secure system, and I think that's a bad trade-off. The details of that, I think, deserve study and deserve careful looking at.

The other thing that I'm less interested, and always have been less interested, in is protecting media companies against people "illegally" using their material. I would never do that, of course. But I am very much progressively interested in having people not gain access to my personal in-

formation, and that is getting to be a serious problem, and it's going to be an even more serious problem in the future.

And protection mechanisms—and I'll avoid the words "rights management"—have a very important goal in protecting my information, and being able to find out who's looked at it, who's made copies of it, who's passed it to whom. The same type of stuff the media companies claim they would like to know for their own market purposes, I want to know for the protection of my own data, and I want mechanisms which enable me to do that. Whether those mechanisms are used by other things is going to be an interesting issue that's going to have to, at some point, be decided by legislatures, by courts, and the marketplace—you don't have to buy it.

Down at the FCC, I spent a fair amount of time being in the middle of long discussions about the other type of rights management, things that sometimes show up as broadcast flags and other various schemes designed to protect the transmission of high quality digital video largely—the Disney problem, I used to call it, or sometimes the Mickey Mouse problem. I certainly do not speak for the FCC, but there was a terrible tendency for people to walk in with technologically inferior solutions, solutions that often when you looked at them, you asked, "Well, how good are these?" In fact, I remember one conversation, "How good are these solutions?" Answer: "Pretty good." I come back: "Nine months to break." "Mmm, maybe six." That type of solution, when put on the marketplace just causes a conflict, causes the FBI to be engaged in trapping people or arresting people. The unwillingness of the media companies to pay for good protection, assuming that we want it, and assuming they want it, is distressing because it gives you these Mickey Mouse solutions. I strongly think that that is a serious, serious problem.

I'm not recommending we have rights management systems. I'm just trying to lay out the framework. But I think the exploration of just what can you do in rights management systems to give us maybe better fair use than we have now, at least in the media stuff, might be an interesting place to do some research, maybe, and some explorations, and to articulate what we find, as technical people, down to the policy arena in Washington, where, believe me, there are precious few technical people. Thank you.

VARIAN: I'm going to spend a few minutes talking about some economic issues in DRM and basically I just want to lay out some points for discussion. I'm not going to express any strong opinions here, but I'm going to try to bring out some phenomena that I think are interesting.

One is: we have heard a lot of talk about business models, and the question is: What are the business models that are out there? These are the seven that I know about. So one thing you can do is you can advertise

yourself—that's the Grateful Dead model—give away the music in order to sell the concerts.

Or you can advertise other stuff, and that's, of course, what most media does—radio, TV, newspapers, magazines, and I include product placement where you try to integrate the ad so completely into the content that they can't really be separated without destroying the content. I actually think that's one of the stronger forces that's at work these days, and we're going to be seeing a lot of experimentation with product placement in the next year or two.

Bundle the content with other things, like t-shirts, prizes, liner notes, chances to win a talk with a band, or whatever. There's all sorts of ways you can take products that are apparently scarce, bundle them with the product that is inherently not scarce, and then charge for the bundle.

Subscription, versioning, non-linear prices are all ways of dealing with something other than a paper use or paper piece structure, and it's attractive because from the viewpoint of economics, what's interesting about information booths is that they have zero marginal cost, so you'd like to have a zero marginal price, and there are various ways you can do that, from an economics point of view.

You could just have much lower prices and higher quality for the legitimate version than for the illegitimate copies, and we've heard some discussion of that, as well.

Micropayments is another thing that I think people are very skeptical about these days, and when you have technology that enables micropayments, like cell phones which allow for the billing as part of the service, then you see a lot of content that can be offered there, and we've seen that happening particularly in Japan.

Finally, the digital rights management which is controlling the terms and conditions under which the product is consumed.

So that's my list of seven. I think it's important to start thinking about these business models, and really laying out what their pluses and minuses are. For example, there are a lot of bad things about product placement as well, but still, it's something that enables certain kinds of behavior.

Now when we look at this digital rights management and the choice of terms and conditions under which the product is consumed, it's important to understand that a rational seller, profit maximizing seller, will want to choose the bundle of rights that maximizes the value of the product, not maximizes the protection; and the trade off here is that the more rights you give the consumer, the more valuable the product is to the consumer, because they can do more things with it. But of course, it may be that you

have fewer sales because of leakage and sharing and copying and other things like this. So the trick is to choose the right tradeoff for libraries, for-profit libraries sprung up in England in the mid-1700s and early 1800s. The publishers hated this idea; they thought it was terrible that you would have these libraries spring up and of course, the availability of the low cost literature increased literacy, increased the number of habitual readers, and created a much larger market than they'd had before. Pretty much the same story happened with the video machines, a couple of hundred years later, where there was a lot of fear and loathing of video machines. Of course, we all know that's created massive new markets. When the DVD came out, it was quite interesting that the DVD was targeted from the very beginning at a purchase market, to make the price low enough to discourage rebels and encourage purchases and the DVD has been a hugely successful technology, in part, because of the economic model that they used.

. . . .

The point is if you sell it for a high price and it has a lot of rights, well then, the trouble is you might increase the incentive to try to share among consumers in that context. So the lesson is that cripple-ware is not the best thing to do necessarily. It inherently reduces the value of the product, and of course, it's easy to compete away copy protection. So whenever you do have a lot of competition out there, as we do in content provision, it's very hard to enforce solutions that inherently make the product more difficult to use.

Now, I want to say one last bit about innovation because innovation is in the title of this meeting. There are very interesting kinds of protection out there, not just for information, but for other kinds of physical products. For example, Epson makes a printer that has an inkjet cartridge. The inkjet cartridge has a chip in it, and the chip says, "You can't refill me." It'll count down, when the ink is all gone, and when the ink is all gone, it can't be reused. Now actually, on the Internet for twenty-five bucks, you can buy a device that will reset this chip. Motorola makes a cell phone that only allows certain batteries, it has to be a Motorola battery, because it has a chip in it that says, "I only want to connect with Motorola phones," and Motorola phones only want to connect to this battery.

But then there are interesting innovations around each of these technologies. We have some people over in computer science and electrical engineering who are printing integrated circuits using off-the-shelf inkjet printers with magnetic ink and metal-coated plastic. So you can just take an off-the-shelf ink jet printer, hack at it a little bit, modify the ink and print out integrated circuits. So it's quite a nice technology, and can totally change the economics of that business if they can ever get it to work suc-

cessfully. There are some people who are making generators in your shoes, so you walk along, and you can charge up your cell phone, and charge up these other devices. Just put a little generator in your heel, and as you walk around, you can create a charge. And finally, the last example is: last summer in England, the number one song in most of Europe was this thirty-year-old B-side single from Elvis called "A Little Less Conversation" that Nike had used in its sponsorship of the World Cup. This had been re-mixed by a Dutch disk jockey who added some techno beat to it and made this new kind of music that people really loved.

Now, each of these technologies, each of these innovations, would have been very difficult to do if you had really perfect copy protection. If you have these non-refillable ink cartridges, you can't adapt them to different purposes. If you have these cell phones that only accept certain batteries, then you can't build this charger that runs through walking around, and if you make it very difficult to rip the CD, then you can't modify the music, update it, change it, and use it as an input to further innovation. One of the best things you can do as a business is try to draw on your user experimentation. There's a very nice set of work by Erik von Hipple at MIT about how strong this force of customer innovation is, and he has dozens and dozens and dozens of examples where you learn a lot about how your product can be used by making it, by providing tool kits, and making it easy for people to modify it; and so if you restrict the way products are used, in some cases, you can lose the benefit of that kind of innovation. So that's a danger that may be outweighed by other benefits, but it's just something people should be aware of.

. . . .

ALBEN: I'm Alex Alben with RealNetworks. I'll start with a confession, which is, when I took real property from Paul Goldstein down at Stanford, he spent the first day of the session talking about a bundle of sticks, and I didn't understand. I was thinking of real property, and he kept talking about sticks, and it actually kept me, for the next 20 weeks, stymied. I wasn't able to get to springing rights and flowing rights and the other things, and I ended up not doing very well in the class, which led me to my career, ultimately, in the software business, where we don't deal with real property. But it really came home to me that what he was talking about in that first class of real property was that intellectual property can be split into bundles of sticks; and I think we should change the metaphor for our world into bundles of splinters, because you can take the digital product and obviously parse it in the ways I'm suggesting. Now this has come into conflict with people's expectations of property and copyright, because when you buy a CD, you don't think about, "Well, I'll only use

this CD and this one CD player," or "I'll only use my CD on Sundays, and that's the only time that we'll play on this device," or "I'll only play it three times and then it will disappear." Actually it will still be locked onto my hard drive, but the rights to it will disappear and I'll have to circumvent and commit a crime in order to listen to it a fourth time. This has become a very real problem for our society, and, I think, for the industries that are thinking of building this digital marketplace. And I'll be a little less abstract than some of the other presentations and talk about the problems that we've encountered in the real marketplace, the early marketplace, for creating digital distribution of media.

I have a thesis, which is that we need to maintain both a personal use right and copy protection in order to build a marketplace that works. Now, we know that DRM enables business models, and Hal [Varian], I think, did a good job with some creative examples of business models and price points. It's happening with music subscription and video subscription in an early way. It's happening in general entertainment for some products that we and other companies have put out.

The problem is not so much, "Is there DRM technology." We don't pretend to have a perfect DRM, and if anyone sold you a perfect DRM, you should probably pay at least a dime for it. We have a reasonably good DRM that is protecting content in the marketplace, making it difficult for the average user to circumvent or break the DRM, therefore supporting the business model and the price point. If you're offering something for $10 a month, you might not need a DRM that a team of scientists led by Ed Felten, or somebody at Berkeley, could spend, three months with 12 supercomputers arrayed and eventually break. It would be easier, maybe, to go and spend the $12 at Tower Records. So, we have a reasonably good DRM, and there are other companies in the market place, such as IBM, such as Microsoft, InterTrust, who also have reasonably good DRMs for the purposes that the content is being distributed for today.

The issue, I think, is not whether the consumers are enabled or whether the technology exists, but one of the issues is, "What's the price point?", because we have split the bundle of sticks into the bundle of splinters and toothpicks and other things that consumers no longer recognize. What's the price point of a 30-day download that's tethered to a single computer? Now we've run into this issue directly with MusicNet and some of the other services that we've brought to market. If you talk to the music publishers, the people who administer the rights in the composition that is embodied in the sound recording that is being distributed in that digital download, they'll say, well, it's about seven and a half cents. Funny that

they should come up with seven and a half cents because that is exactly the same price that they get when a CD is sold.

Now you can say, "Hmm, do we live in a parallel universe?" A CD has a lifetime of what? Let's say 10 years. It's really, you know, until somebody in your house scratches it or you lose it or you move, but 10 years with how many unlimited number of plays? How many months is 10 years? 120 months, right. So, you're getting 1/20th of that value, and of course, you can only play it on one device in my scenario. So let's say you discount it further, so maybe you should pay 1/240th of the price of seven and a half cents. I'd say that's reasonable. At least that's supported by the differences in the technologies, but if you talk to some of the publishers, they'll say, "Well, we'd be happy to license this to you, but at seven and a half cents per copy per month."

I want to talk about what we need to build the marketplace, which doesn't involve everybody taking. It actually involves everybody giving a little to make it work. For content owners, not just the record industry, but the entertainment industry and anybody else who has valuable content to protect, I think the requirement is that they put the product into the marketplace.

And in order to effect the licensing of that product, we need licensing mechanisms that allow for mass distribution of content. I'll pick on the music publishers again because after a time, the tech industry, with Microsoft and RealNetworks and others, was able to convince record labels and work with them in partnership to create some systems. You can say they're imperfect; you can say the rights aren't there. You can say the Beatles aren't there—and I wish they were. But the problem is that another set of rights was necessary for licensing, and if you address the music publishers, they'll say, "We're happy to license this to you. Give us the form." We'll say, "Well, we have 100,000 songs we want to license tomorrow." "Well, we can't accept that in electronic form." "Well, can we send you a spread sheet?" "We're working on that." "What do you want to do in the meantime?" "Well, could you send us some written, per request of what you need to get per song, and then we'll try to identify the rights holder."

I said, "This isn't going to scale." We have the rights already to distribute 100,000 songs from the labels, but we don't have a licensing mechanism that is easy enough to support the business model that we have built. And this, I challenge the audience, is where we should pressure our legislators to actually do something. It's worthless to create a quasi-compulsory license for one half set of rights without another compulsory license to affect the purpose of that compulsory license.

Maybe we don't have to call it a compulsory license because that's a loaded word. Maybe we should call it a safe harbor. Maybe we should call it a notice provision. Whatever it is, we want to pay the songwriter. We want to pay Lennon and McCartney, or Michael Jackson or whoever owns that catalogue of Beatles songs. And we're willing to put money into a pot, but what we want to say is, we want to put this in the marketplace tomorrow so that then we can collect the revenue and divvy it up according to usage. It's an important gating item for this marketplace to work.

Consumers have to use products in ways that are consistent with personal use. If I went to my neighborhood in Seattle, and took my CD burner and had a stack of 1000 CDs and stood on the corner and put up a sign that said, "CD Burns Free," everyone would come by. I'd just say, "Here's the CD. There's one for you and one for you and one for you." Eventually I'd cause a traffic jam, but the point is it's not legal activity within the scope of accepted personal use, and file sharing to 1000 people that you don't know is also not personal use. We need to disabuse ourselves of a concept that just because the user may not know that the default setting on their PC is to share to the rest of the world, that that is somehow justified behavior. It isn't justifiable behavior. If consumers want a reasonably placed product in the marketplace, if they want to encourage content providers to put that product in the marketplace, then they need to act in a way, we need to act in a way, that's consistent with our traditional rights in personal use.

Tech companies, we need to enable the business models, make DRMs transparent to consumers and not make them jump through 12 hoops in order to authenticate content and get rights.

For the government, we would say, and I'm really happy that RealNetworks and Microsoft and Intel and other companies will violently agree on this point, please don't regulate this industry, please don't mandate, and please don't choose winners. That is not a formula for innovation. You know, the government in India has the spec for automobiles, and they say in India you can buy the best 1950s car on the market today. We need to live in an industry with a vibrant society, creating new technologies, and constantly innovating. It's not going to happen if we have to go to an FCC rule-making every time we need to change the spec for a product. To thinkers, such as people in this audience and the people who put together this conference, we need to create this intellectual framework for the new paradigm.

What are the challenges that remain? Crafting a fair use exemption for distribution of a circumvention tool that does not swallow the rule. This is a hard problem. I don't know how to figure it out. I would love for a prod-

uct of this conference to be a variety of proposals and papers that allow this.

The second is limiting application of the DMCA to protecting valuable media. Was the DMCA intended to protect the distribution of garage door openers and printer cartridges? I was told today, there was an injunction issued this morning in the printer cartridge case, the Lexmark case against the company that was distributing substitute printer cartridges because it read a bit of code on the header file, or inside the printer, that enabled them to substitute. Now, I would say this is out of the scope of the DMCA. It was not what we intended when we were drafting the provisions of the DMCA. I think that we need to come back to reality because we do not want to live in a society where, by putting five bits of code in front of any product, you are not allowed to, and you are committing a crime if you use that product. This is a travesty, and this needs to be addressed legislatively because the law here is not at all clear.

The last thing I am going to talk about is the Broadcast Flag. We have a modest proposal on the flag. I think that, in the interest of what Mr. Farber said, and I take him seriously, we have to stop with the religious objection to something just because it's proposed from one side or the other. We really have to try to listen to what they are trying to effect. The point of the Broadcast Flag is that it is a very limited technology. The way it is proposed today, you can make unlimited physical copies of television programs if that's your desire. You can also circulate it within a home network. I think if we religiously oppose the Broadcast Flag as an industry, we are going to be sending the message to the entertainment industry that we're not willing to cooperate on anything. And that is going to lead to a Hollings-type approach, which I think we can all agree is anathema and is going to retard innovation in our industry for years and years to come.

We do have questions about how a Broadcast Flag would be implemented. We would prefer that the FCC not take jurisdiction over this because we think it is the thin edge of a wedge for government to start regulating the network. But if we don't listen to the concerns of copyright owners and effect reasonable rules for distribution of content within a home network, then we're not doing our part as an industry.

So, there are challenges for all of us, but DRM is here today, in the marketplace. DRM is an abstract concept. It's just a set of technologies. It can be used for good or for ill, and as always, the challenge is to craft the balance that will enable us to move forward. Thanks.

GREEN: I would like to make one comment to Alex's statement regarding Lexmark. I think most consumers and most rational, reasonable people probably would agree that the uses to which the DMCA has been

put by the industry were not within the scope at the time the legislature passed this law. However, everybody, certainly those pushing DRM onto the consumer, will all readily agree that DMCA has been overused, and some of these uses of it have really been an abuse—for example, we had the printer cartridge, and another one that you may not be aware of, which hasn't been litigated yet, is the cell phone batteries in your phone, which not only do cell phones not accept some third, some after-market batteries, but the ones you are getting from your vendor in many cases have secure chips in them that keep track of how many times the battery has been recharged, and as this counter goes up, the battery will accept less and less charge, not because the battery's running out but because the chip counter tells it to accept less charge so you have to buy a new one.

. . . .

It really does not matter what the proponents and providers of DRM believe that DRM should be placed to. All that matters is what the courts believe, and the courts believe that these uses of DRM and the DMCA are legitimate. I would like to echo what Alex said. Unless the law is changed, these abuses are not unlikely to diminish, but only likely to increase. So let's be careful with what we're asking for.

. . . .

QUESTIONER, PAM SAMUELSON, BOALT HALL: I would like the panelist to talk a little bit about patents on DRM technology. It's my understanding that there are two seemingly conflicting patents, one owned by InterTrust and one owned by ContentGuard, and it seems to me that when we're talking about competition and innovation, if you have two—the InterTrust patent, as I understand it, has recently been acquired by, I think, Sony and Philips—big players, how does an open source developer who might want to do DRM do so, or where does the individual author turn, who might want to self publish and use a DRM system, but finds him or herself in a marketplace where only the big players are licensed to use these patents? It seems to me that there are some interesting issues, and I'd just like to see what, if any, comments you might have about that.

FARBER: There are more than just those two in the rights management patent game, and there's going to be some interesting battles on those. That's a big problem. A lot of those patents, in my humble opinion, aren't worth the paper they're written on, but that doesn't prove very much in the courts. My main observation is it's more than two. There are a number that have patents that are put in this area, and a lot of old technology that I think is prior art.

MANFERDELLI: I would say so; the InterTrust one, we're the one being sued, so I'm not going to say a word about that. I know that much. I don't think ContentGuard is in any litigation at all. I do think that whatever the terms of use are quite important. I think, you know, there are several levels of use. There'll be many vendors selling DRM systems, and my expectation is that after the mess quiets down, they'll be licensed one way or another. And the publisher, whoever is trying to publish the content, whatever it is, will most likely use one of them under reasonable terms, but it's got to settle down first. I'm not sure what else to say since I can't tell you what the patents are going to cost under certain circumstances, and as I said, in the particular circumstance you brought up, I don't control that. Microsoft does own a part of ContentGuard, but it's a minority share. Patents are a difficult issue, period. You could probably have several conferences on that without a complete resolution of the details. And I don't know what else to say, except we, in technology, not DRM, who live in that patent environment, we're just going to have to muddle through for a while.

. . . .

GREEN: Certainly patents by their very nature are intended to prevent competitors from producing products that will compete with the offerings that you are making. If a company chooses to not license a patent that's underlying some dear and near technology, and thus, prevents, for example, open source competitors, for whom it is very difficult to license patents on anything other than a world-wide, royalty-free basis, I would contend that the not licensing, and thus preventing the open-source competitor from entering a market, is not necessarily incompatible with the business models of the patent holders.

One patent that springs to mind here, that actually I haven't heard much about, and maybe John [Manferdelli] can enlighten us here, the new DRM technology, formerly called Palladium, now an acronym nobody can pronounce—Next Generation Secure Computing Base—is based on a patent that Microsoft holds called the Digital Rights Management Operating System patent. In the past, and certainly in the present, Microsoft has frequently stated that one could build an open source implementation on top of the underlying technologies, build their own secure micro-kernel on a technology on which Microsoft holds the patent, as an open source application. What I haven't seen so far is a public statement by Microsoft that Microsoft intends to license this patent world-wide on an open source development, on a royalty-free, in perpetual, basis. Is that Microsoft's intent?

MANFERDELLI: Let me first say, the technology, whose name I'm not going to try to re-pronounce, is not based solely on that patent. We'd

probably name it differently than we did for that patent, not just because it would have sounded better, but because what we're thinking of doing with it is a bit different.

You're right, though; Microsoft has not announced any patent licensing policy on that particular patent. I can't tell you anything other than I hope we do soon.

III. IMPACTS OF DRMS ON FLOWS OF INFORMATION

Panel:

David Wagner, Computer Science, University of California, Berkeley (moderator)

Hal Abelson, Massachusetts Institute of Technology

John Erickson, Hewlett-Packard Co.

Joseph Liu, Boston College Law School

Edward Felten, Computer Science, Princeton University

Larry Lessig, Stanford Law School

WAGNER: We've got a great session for you here. My name is Dave Wagner, I'm from the computer science department here at Berkeley and we're going to be talking about the impact of digital rights management on information flows. We've got a fantastic lineup of speakers today. So let me introduce you to our panelists. I'll introduce them in the order they are going to speak. I've asked them each to speak for ten minutes on the topic, and we should get a nice diverse set of perspectives.

At the far end, Hal Abelson will kick us off. Hal is a professor of computer science at MIT. His name is familiar to me as a computer scientist because he is one of the co-authors of one of the classic introductory textbooks of computer science. He is also a long-standing member of the computer science committee. He's done some great work. He's widely recognized for his teaching and other efforts. Second speaking will be John Erickson, who is a principal scientist at HP Labs. He tells me he's been doing work on digital rights management since before it was called DRM. It's great to have industry's perspective. Third we have Joe Liu from Boston College Law School, where he is a professor. He has a paper in the proceedings addressing the impact of DMCA on researchers and on scientific research, which I highly recommend to you. And then Ed Felten will be speaking fourth. Ed is a professor of computer science at Princeton University. You may know Ed—Ed is famous for many reasons. He served as an expert witness in the Microsoft trial. He's been threatened

with a lawsuit because of a paper he wanted to publish. But I can tell you as a fellow computer scientist, he has also done fantastic research in computer security and related fields. I suspect he's become more of an expert on the DMCA than he expected to be, and he's going to give us a perspective on some of the public policy impacts of the laws. Then finally Larry Lessig will speak. Larry is a professor of law at Stanford University and has written a number of seminal books in the field, and is the chairman of the Creative Commons project. He'll be speaking about the Creative Commons. So without any further ado let me just hand things off to Hal, who will get things started.

ABELSON: I couldn't help putting up this nice picture of the Statute of Anne where supposedly all of this recognition of the rights of the creators comes from. Pam [Samuelson] also said that of the communities that are here, she'd like us to talk to the policy makers, so what I want to say to the policy makers is: watch out. You are surrounded here by two very dangerous, delusional communities: the lawyers and the computer scientists, who tend to suffer from the same delusion, and that delusion is that you make things better by making them more precise. So let's take a reminder of what it is we're trying to do. See, there's this thing called the public good, and then the lawyers go and create laws about the public good, and already you see the legal code—Larry [Lessig]'s word—is at best a fuzzy reflection of this thing called the public good. Then the computer scientists get into the act and they create these things called standards, which supposedly implement some impression of what the law is. And while it's actually pretty bad, it's hard to make a DRM standard that has fair use, so let's sort of not worry about that now—maybe we'll get one in ten years and then the real joke happens. The computer guys really get into the game, and they make supposed implementations of these standards, which are the biggest distortion of all. Ed made a very good career pointing out the difference between java implementations and java standards as it comes to security, and this is ok, right? This is how the world is. It is not perfect; you're not going to get that last precision of law that reflects public good, you're not going to get that last precision of implementation that reflects standards; and the real problem is, now we come in and we put on this thing, the mattress tag, "do not remove under penalty of law." So let me say to the policy holders as you listen to these things about DRM, the key legal principle that is missing from this discussion is not fair use. That's a lawyer thing, and we've been talking about it the whole time.

The key legal principal missing is the de minimis principle. When we design, when you look at these DRM designs and you evaluate them, you

say, "Have you fallen into the delusions of the computer scientists and the lawyers?", which is often expressed as, "Boy, it would be really great if we put up a system where practice has to conform to policy." It doesn't work that way. We have to look for the friction, the flexibility, the fuzz in these systems that avoids them from being these legal-computer science wet dreams, that if we can only be very precise about everything, that will serve the pubic good. That's not really what I want to talk about. I wanted to selfishly tell you a little bit about my world and what copyright looks like there. This is all about copyright, where we're putting all these systems in, and I wanted to tell you what scientific publishing looks like from the perspective of the research universities.

So the lawyers tell us that this is about the world of scientific journals the lawyers tell us that copyright is policy. So inventors, authors, scientists, are now invited to give their property away to the journals. Give it for free, or in some cases even pay journals to take it by paying page charges. The journals in turn now own this property and all rights to it forever. Well, limited time forever, but forever. And the journals, in some arbitrary scheme that's totally up to them, magnanimously give rights back to the authors. The university actually doesn't enter into this deal at all, and who knows about the public.

So I just wanted to show you for fun some of these contracts by which authors give rights to journals. Here's my association, the ACM (Association for Computing Machinery. I give the ACM the property. It is now their property, and in their generosity, they allow me to post that for my own personal use on a website. But of course, my profession is pretty liberal here. We could look at a more standard thing like Elsevier, we're going to give Elsevier our property and Elsevier is going to give me the right to present my paper at a conference. Isn't that great? Actually, Elsevier's not the worst either. I'm really glad I'm not a chemist. If I were a member of the American Chemical Society, I would have the right to send the paper to fifty of my colleagues and to post not the paper, but the title and the abstract and the figures from it; and of course, all these guys are amateurs if we go look at the New England Journal of Medicine. The New England Journal of Medicine is not confused at all. They said, "This is ours, period. What we give you is, well, you get the same fair use rights that we have to give to everybody else."

Now, why are we making this deal? We're making this deal because publishing is a serious business. This thing is either under the control of the journals or unknown individuals, and "we should not cede copyright to the individual authors." Where did these guys get the copyright from in the first place? So this is not the world that the Statute of Anne ushered in.

This is the world that the Statute of Anne helped usher out, which is the world of the stationer's company. It's the stationers' fall in the early 17th century, and what that world is about. It is not about the creativity of the individual authors. It is about the right going to responsible parties who will exert sort of cartel control because they control the infrastructure. Now is that a good idea? Well sure, publishing is a serious business, and we want all the great things that journals give us, but there's all sorts of other stuff that we might want. We might want indexing. We might want integration into semantic web. We might want all sorts of things that nobody has thought of yet. This is the promise of the Internet.

We put up Google and there's all this wonderful stuff. Unfortunately, it's not the most wonderful stuff because the most wonderful stuff is locked up behind some publisher's wall. What kind of applications can we imagine? Well here's a nice one: it turns out you can go on the web and look at a concordance of the works of Henry James. So I might want to go look at the concordance of *The Turn of the Screw*, which you remember is this wonderful novel about evil. So you might want to see how many times "evil" appears in *Turn of the Screw* and you hit this button. It turns out to be only seven; and then I can look at any one of these places, and I can see the context of where the word "evil" appeared. High school term paper heaven. And I can get that from Henry James and I can get that for Henry Way. I can get that for all sorts of things. No one, of course, after 1923, because the innovation has been stopped. So, the thing I want to leave you with is: Will the need for sophisticated access tools be stillborn? Or, there's actually a flip-side, and the flip-side is that lots of people in this new stationer's company will make lots of investments for this, but what they're going to create are network effects. And these network effects are not about the content. The content, I heard Bob Blakley say, "This is all going to go priced down to zero." This isn't the problem. The problem is that the content infrastructure is going to be owned. If I'm a publisher with a journal which has cross-indexed 50 percent of the literature, why would anybody want to go to another publisher to be a journal? So digital rights management with the force of law behind it can effectively re-create the role of the stationer's company. And I'm not kidding. Here's a quote from a publisher, and this is a marvelously paternalistic quote: "We're going to give scientists all the data they need, universities are going to license it, and we're in charge and you should be happy." Probably half the people in the room can guess who that is. That's Elsevier. Dirk Haank, head of Elsevier should be very happy because Elsevier Science runs at the 37 percent profit margin, and their cost to the libraries has increased at a nine percent annual rate since 1991. The question is: Are we headed back to the

world where we have legally sanctioned monopolies that dominate the infrastructure? The question we should be asking is: Is that world going to be ushered in and cemented for a very, very long time by this approach of digital rights that we're taking? Okay, thank you.

ERICKSON: What I wanted to focus on was the very beginning of what Hal was talking about when he had those overlapping bits and pieces getting fuzzy. I was sort of troubled in what I should call this, whether I should call it "policy enforcement and the free flow of information" or "policy enforcement versus the free flow of information". I think that ultimately, because it's a cautionary note, it needs to be called "versus." I wanted to give some thanks to Larry as well for this notion of "code" being de facto law. The kind of policies I am talking about, fundamentally, are those that are expressed separately. Actually policies are code. They are just separate code, separately managed. The "good parts" version of this story is that we are seeing regimes come out where they are not being built in. We have had generations of policies built with code, bits that are set or not set in digital stream, or simply formats, whether they are analog formats or digital formats, that are used and controlled. By having separately expressed policies, they can be separately managed, they can be dynamically modified. Policies are used wherever a system has to make a choice, and DRM systems are obviously just a subset of that whole world. We are seeing also this emergence of trusted systems, trusted computing bases, platforms or stacks where policies can be enforced in reliable and deterministic ways. As more research is done in the expression of policies and the applications of policies, we see potentially better ways to have policies apply to exact contexts of use.

So the upside is that, this concept of policy enforcement where policies are declaratively expressed, where policies are managed separately from applications, they are yanked out of the hard coded platform, or yanked out of the code, separately managed and applied where they can be studied, analyzed, improved, dynamically changed based upon context, where they can be transparent to what they do and also where the applications that apply them can be transparent, these are all good things. There is a potential to do things in a lot better ways than how they have been done. The scary and nasty bit is that where of course there is still "code." We are limited by the way that the languages themselves are designed, their expressivity. We are limited by the choices that the people make when they write those policies, what they put in, what they leave out. We are limited by the ability of that thing which is going to make that choice, about "what policy do I apply?", of making that right decision. We are limited by that end system which is supposed to apply that, having that capability to actu-

ally do that, regardless of what the policy actually says. We are also limited by the ability, even the scalability of systems, to determine whether or not they trust some other subcomponent which they may have to interact with.

Another way to state a lot of our concerns is policy enforcement regimes allow a sort of private law to be created because, let's face it, they are in fact detached from reality. They are what the implementers decide them to be. As I said in a previous slide, it's what's encoded, what can be encoded, the decisions that people make. There's no governance into what goes into it, there's no social governance into what goes into a rights expression language, for example. But there are other examples: privacy management languages. One exception might be health care, controlling health care information. But you can aspire to have these constitutionally inspired values in these things. I would say that as we look forward into these regimes, if we are to have these regimes, and I think it's a given that we are going to see these things increasingly, we have got to figure out how to include people in the loop. If you count on policy enforcement regimes, DRM systems, to make the right decisions without people as part of the loop, without people being encoded into the loop, without people being able to make their own decisions about whether they will themselves accept liability if, for example, text is exported from a secure format for them to use in like a review, then we have got a problem. So we have to figure out as we establish policy enforcement regimes how to have escapes.

Another problem that is semi-related to this is that DRM systems can make information opaque. DRM systems don't have a monopoly on this. Lots of digital formats make information opaque—you can't see into it. We've got to think of the ways that encourage the rules that enable enhanced usage of the information, but doesn't constrain the flow. We see here that metadata regimes that augment the deployment of information in various formats are absolutely essential. You don't have to look inside that opaque container, even if it's locked up. If you have got appropriate metadata regimes, you can find the right stuff; find out what you need, even if it is in a secure format. But you've got to have both the accessibility of formats and rules that allow you to use that stuff in appropriate ways. There's this notion of closed information spaces which are defined by built-in policies, the formats that are used, the policies that are written. Examples of these include communities that don't work with certain browsers. They break. That's a policy decision, even though it may seem to be a technology decision. Somebody decided that they were going to exclude a particular browser. Also, information control, the use of proprie-

tary media formats, all these sorts of things. So finally how do we—this is borrowing from Larry—how do we challenge the code? How do we hook reality into these systems? How do we write policies and apply policies in a way that both can be processed in an automated and humanistic way? Thank you.

LIU: My brief remarks today are going to focus on a paper that I've written for this conference. The topic of the paper is the impact of the DMCA on academic encryption research. First some background. As you all know Congress enacted the DMCA in 1998, as a response to perceived challenges presented by digital technology. There are provisions in the DMCA, which are the ones we have been talking about, that impose liability for acts of circumvention, and also impose liability for distributing technologies that facilitate circumvention. Now again, all of you know there has been a lot of debate over the wisdom of these provisions. They are very controversial, and in fact, a lot of the discussion in both today's panels and tomorrow's panels will deal with this larger issue, whether this represents a sensible response to digital technology. My paper takes a much narrower focus, and really looks at how this statute impacts a specific group of individuals, namely encryption researchers—even a subset of this group, namely academic encryption researchers. This group is really a group that pretty much everyone agrees should be largely untouched by the DMCA. Even people on the content side, people in Congress and people who oppose the DMCA, have all at least said that this group should be largely unaffected by the DMCA. So what I want to do here is take a look at that, and see exactly to what extent they are untouched by the DMCA.

When Congress was first considering the DMCA, there wasn't any exemption originally for encryption research, and so encryption researchers testified before Congress, explaining that this was problematic because it could impose liability on them for certain activities that they routinely undertake when they are conducting this research. So in response, Congress enacted 1201(g), which is the Encryption Research Exemption and basically exempts good faith encryption research. That of course wasn't the end of the story, because a lot of encryption researchers subsequently objected that this exemption was a bit too narrow to really be of any good, even after the DMCA was enacted. In fact there have been a number of cases since the enactment of the DMCA where researchers have been threatened with suit. The most famous example would be the case of Ed Felten and his group of researchers who cracked the SDMI watermarking technology, and then were subsequently threatened with a possible lawsuit under the DMCA. You have these concerns that this exemption isn't doing

what it's supposed to be doing, and at the same time, other commentators basically suggesting that a lot of these fears are overblown, that in fact if you look at the exemption carefully, researchers really shouldn't be that worried and shouldn't fear liability to any real extent.

The paper itself essentially makes two claims: one a descriptive claim and one a normative claim. The first descriptive claim has two parts: in the paper I basically argue that academic encryption researchers should still be able to conduct some research without significant fear of liability under the DMCA, but the DMCA will have a non-trivial impact on the conditions under which this research takes place. Taking the first half of this descriptive claim, the argument is that if you look at the statute and the legislative history, and you try to anticipate how courts are going to interpret the exemption for some academic encryption researchers, there should be some area within which they should be able to conduct and publish their research without significant fear of liability. The details are in the paper, and I will refer you to the paper itself, but I think this is an important point to note, simply because I think there is a danger when faced with a new statute, and one that hasn't really been interpreted, to see so many flaws in the statute that you really wind up censoring yourself more than you really need to.

That really isn't the end of the story because the DMCA still, even for these folks who might fall within this category, will have a pretty significant impact on how the research is being conducted. This is because the exemption itself isn't a categorical exemption; it's phrased in a way that actually puts a lot of conditions on people who want to take advantage of it. What are those conditions and what sort of effects can we expect the DMCA to have on people who engage in this kind of research? Here are some of them, and these are based again both on a reading of the statute, and also actual cases involving encryption researchers that want to publish their work and are dealing with the DMCA. I am pretty much going to list these rather than going into them in much detail, in the interest of saving time. First, the DMCA is going to have an impact on limiting who can actually conduct this kind of research, and that's because the DMCA itself, if you look at the exemption, gives a preference to folks who have a formal training in this area or are affiliated with a research institution, or some other institution like that. This is despite the fact that a lot of research in this area is done by people who may not have that sort of affiliation. Second, it's going to impose additional hurdles that researchers have to go through before they can engage in this kind of research. Initially, because you need to probably consult a lawyer to make sure that what you're doing falls within the exemption; and secondly, one of the requirements of the

exemption is that a researcher must seek permission from the copyright owner before engaging in an act of circumvention. The statute doesn't actually say that you have to get permission, just that you have to seek it. Third, it will very likely have the effect of limiting free communication about the results of your research. Fourth, it may also limit the avenues for publicizing your research. Again, this is because the statute gives preference to folk who publish in a manner that, generally paraphrasing, encourages the advancement of knowledge in this area, as opposed to facilitating infringement.

Finally, you can expect the DMCA to have an impact on the actual content of the published work itself; and this results from at least two things. First, to the extent that your paper contains actual code, or very specific descriptions about how to circumvent a technology, it begins to look more like a technology or tool that others can use. Second, because the whole structure of this exemption gives notice to copyright owners during the research process, and actually involves them in the process a little bit earlier, you can expect copyright owners then to ask for changes in the paper, changes that might be very hard to resist. So at the end of the day, I'm saying that even though some research can still take place, the conditions under which this research is going to take place are going to be heavily regulated.

Now, how should we think about this impact? The fact that there is an impact on this research may not be the end of the story, because I suppose you could argue that these burdens are a reasonable burden that these researchers should bear in order to have some additional benefits. Well, on the normative front, this paper argues that this impact is in fact extremely problematic and something that we should be troubled about. I think the easiest way to see this is to sort of back up and consider just how far away we are from copyright infringement. In this specific context, the DMCA is having an impact not on copyright infringement, or even the devices that can be used to commit copyright infringement, but here we're regulating basic research that can be used to create devices that can be used to commit copyright infringement. So we're really quite a long distance away from copyright infringement; and when regulating activity this far upstream, I think you need to be really careful about the potential downstream impacts, because potentially there may be all sorts of downstream effects that are unrelated to the problem that this is trying to get at, which is namely copyright infringement. That's really sort of the main message in this paper, and the argument at the end of the day is that the DMCA itself really is not sufficiently careful about these downstream impacts. That in trying to get at copyright infringement, it really is having this impact in

this specific area, on some collateral area that really is quite unrelated, or can be unrelated, to copyright infringement. Thank you.

FELTEN: I'd like to talk about the interaction between DRM and public policy, but I'm not going to come at that from the ordinary direction, saying what public policy should be about DRM. I want to talk instead about what the impact of DRM is on the public policy process related to other issues. That is, my argument will be that DRM not only is a public policy issue itself, but that it has a negative impact on the public policy debate.

Basically this stems from the fact that DRM strategies tend to take devices, whether they are computers or media players, and turn them into black boxes, black boxes that users are not supposed to, or allowed to, analyze or examine or understand. This goes under a lot of different euphemistic names. Sometimes it's called a secure execution environment, sometimes people say that the device is an appliance, although that's also a misnomer. It's not like any normal appliance you might have in your house. Sometimes it's called the robustness requirement. But all of these things really mean that the technology is supposed to be a black box, you're not supposed to be able to look inside of it. And this black box effect tends to grow over the scope of the system. For example, if you're talking about a computer system, you might say, "Well, only the part that deals with the media has to be a black box." The boundaries of that black box tend to grow because there's concern that the content will be grabbed off of the video card or the audio card, that it would be grabbed off of the disk, that it will be grabbed as it goes across the system's IO bus, and so on. The result is that the entire device tends to get turned into a black box. There's a combination of technology and law that's used to try and make these devices into black boxes. The devices are engineered in a way that armors them so that it's difficult technically to analyze or understand what's happening inside the device.

The use of a particular kind of black box design may be mandated by law—that's essentially what the tech mandates in the Hollings bill would do—and possibly, the black box nature of the systems is backed by laws like the DMCA that tend to ban analysis or tinkering or discussion related to the device. So as a result of all of this, DRM and the things that come with DRM turn technological devices into black boxes.

Now, the other side of this has to do with the interaction between technology and public policy. There are a lot of important policy questions that depend in an intimate way on understanding technology, and understanding of the technology: an important input to making reasonable public policy decisions. This is especially true right now with respect to the

things that are at stake with DRM; and so I'm going to argue that bans on understanding technology tend to cripple the public debate about these issues.

Now there are lots of examples of issues in which this is true and I want to give you three examples, but just to raise the degree of difficulty a little bit and hopefully help convince you that there are many, many examples, I'm going to use what other people have already mentioned in the conference. The first one was mentioned by Dave Farber this morning, the Total Information Awareness Program. This is obviously a public policy issue that's very much at the forefront now. I managed to get a copy of their logo off another website instead of taking it down. The logo's not too popular. I imagine the name Total Information Awareness is likely to get changed to something like Next Generation Secure Information Awareness. So here's the public policy issue with TIA. Law enforcement and intelligence communities in the United States want to mine commercial databases. They want to do it for good reasons, to catch people who would like to blow us up. But there is a significant privacy issue involved here. The advocates of TIA say that we shouldn't worry too much about abuses by rogue agents, by rogue law enforcement personnel, because methods like DRM, methods designed to prevent misuse of information or violations of policy, will prevent them. Is this true? Well, if you want to know, then you need to understand the black boxes, you need to understand the efficacy of DRM technology, whether it's going to work. You need to be able to take a skeptical look at this technology and understand how much can we count on it. And that's an important factor in any public policy decision that one might make about TIA.

My second example comes from Bob Blakley's talk this morning: the "Girls Gone Wild" video or, in particular, the attempt to block it. Another public policy issue before us has to do with blocking and filtering technology. For example, there are products out there that claim to block pornographic websites, and they claim not to block non-porn content. Is this true? Should we use this technology in schools and libraries and homes and so on? The advocates of this technology claim that we shouldn't worry about over-blocking because their blocking list, the list of sites to block, is accurate. Is that true? If we want to know whether or not it's true, we need to be able to open up their black box and see what their block list actually is. There's a lawsuit brought by Ben Edelman, a researcher at Harvard, about this very issue under the DMCA. We need to look inside that black box in order to understand the accuracy of the block list, and again, that's an important input to the public policy decision that needs to get made.

My third example is an electronic voting machine—all electronic. You walk up to it, you push some buttons on the front, and it records your vote. At the end of the election, it spits up a count of how many votes were cast for each candidate, or at least we hope it does that. So after the Florida 2000 election, there was a big push toward different voting technology, in particular computerized voting machines. Counties all over the place are looking at that. Santa Clara County, California, is in the middle of a decision process, and my own county, Mercer County, in New Jersey, is also in the throes of a decision about whether to go ahead with computerized voting, or what kind of computerized voting. You face a lot of tradeoffs there. There's no doubt that direct-recording electronic, the all electronic machines, are convenient to use and at the end of the election you get a count really fast. The big problem, though, is the risk of fraud. How do you know that the election result is right? How do you know that there hasn't been some sort of horrible mistake? Of course, this is a problem that has gone back a long time in elections, but we change it when we move to an electronic system. We change the kind of failure modes that we face. The advocates of these technologies, mostly the vendors, say, "Don't worry about tampering. We use methods to seal the devices so that outsiders can't tamper, people at the polling place can't tamper with it." They claim to use methods that prevent even their own engineers from changing what the machines do. Is that true? Do the technologies they use actually prevent tampering? How difficult is it to tamper? Is it even possible to do that? We need to understand the black boxes that they're building, and we need to understand black box technologies in general, to be able to evaluate that.

In all three of these cases, all three of the policy examples, we need to answer basic technological questions about black boxes in general, and specific black boxes, in order to make good public policy decisions. Given more time, I could go on and on and talk about other examples. There are lots of examples related to technology policy, to regulation of spectrum and examples related to defense, and so on. I'll just point out that in my view this is a serious problem. People don't understand enough about technology. Technology, God knows, is hard enough to figure out. What we don't need to do is make it harder. Thank you.

LESSIG: Excellent. So, we've been talking about DRM forever. Forever. For as long as I can remember, and that's forever for me. So forever we've been struggling with this issue of "How are we going to confront the world where not only rights existed, and were expressed strongly, but technology enabled people to enforce rights strongly?" And after struggling with this forever, I'm increasingly convinced that we've got to re-

frame this problem because a lot of bright people have tried to figure out the answer to this problem, both on their side and our side, and none of us have a good clue yet about how to solve this problem. So, re-frame the problem.

There are basically three kinds of people out there. Usually there are two, but I found out there were three. There are three kinds of people out there. There are basically people out there who believe in not controlling their stuff at all. We call them communists, you know, but there are people that say, "Take my stuff and do with it what you want." Then there are people out there who say, "Don't touch my stuff unless you ask my permission. Don't do anything with it at all unless you've got some affirmative rights from me." And then there's the rest of us in the middle who say, "Go ahead use it for lots of obvious reasons. Of course, don't make a Disney movie out of it, but for most reasons we're completely happy that you take and use my stuff." There are, therefore, the "none," none of my rights respected, and the "alls," I want all of my rights respected, and the "somes," I want some of my rights respected.

Now in the beginning, the beginning of the Internet, we had an architecture that essentially ratified the position of the "nones," the people who said, "I don't want to control my stuff at all." We had a technology that enabled basically everybody to take everything that's out there, and to share everything, and to share it in the most extraordinary efficient way, and that was great. But, that created a lot of complaints, obviously from the people who are at least in the "all" category, because their fear was that this architecture of the "nones" would increasingly shrink the space that the "alls" could adopt. Also, those out there putting stuff up in the "some" category, too, would have their rights shrunk if none of the rights that might be respected here would have been respected under the architecture of the "none."

So that was where we were, and the problem from that perspective was that there was an obvious political response: Those with all the money are also those with all the rights and those that want to assert the rights, and they would force on this world a shift in this architecture. They would try to flip the default away from a default that supported the "none" to a default that supported the "all." So in the future, increasingly, they promise us an architecture which is the DRM architecture that takes this world where there are three categories and flips it from the default where "none" control to the default where "all" is the rule—where all rights being controlled is the normal way in which we engage in interactions with each other, and the consequence of that is the exact same consequence we've seen before, but now flipped. It becomes harder and harder for the

"somes" to actually be out there, and express themselves in a way that says, "Here, take and share and use," because they must embody and adopt these highly expensive and burdensome technologies to say, "Do with my stuff as you wish so long as you respect the following rights." And also, it criminalizes the category of the "nones" out there, criminal "nones" running around, who are increasingly pushed off this space so that the default world of total control supported by total information awareness makes it possible for the "alls" to control—you got it—everything.

Now here's the problem. We've been solving for the extremes here. We've been thinking about the world as if there's either those who care not at all or those who care in the extreme; and the problem with that solution on either side is that it defeats the massive and most important category of people in the middle, who would actually like a way to express the view that you should be able to take and share the content without suffering the deep burdens of DRM. So what we need here is a way to recognize this middle. Now, there are two strategies that have been adopted to attempt to recognize this middle. The first strategy is the one we're familiar with because a lot of us have been fighting it, maybe all of us have been fighting it, on one side or the other. We've been fighting it in the courts and Congress to get them to say, "Regulate this world in a way so that the potential for the 'all' to control everything is balanced. Restrict DRM in the following ways so that we can at least have fair use or ensure that the DRM technologies that go out there don't displace the possibility of free content to be distributed."

That's a strategy. But increasingly I'm becoming convinced that that's not a strategy that is going to work in time. And that forces, I think, us to consider a second strategy, which is increasingly the one I think we ought to be spending our time on. Instead of ways to fight or limit DRM, what we need is a strategy that expresses this middle space. So I and Hal and other people in this audience are part of an organization called the Creative Commons. The Creative Commons believes that we need to distinguish between this idea, DRM, and this idea, DRE. We have to understand that there are two separate issues here, and we shouldn't be solving them together, at least not now. We ought to be finding a way for people to express, simply and easily, "Here is the set of rights that I'm happy that you respect," without building into that expression the technologies that make it so that those rights are automatically, by machines, enforced. Not because no one should be able to do that—let the "alls" do that, that's fine—but because most of the content out there is not content for which this extraordinarily strong mechanism of control is needed or valuable. The point is, for the green space in the center, these technologies of control are not

just hassles, they defeat the opportunity for this content to be shared freely in a way in which the author plainly wants. So we need a way to express digital rights without that expression forcing them necessarily. A technology to say that this is free, or at least this is sort of free, some rights reserved, not all rights reserved, and that's the role we believe Creative Commons, in its first instantiation, plays.

Creative Commons says, "We are going to build a layer of reasonable copyright law out there on top of this background of unreasonable extremism." We live in a world now governed by this unreasonable extremism, and we can do something about that by expressing a reasonable middle. This is a technology to do it, so that this background of control gets flooded by a default expression that says, "Go ahead a share in a certain way," without attempting to say to the "alls," "You shouldn't be allowed to do what you do," but instead by enabling the rest of the world to create content that is shareable freely, and can compete with those who insist on controlling all of their rights—restoring, then, in this context, reasonableness through voluntary action.

Now why is this important? Well, one story that's been told out there about why the Creative Commons project is important is that it's going to be good for the incentives of certain artists. We have artists who are out there who have begun to say, "Yeah, it's better for me to share my content in this way than to adopt the all rights reserved model." So Cory Doctorow, a hero of mine, published an extraordinary novel, *Down and Out in the Magic Kingdom*. On the same day it's in the bookstores, it's on the web under a CC license; download it, do with it as you wish. He sells an extraordinary number of books in the bookstores; he gives away a massively large number of books on the web, and what he's done, thereby, is increased the exposure of the world to Cory Doctorow's extraordinary writing, and he believes that will make it easier for him to be a successful writer in the future.

I'm all for it. It's exactly what we should be enabling: this creative use of the 'Net in a way that spreads culture broadly. But that's not the important, or most important reason, that people ought to participate in this expression of something different. The most important reason is we ought to begin to identify, to put our hands up around the world in a way that says, "I believe in free here. The default is control, but I believe in free, or I believe in somewhat free, but I believe in it now and urgently because the shift that we've seen has radically transformed the opportunity of this technology, of the Internet, to be used to develop something different, some expression in creativity innovation different from the innovation and expression controlled by that tiny little red box in the corner."

Now when this battle began, people said, "If it's either the 'nones' or the 'alls,' the 'alls' are going to win." And when you think about the places where this battle can be fought, I believed we would lose if all we had to do was fight it in the context of Congress, because the "alls" have it all and they can go to Congress, which responds to the "alls." So they were lobbying away. I was that naive person who believed that there was a place out there that we could argue this, as a matter of ideals and principles, to establish a balance here that I thought the framers of our Constitution already gave us 210 years ago. I was wrong. I was wrong. People said, "They weren't ready." I said, "Yes, they are." I was wrong. They were right.

And the consequence of them being right and me being wrong is that the courts have backed out of this battle just at the time when they could have done the most good by expressing ideals that the best interpretation of our Constitution says our framers already expressed, because our framers recognized what Hal was teaching us about, the ideals behind the Statute of Anne. When I lost and we lost, a very kind lobbyist from the other side called me and he said, "You know Larry, look, all you had was ideals and principles on your side." They had, or "We had," he said, "all the money in the world." And he said to me, "When was the last time ideals and principles won over all the money in the world." I thought, "My God, racism, we were just fighting a bunch of racists, right?" The 14th Amendment was about the ideals of the civil rights movement, it wasn't all the money in the world. Here and now, the question we ought to ask is not "When's the last time?" but "When's the next time?"—"When's the next time that ideals and principles win over all the money in the world?" And the next time it does is the time when we, all of us, begin to express in our every step, an expression that says we believe in something different, that we believe in this reasonableness, not the extremism, and we show reasonableness by building this balance in the space that marks the place we're most familiar with, this extraordinary space of potential creativity we call the Internet. We can reclaim, through voluntary efforts that say, "We believe in freedom and we show it because our content expresses it," and let them respect what we say. Thank you very much.

. . . .

QUESTIONER, SAMUELSON: So yesterday when I was doing the tutorial, Alex Alben asked me a question which, because I'm not a technologist, I was not in a very good position to try to answer, but there are several technologists on this panel who are interested in information flows. The question that was put to me was a question about whether it was possible to develop technologies that would allow circumvention for

fair use or other non-infringing purposes. Is it possible to sort of think creatively about anticircumvention laws that might allow some room for circumvention for fair uses without opening up the Pandora's box so that allowing these technologies means that you've essentially repealed the anti-circumvention laws?

ERICKSON: Yes and No. Well, I think that you can try to approximate and perhaps reach a reasonable compromise in how you write the rules that control how the systems operate. So that's one approach. Depending on how far you carry the discussions that lead to that compromise, and, I would argue, how you would include people in the loop so that it's not a completely automated thing, you might be able to do some things. I don't want to talk to the other questions about the increasing of circumvention devices to do the fair use piece, but the one particular piece that I'd like to offer up as a "maybe" or a "yes" is the creation of good policy that includes people.

FELTEN: I think this is one of the most important technical questions surrounding DRM: whether we know, whether we can figure out how to accommodate fair use and other lawful use without opening up a big loophole. The answer, I think, right now, is that we don't know how to do that. Not effectively. A lot of people would like to know whether we can do that, or how we go about doing it, but it's a big open question right now.

ABELSON: I'll give you a little piece of an idea I wouldn't necessarily advocate. This was a little system that was designed by a couple of students in a class I taught in the fall where the notion is that you did this digital rights decision based on some combination of what's carried with the work and something that's asserted by the user, partly who they are and what their intent is. So you get something that sort of gives you increased extra access to this work. On the other hand, either you have some way of saying something about yourself or some way of testing the thing that goes into some record. I don't actually think this is a workable solution, but it's the beginning of an idea.

LIU: I will say something about the legal side of things. I don't know very much about the technical question, and technologically whether this is feasible; but on the legal side, in hearing about this debate, about whether we can effectuate fair use in some sort of technical way, I sort of thought about a thought experiment of what would fair use look like if we tried to implement it in terms of a legal regulatory framework. If we actually tried to spell out, in the law, in a detailed manner, instead of the four factors, what exactly copyright and fair use would look like, I think you would soon find a statute that would begin to resemble the tax code in its complexity because it would be volumes and volumes and volumes of

very detailed regulations depending on who you are, why you're using it, which context, and all the rest. So I think, in sort of referring back to Hal's very initial picture, that first layer that's put on the public interest, I think itself is really subject to a lot of these issues. That's entirely understandable because people's interaction with information is a very complex thing, and I think that it's just really hard to specify, even from a legal standpoint.

QUESTIONER, LEMLEY: This is a question for Larry Lessig primarily. So five years ago at this conference, Bob Gomulkiewicz of Microsoft pointed out a very nice sort of inversion, which is that shrink-wrap licenses and contractual enforcement of big package software on uniform terms also turns out to be the legal basis, to the extent there is one, for the support of the open software movement. One of the interesting things that that pointed out, in a contract sense, was that in order to make a judgment about whether regulation, or freedom from regulation, was the right choice, you had to look not just at what the big guys were going to do, but what the little guys were going to do. I guess I wonder why there isn't a similar kind of dichotomy, and a similar issue that Creative Commons brings forward. It's very easy to write a set of legal rules that says everyone gets a certain set of rights. What you want to do, I take it, is to write a set of legal rules that says everyone gets a different set of rights, they can choose from among an infinite palette. But in order to implement that, it seems to me you need some kind of DRM, or if you want to call it DRE, that's fine. That requires you, though, to take a position about whether regulation of DRM by government is a good thing or a bad thing, right? And I guess what I wonder is whether a group like Creative Commons, that depends, in some sense, on the enabling features of DRM, is also going to facilitate, by allowing DRM, the problems that other people have mentioned at this conference with DRM, not limited by consumer regulation, privacy regulation, whatever else we think is problematic.

LESSIG: So the only part that I want to really resist in the structure of your question is not that it begins with the word 'so.' I did that too. It is the quickness with which you passed over the possible distinction between DRE and DRM. Because I really do think—I didn't think this originally, so I hope this is progress in my thinking—but I really do think that there is a difference between DRE and DRM. And the reason isn't the static difference because, you know, in some sense DRM includes DRE; you've got a digital rights expression language within DRM, and then DRM adds a dollop of control on top of it. That's not the difference. The difference is the dynamic effect it would have on this debate if we had a bunch of content out there that was efficiently expressing the freedom to use it in cer-

tain ways, and a bunch of people out there respecting how it can be used and how it can't be used, and a bunch of people building on that expression of freedom, versus those who continue to insist on this extraordinary overhead of technology that gets built into their content before they share their content. I think those who adopt the DRE side would be in a competitively better position against the DRM crowd in selling and making their content available. They'd be able to say, "I've got better content, not just because it's good content, but because it's freer content," right? So I want to enable that battle because I believe we're in a world where DRM is on the field. I would prefer to be in that world where DRM just wasn't getting on the field, and so if five years ago we could have found some way to keep DRM off the field, then of course we wouldn't be here fighting for Creative Commons, right? There wouldn't be a need for it. But the fact is, if DRM is on the field and is the default, and you allow them to suggest that those of us in the "some" category should just adopt the DRM technology and open up all the permissions. If you allow them to suggest that that's the same, then I think that that world of that technology of control, controlling and taking over more and more of the creative process, is inevitable. And so what I want to do is just break that down. I don't know if it works, I don't know the consequence of it.

LEMLEY: Let me just try one push. That argument makes sense to me. I guess I wonder what the impact is on regulation of DRM technology that might in other circumstances occur for purposes of consumer protection. So Julie Cohen's got a paper that makes the very nice point that DRM is necessarily at odds with strong privacy protection. Isn't DRE also necessarily at odds with strong privacy protection for the same reasons, and don't you find yourself in a position in which, if we move to a DRE world, we're less likely to be regulating privacy protection?

LESSIG: I'd be interested, but I don't think DRE technologies have the same problems that Julie articulates in the "right to anonymity" argument. I don't think it has the same problems. But the other side of this is, this is not a way of saying, "We don't have to worry about the regulations that DRM affects." We've still got to worry about them profoundly, and we've got to worry about DRM technologies restricting fair use. We've got to think creatively about how to carve that back, and so that means pursuing Pam's question and finding a technological answer and figuring out how the law shouldn't be regulated. I'm not saying that these aren't important issues anymore, but I'm saying that it's going to be easier to make those arguments if the other side of the debate is not a picture of a child with forty billion songs on his or her hard disk. It's going to be easier if you can say, "Here's something different from your model of total con-

trol and total anarchy, and one that I don't think runs into a lot of the same problems because, again, remember the DRE here is just enabling a simple way to identify so then I can make a decision about what I want to do with the content." So we want to build on top of the Google API so you can say, "Give me all the pictures of the Empire State Building available for non-commercial use." Bingo. There they are. And now that's content that I can decide to incorporate in my webpage or in my publication that competes with Microsoft's, I mean, sorry, Bill Gate's technology. To have all of this content wrapped in DRM stuff competes with it. So I think that if we had a competition between freed and controlled, freed would win in a large range of cases. Not all. But I still think that it would generally win.

FELTEN: There's an important distinction here between DRE, which gives a way to express the content creators' desires over how something will be used. I think when you talk about rigid enforcement mechanisms, then you raise significant privacy issues. If you just want to give the content creator a way of saying what permissions they grant, then the privacy issues are much easier to deal with.

QUESTIONER, EDDAN KATZ, U.C. BERKELEY: This is a question also for Professor Lessig. In the spirit of avoiding the binary, I'm afraid and troubled by the fact that I leave your talk with, imprinted in my memory, the courts and Congress crossed out in red from when you said, "We asked a question and we lost." I'm wondering if the way the question was posed was the only possible way and if you could think of another way that the question could be posed so that those two channels could further be pursued.

LESSIG: We're lawyers; we can't give up the courts, so we're going to be fighting lots of issues in the courts forever, and the Center for Internet Society at Stanford is fighting. EFF is fighting. We'll continue to fight. The fact is, we lost in the Supreme Court because the average view in the Supreme Court is just like the average view of most Americans about these issues, right? So that means we have a lot of work to do so that most Americans begin to understand how this is a more complicated issue than the binary framing of it. This is the optimism: ordinary people get it when you tell it to them and you explain it to them. They don't have a vested interest in the red "control everything" box, they don't. Ordinary people understand that when we can start thinking about digital creativity, when we can contrast the analog consumer, that's the couch potato, with the digital consumer, that's the person who's taking content, and remixing it, and releasing it in this creative way. The point is, this movement, not because of these lawsuits, but because of what thousands of people have done and lots of them here, is salient out there among ordinary people.

Now, I can shift into pessimism mood really quickly. I won't. Let's just end on the optimistic side. I think if you explain it clearly and repeatedly, over time they will get it; and when they get it, we will win. But it's going to take a lot of work. It was easier to imagine the happiness of five votes than it will be to imagine the battle that is required right now; but, you know, we have no choice. It's got to be that battle right now. I take the only solace from this loss to be the literally thousands of e-mails of people who wrote me and said, "You know, we're going to fight this until we win." That's the solace, and so let's turn that into something productive and optimistic, and I'll be happy to be proven wrong in my pessimism.

IV. DRM-RELATED LEGAL AND POLICY INITIATIVES IN THE UNITED STATES

Panel:

Pam Samuelson, Boalt Hall School of Law, University of California, Berkeley (moderator)

Fritz Attaway, Motion Picture Association of America

Jerry Berman, Center for Democracy and Technology

Ed Black, Computer & Communications Industry Association

Richard Epstein, University of Chicago Law School

Jon Healey, Los Angeles Times

Emery Simon, Business Software Alliance

Mozelle Thompson, Federal Trade Commission

SAMUELSON: This session will be different in format than the other sessions in that each person will not present a paper, but rather it will be a discussion focusing on legal and legislative policy initiatives about DRM in the U.S. So start thinking of your questions. We are going to focus on legal and policy issues related to digital rights. I think it is fair to say that in 1998, when Congress passed the DMCA, they hoped that it had resolved for the foreseeable future the problems or challenges that digital technologies would pose to copyright holders. And they were told, "Just give these few additional rights and everything will be fine." Just five years later, that seems an over-optimistic hope, if there was one. So instead of the thriving e-commerce markets that were anticipated, we have actually a wide array of content available, some of which is freely distrib-

uted, and lawfully so, and some of which is freely distributed, and not so lawfully so.

So Congress and other policy organizations such as the FCC are faced with a number of proposals. Some of those proposals, like the Hollings bill from last year, would have required standard technical measures that would have been embedded in every digital media device. The Broadcast Flag proposal that's now pending before the Federal Communications Commission would strengthen the rights of the rights holders considerably more; and so there are other bills, such as the one Representative Lofgren (D-California) just talked about, and a similar bill that Representative Boucher (D-Virginia) just has already introduced into the 108th Congress, aimed at finding a somewhat greater balance and undoing the excesses of the DMCA. Senator Wyden (D-Oregon) has recently announced that he has some interest in some consumer protection type legislation in relation to labeling DRM-protected material. So I think this Congress will be dealing with consumer protection side issues as well as the content owners' efforts to get stronger and stronger protections.

In addition, I think there have been lawsuits under the DMCA, and also there is a lawsuit brought against one of the recording companies for a defective CD because it caused harm to the computer. That lawsuit just survived a motion to dismiss. So the courts as well as the legislatures are going to be dealing with some consumer protection issues about DRM.

Five years later we know that the DMCA is not being used just to get rid of those black box piracy-enabling technologies, it's being used in a wide variety of other cases like the *Lexmark* case which Representative Lofgren mentioned, as well as the *Chamberlain v. Skylink* case which is about garage door openers. So I think in some sense the DMCA is more controversial now that it was in 1998, and there are calls for an effort to reform the DMCA to get rid of these unintended consequences.

We have with us today a great panel of experts on a wide variety of topics. At the far end of the table is Emery Simon, BSA, and next is Jon Healey, L.A. Times, then Richard Epstein, Fritz Attaway, MPAA, Ed Black, Jerry Berman, Mozelle Thompson, Commissioner of the FTC. The thing to do first is to start with a general question. It seems as though there is a lot of concern over widespread copying. Since this conference is about DRM technology, it seems like a good place to start. Will DRM technology actually solve the piracy problem, mandated or not?

SIMON: Okay, so first of all, let me tell you that I'm in support of the DMCA, and I think it's a good law, not a perfect law, it's got problems, but it's done a lot of good things , but the vilification of the statute astounds me. I work for the software industry. Software piracy costs the

software industry over $11 billion a year. It's not a hypothetical problem, it's a real problem. That piracy steals jobs, tax revenues, steals money for our innovation, The DMCA is a tool. And to see it as an incarnation of a powerful weapon of copyright holders to overreach to extinguish your rights, I think is a little fantastic, in the sense of the reality doesn't match well with that. So to answer your question, piracy is a real problem, and the DMCA is a tool that helps in that fight, and we've had some pretty good litigation to help in that fight. The courts have not had trouble interpreting it, though people may not like those interpretations .

SAMUELSON: If you'll forgive me, that wasn't actually the question I asked, you can say something about that, but the question was not whether the DMCA, but whether DRM, is a solution to the piracy problem.

SIMON: They are a tool in that fight, not a solution, and there will never be a perfect tool, but they are a very powerful and worthwhile tool, absolutely.

EPSTEIN: I think a lot of this depends upon exactly whether you think the tool in this case is sufficient for this task, or whether you think it's overbroad. Going back to the Betamax case, if you stop all contributory infringement, and you stop all use, the question is: Did the legal remedy create a partition between the things you want to stop versus things you don't? And I think the only way to succeed, at least for a part of that task, is to have fairly strong kinds of management rights. To the extent you kill the box, it's taking all kinds of non-infringing uses and subjecting them to similar kinds of restrictions that are imposed on infringing uses. But if you develop a system which in effect will allow owners to charge for digital content, much in the way you charge for telephone use by a per-play basis, then you don't have to worry about improper assignments of digital content, you don't care whether I watch it or someone else watches it. I think the whole point—you know I disagree with Congresswoman Lofgren—is that you really don't want the first-sale doctrine in this kind of a world, but you do want to have the continuous monitoring of this kind of use so that price discrimination can take place. We have to completely rethink the analog world where, if one free copy gets out and is capable of infinite reproduction, then the entire technology is capable of being lost.

ATTAWAY: Well, Emery [Simon]'s answer was the correct answer in my view. DRM is part of the solution, not the entire solution, and the problem we face is uncontrolled trafficking in illicit content over the Internet. DRM technology will help the leakage problem that allows content to get to the Internet in an unprotected form. It will provide us a means to deliver our content to consumers in a secure fashion, but there

will always be leakage. We will have to address that in a couple of ways. One is by increasing security. Second, we have to enforce our rights under the copyright laws. We have to bring actions against mass infringers. We have to use the expedited subpoena rights under the DMCA. I know you probably heard about yesterday with Sarah Deutsch, but in fact a deal was made with the ISPs in 1998, under which they received a broad safe harbor against contributory and vicarious infringement actions, in return for which they agreed to a notice and take down notice, and an expedited subpoena process. Unfortunately some ISPs are trying to renege on that, but at least one district court judge said that they couldn't. The third thing we have to do is to provide consumers with content, in a more convenient and enjoyable form than they can get through illicit methods, and we are trying to do that.

BLACK: Let me just say, first of all, I work for a great cross section of companies that have a great need for, and utilize, IP in many ways, and we are strong supporters of a strong copyright system. But we also, over the years, have understood the value of the balance of that system, and have worked to kind of make sure that we keep a system, which in all ways promotes innovation and keeps competition alive. With regard to the question of DRM, though, in a way, I think it's a little bit the wrong question because, does DRM help solve the problem? Well, the problem is not piracy. The problem is: we are in a different era now. The digital revolution has truly thrust change in innumerable ways, and it requires a rebalancing, a recalibration, a new equilibrium of all the legitimate interests. Hollywood is a legitimate interest. Consumers are a legitimate interest. Libraries, a lot of intervening players—there are a tremendous number of interests here that frankly have been thrown into turmoil because of changes in technology. And the second level changes resulting from that, and what we need to be thinking about, is not solving a piece of the problem, of which too much piracy is part of it, but we need to be rethinking how to restructure our whole information flow restrictions and access issues in a comprehensive way that is fair and is reasonable to most of the players. It's a much bigger issue, and in that context, DRM is a valuable tool and a very dangerous weapon, and it is not easy to define the discussion because there are so many variations of it that are going to be in play.

BERMAN: I'm representing a consumer organization that is very concerned about the Internet and the role of the Internet, as an open communications medium, and an open platform, but I'm just going to answer Pam's question. It is part of the solution, and there will be lots leakage, lots of leakage, but it's part of the package. No one is looking for the perfect solution, but DRM is part of the package, and it's going to be de-

ployed, and consumers and Internet organizations that care about balance within the DRM structure have to pay attention to that deployment.

HEALEY: I don't have opinions, and I'm not speaking for my organization. Just a couple of quick observations: EMusic had been referred to yesterday. They distributed content in a non-DRM format, and their business model was like the major record labels—based on distribution—and they wanted to be paid for their content. When Napster happened, EMusic still had an enforcement tool available to them. They didn't need DRM to go after Napster because essentially, they could use their hash assigned to each of their files. So on the enforcement front, DRM is a tool, but I think from history you can say it's not a necessary tool. On the question of whether EMusic's business model is successful or not, you couldn't conclude that it was successful or not based on whether they had DRM attached or whether the MP3 files are more appealing than DRM files. The question really came down to: what content did they have. That might also involve the DRM issue: because they weren't willing to use DRM, they weren't able to get certain types of content. You have to think very carefully about the relationship between DRM and the business model, because it is not necessarily a given that you have to have it in order to do things like enforcement.

SAMUELSON: The Hollings bill hasn't been reintroduced in this Congress, and it seems unlikely that it will be, but it does seem like the Broadcast Flag issue is a very similar kind of proposal, and so I think it would be good for us to talk about the Broadcast Flag. So Fritz, perhaps you could start us off by telling us why the motion picture industry is so keen on having a Broadcast Flag, and then maybe we can talk about why the BF is not such a great idea.

ATTAWAY: I have to take issue with you. It is not at all a similar proposal to the Hollings bill. It certainly has copyright implications, but at its core, it is a communications issue. Cable and satellite delivery systems, because they have a conditional access system, have the ability to protect content, including preventing content from being redistributed over the Internet. Over-the-air broadcasters do not have the ability, and the question before the FCC is: Should they give off-air broadcasters a level playing field where they can offer program suppliers some security against the redistribution over the Internet? Without that security, content providers will naturally migrate away from off-air broadcast television to cable and satellite. So the issue is maintenance of free television. We support that because free television is a major customer of ours, and we want free television to continue to exist in the marketplace. However if it doesn't, we will market our content through conditional access systems and bypass

free television. I don't think that is in the best interests of consumers, but if one wants to argue, I suppose one can.

BERMAN: I think the Broadcast Flag is certainly not the Hollings bill, and its intent is not. It is in a much narrower field. It's not a bill or a proposal, so it's one size fits all, one technology. But it's very difficult to describe how the flag is going to be deployed, and that's why we have to pay attention to whether it could take on characteristics of the Hollings bill. I think that turns on a number of things. For example, "What kind of process will be available for other technologies to get on both? Table A? Will that be an objective set of criteria? Who will make the decision, the government, or a technology board, or the market, about how you get on that table?" Because it is saying that the government is playing a regulatory role, in terms of putting an imprimatur on technologies. But you have heard the cable people say that they are going to take a standard to the FCC, and also look for a governmental blessing. There is an interesting issue of language. What the Hollings bill was considered was a mandate. When standards bodies involving industry, content and IT agree on a DRM standard which they take to the government, that becomes a standard, not a mandate. The problem has been for consumers, who have not had a clear role in the standards process. It's hard to say it's not a mandate from their point of view if their legitimate concerns have not been taken into account. I think is a serious question: getting the consumer voice into the standards. I'm not saying the Broadcast Flag is wrong, or that it can't be a part solution, but there are serious issues about how it works and whether it's an open process.

SIMON: So the technology companies I work with have been pretty vocal and vehemently opposed to the Hollings bill, and we have a coalition to work hard against it. Is the FCC going to exercise a mandate? The answer is: it's too early to tell because we don't know what the FCC is going to do. The FCC could certainly issue regulations, which would have a pervasive effect on downstream devices, in fact any device that comes into contact with content that originates in the broadcast. In the alternative, the FCC could do very little. So it is simply too early to tell, but the potential is certainly there, for it becoming the kind of mandate that has a pervasive effect that the Hollings bill was intended, or at least conceived, as having.

BLACK: I would agree with the later part of your statement there, that we don't know, but it has aspects of being a mandate. A quick reference to the Hollings bill—I think it was a terrible idea, but a wonderful piece of legislation because it helped galvanize a tremendous amount of interest on this thing. The BF is very complex, and it's hard to separate out the proc-

ess that led up to where we are right now. There are issues of participation, openness, competitiveness, that cloud the concept of a flag. The idea that you could have a flag, in an open container setting world, where you didn't have a mandate from the government a lot of people could say, "Hey, let's try it. See if it has some value." When it starts getting to be a standard chosen by a small group of players, and in the formulation we think it is likely to be involving, which gets into the future leverage over how it will be done, they will be able to change it with no outside involvement, just on their own will, a small group of companies. There are a lot of aspects of this broadcast right proposal that are terribly troubling, and if it, in any version we are seeing, is even close to coming to fruition here, and is in fact supported by the FCC, I think we would have a very bad situation.

THOMPSON: I'm from the government and I'm here to help you. (laughter) At the outset, my general counsel requires me to say that my comments here are my own and not necessarily those of the other commissioners. Listening to what I've heard so far, I hear your questions, Pam, but I'm not sure the questions you ask are the ones you really mean to ask. It's like how we view antitrust and consumer protection. There is nothing wrong with being a monopolist, it depends on how you achieve the monopoly and it depends on how you achieve market power. The same principles are applicable here because what we are talking about is standards setting, whether it's done by a self-regulatory body or whether it's done by the government. The question is: Does the standard actually appear to be overbroad, so instead of protecting innovation and incentiving innovation, it actually casts a chill on innovation, and actually thwarts the very purpose of having intellectual property rights? The question is not: DRM, yes or no? It can be a helpful tool. It's under what context it's being developed and how it's being used. The same thing for the Broadcast Flag legislation too often we hear people talking from the polar extremes. We are not talking the field of dreams: Build it and they will come. We have a lot of people out there who want access to content. What I find very interesting is that we are increasingly a demand- driven economy, where consumer confidence becomes important, but what I see is very little being done to focus on what the demand is, and what are the levers that you can use to create demand. So no one knows exactly what consumers are thinking, or they don't think in the long term. Instead you see proposals, which are kind of like eating your young. "Let's figure out how to make this work against the people we want to attract." I don't think that's a long term winning strategy for anyone.

EPSTEIN: I have a simple question, as someone who is kind of an outside expert to the area. I think the basic thing you want to achieve by this system is to make sure that marked content, which in fact is proprietary and protected, is not subject to unauthorized use. The question I have to ask is whether or not when you do this, you engage in various kinds of restraints, which blocks free entry by other parties. So protecting property rights without creating monopolies is the basic task you are trying to achieve; and until someone tells me enough about the specifics of the legislation, I don't know whether or not we are cartelizing an industry, or whether we are protecting property. Until someone answers that question, I can't tell you whether or not I'm for or against the proposal, and if you are going to try and win the public over, they are not much more educated than I am on this kind of issue, and somebody is going to have to be a little bit more specific. So I can almost answer this with, "How are you going to avoid the monopoly problem while you solve the protection problem?"

ATTAWAY: What monopoly problem do you see? (laughter) We are not in the business of creating the essential material. We make entertainment. Quite frankly, sometimes we make movies we can't subpoena people to see.

THOMPSON: You fly to Washington and tell us how important your industry is, and now you come here and play, like "Oh, we're just fluff ?"

ATTAWAY: Well, just the opposite. We are very successful in creating entertainment that a lot of people want to see. We are successful not only in this country, but around the world, in creating content that people want to see. But copyright has been described as a monopoly. It is an exclusive right to maintain control of that creative content, and that is not a bad thing, it's a good thing, because it incentivizes the creation and distribution of that content, which is what the Supreme Court just said in the *Eldred* case. That was a ringing endorsement of the monopoly of copyright. It is a good thing, it's not a bad thing.

EPSTEIN: Well, monopoly could mean one of two things: it could mean the protection of an individual work, or it could mean the cartelizing of an industry. It's the same problem as you have on the patent side. If it's just the former, I'm with you. But if it's the second, I'm against you. As far as *Eldred*, it was one of the most disgraceful decisions that ever came down, in the sense that it gave a monopoly to existing copyright holders for nothing. And when you are running a bargain, you don't want to have those retrofittings going on here. So again, I want to know something about the mechanisms, not about the aspirations. At this point, God lies in the details and the plumbing, and until I see the way the pipes are put together, I can't tell what's going on. I'm putting myself in the position of

the consumer, and from what I have learned about what this conception of what the Broadcast Flag is, and does, and how it operates, I haven't heard enough to be able make a judgment. Until I have more information, I think everyone will be extremely skittish and skeptical of what should be done.

BERMAN: Well, let's explore a little bit. A lot of the comments on the Broadcast Flag were for it, and then a lot said it's ineffective. I don't think that is responsive. Who controls and makes decisions about the technologies that would create a market of technologies that would recognize and permit over time a range of other uses and permissions that are not a copying of millions of copies over the Internet? For example, the technology and encoding rules that would allow the Internet to be part of the home entertainment network—right now, as I read it, Fritz, the rule would say that three studios would have to agree that the technology is robust and compliant. Isn't that a little close to giving the power over the technologies to the incumbents?

ATTAWAY: Jerry [Berman], unfortunately you engage in selective reading. You are right, that is one of the criteria, but it is one of four. There are other criteria, as well. One of which is technology that is equally effective as what is already on Table A, and I would say that is a very objective criteria, one that the FCC can easily measure. It is open to absolutely any new innovative technology, so long as it is equally effective; and I would also like to point out some of the irresponsible rhetoric you have no doubt heard. The Broadcast Flag only does one thing: it only prevents the redistribution of digital content over broad digital networks. It has no effect on copying whatsoever. You can make all the copies you want to. You can do anything you want to with those copies. You can make copies of copies. It does not affect copying.

HEALEY: Could I jump in on that? One of the impacts though, correct me if I'm wrong, is that in today's digital networking technologies, there is no way to have Ethernet in play. Basically, the digital connection would have to be encrypted, so if I have Ethernet set up in my home, and I want to move video—broadcast digital video—around that network, which I imagine people are going to want to do someday, I couldn't do it with Ethernet. I'd have to come up with a different technology.

ATTAWAY: Using today's technology, yes, you are correct, but I think that will change very quickly. I think there will be secure methods of moving content on Ethernets, and even over the Internet by e-mail. It's just a matter of developing the technology to do that, and we have no problem with that. Our only problem is the mass redistribution of content to tens of millions of people over the Internet, which destroys the aftermarket for television programs.

BERMAN: Fritz [Attaway], with copying, let me ask you this. We've been having a dialog with CET, and Consumer's Union, with a range of companies and across sectors, but we get different answers to different questions , and I'm not foreclosing that the Broadcast Flag is wrong, but take this example, and I get different answers: Pam Samuelson appears on Nightline to talk about copyright within the flag structure. I want to take a snippet, and put it on a compliant computer, and I want send it to someone downstream. Not the whole Nightline, and maybe it shouldn't even be flagged, but I want to send that snippet to her office. Can I do it under the Flag proposal?

ATTAWAY: Yes, if the technology exists for you to do that securely.

THOMPSON: Maybe this highlights a bit of the problem, because the question is, "When does a grant of any sort of intellectual property rights happen?", which I do think is a monopoly, and a legal monopoly. When it bleeds over into non-infringing uses, that's when you have an innovation problem and a competition problem that gives me great pause, because then consumers don't even know what they are not getting, they don't know what they are not seeing, they don't know whether they could have gotten something cheaper either. So the question is whether you use a blunt instrument to get to a pinprick problem. Now I'm not going to say that there is a de minimus problem here, but what I am saying is, it gives me a bit of hesitation. This is an area where I have not formed judgments, but the answer is not 0 and the answer is not 100. It's somewhere in between, and it has to have some flexibility. And I'm worried about when you wind up creating standards that at the outset wind up appearing to be overbroad.

ATTAWAY: I agree with you. The tools are often more blunt than you would like them to be; but let me give you an illustration of a balancing test. The DVD. It is true that certain possible uses of the fair uses are not possible because of the Content Scramble System. However, the Content Scramble System was essential to induce movie owners to release their product in that environment. The DVD has become the most popular consumer electronics device in history. Millions of consumers are enjoying movies, in a way that they never had an opportunity to do so before. So you weigh what consumer benefit was produced by the DVD, against what consumer negative impact there was, which I submit to you is de minimus, and consumers are a whole lot better off today than ten years ago when the only home video source was VHS.

THOMPSON: Let me point out some issues. It strikes me, that the potential chilling effect, as mentioned by Congresswoman [Lofgren], if you wind up selling product that could potentially harm machines people have,

and you fail to disclose it, that's problematic. So I can't think of that as being a good thing. But I'm going to take a step back even further. Two years ago, when I was looking at the merger of AOL/Time Warner, and we were looking at Time Warner owning monopoly cable power over 22 large markets in the U.S., the movie industry and others asked for us to put some strong conditions, so that the people providing the pipe weren't able to have a chilling effect over innovation by jiggering with standards for sets with set top boxes, so that there could be a variety of ways that content producers could get into your house. Now, how am I supposed to respond, when those very same producers come back and say, "Yes, so long as it's done our way"?

EPSTEIN: Ignorance is bliss, I think, on many of these panels. As best I can tell, the objection against the Broadcast Flag seems to be at this particular point that it will stop fragmented use that would normally be protected under the fair use doctrine. I haven't heard any kind of other monopoly arguments, and if that's where it sits, then I guess I'm with Fritz [Attaway], although, two seconds ago, I was against him. The problem with fragmentation is, I think, much more serious. You get ten people who want fragments, and they each take ten minute fragments, and then somebody could reassemble the movie on the outside, and the difficulty that you have to remember is that he is working in a precise environment, and if he loses one pristine copy of a DVD to an unauthorized network, then he's lost a billion copies to it, and so when you start saying there is just a small breach in the wall, this is an industry in which everything cascades instantly. It seems to me that if a Flag can do what he says, and does nothing more, and I don't believe this yet, because I don't know enough about the technical stuff, but if that's the representation, you don't have the problems that you have with the Hollings situation, where you are mucking up computer hardware, which compromises the use of all sorts of non-protected software. What is needed is a remedy that is software specific and content specific, rather than machine general. Therefore in effect, that should be the path we go down, and we should be pleased that at least in the first instance, we've got Hollings off the table. Now you can tinker with this thing, but it's a question of doing it all in his way, or doing it none, because if the fair use leakage becomes essentially a complete stream, then I would rather give up that little bit of consumer right in order to keep the instruments working.

BLACK: Let me try one more on this. The problem is not the technology of the Flag being inserted, or companies trying to say, "Here's what we think should be done." It is that there is a specific solution, investing huge power in a small group of companies. We see ways in which it can

have an impact steering technology, choking off viable alternative options for technology, in spite of Fritz [Attaway]'s saying "Well, there can be similar functionality." Yeah, we can end up in litigation for lots of years. In the interim, you will be in a situation where lots of people will be chilled from going in those alternative directions.

SAMUELSON: As I understand it, part of the concern is that the Broadcast Flag doesn't just constitute a regulation of TV tuners. It will also affect modulators and demodulators, and downstream devices, and to the extent that motion picture companies have the power to say "yea" or "nay" to the development of these technologies, that, I think, is the concern.

ATTAWAY: There is no proposal on the table that gives us that power. I don't know what the source of that statement is.

SAMUELSON: Well, Emery [Simon] is actually in disagreement with you.

SIMON: That's not very accurate, Fritz [Attaway], because the motion picture industry has identified universal problems of piracy, of which the Broadcast Flag addresses one, and that's free over-the-air digital transmissions. But there are lots of other sources of leakages, and the model that is, or is not, put into regulation, undoubtedly will create precedence for how subsequent piracy problems will be resolved. Moreover, we know that five years ago, p-to-p piracy was not something we were aware of, and today it's a huge issue, not only for the movie industry, but for the software industry as well. I can assert with full confidence that in five years it will be in yet another form. The piracy problem that studios confront, software companies confront, the film companies confront, all copyright holders confront, will be a constantly evolving and changing one. The fear of the Broadcast Flag approach is that it sets into motion a regulatory interventionist model, which will then become a model that will have a certain gravitas, a certain center of gravity, proceeding thereafter with these issues. And if you think technology drives your products, and you think technology is good for your industry—and we appear to—by solving the problems with certain bad ways, we end up chilling technology and by that you'll be hurting yourselves in that as well.

ATTAWAY: So your position is that we should not solve a problem that you readily admit exists, because the solution, although itself is benign, could possibly maybe someday in the future perhaps be a precedent for something you don't like? What kind of a position is that?

EPSTEIN: That's not my position.

SIMON: That's not mine either. (laughing)

EPSTEIN: I'll tell you, it's not mine, and maybe that means something a little different to Fritz [Attaway], but what I've heard is a delegation to a private body to set standards which would act as an exclusive barrier to entry to new technologies. That's what I hear. The question one has to ask is: As you hear it, is it true? And I would like someone to tell me whether or not there is a scenario in which, if we give this man and his friends a part control over the lever, he can stop a new form of technology from emerging. I want to know that. I also want to know why it would be in his interest to do such a thing. I don't quite hear the answers. I hear the fears. I don't hear that they are as ominous as Fritz [Attaway] makes them out to be. On the other hand they are not as specific as I would want them to be before I would be prepared to say this technology has too many interests to go forward.

SIMON: Your example is, the premiere example is, the technology that was developed to protect DVDs before CSS came along, which was a technology worked out by the motion picture industry and the consumer electronics industry, and which they legislated. There was a big long bill and a big long standards document that went along with it, and it was a mandate. When the computer and software industry looked at that technology, we came to the conclusion that it would make so many calls on CPUs, so constantly, that performance would be degraded dramatically. So there is an example of a way that you can come up with bad solutions. The way that CSS came about, and the DVD solution came about, was to abandon that approach where a whole bunch of engineers sit down and do the standards process, which is what they do all the time, figure out standards; and when they figured out a standard that worked, people kind of made it into what eventually became CSS. So yes, you can have bad solutions that have substantial negative impacts.

SAMUELSON: Jon [Healey], I wonder if you would say a few words about how you try to, as a reporter, cover stories about things like Broadcast Flags, which involve so many complex technologies and people who have so many different views about what the proposals are about.

HEALEY: Well, I try to understand it as a user would understand it, which means getting past the engineering details as fast as I can, with as little insight as I can bring to bear, because a lot of these things are process debates. My average reader doesn't care about the process, they care about the results. That's not to say the process isn't important. So, the first thing to do is figure out what the problem is that people want to solve, which in the Broadcast Flag instance, was all about Internet redistribution. This is a problem for us, but wasn't much of a problem until Napster pointed it out for the music industry, and sort of by assumption or extrapolation, the

video industry figured it would come to them as well. So after that, you have to look at what technologies might be out there to solve the problem. In this case of the Broadcast Flag, the standard setting body for the TV industry, the ATSC (Advanced Television Systems Committee), had already identified a set of bits that could be used to act as a trigger, right? So then it became a policy question. That's the hardest part of my job: seeing all the ramifications of the different policies, which also means understanding in a better way what the problem is. Because everyone is concerned, I think, in the Broadcast Flag debate, not about solving the problem. There is an agreement that unauthorized Internet redistribution is an issue for the video guys that needs to be addressed. What they are concerned about is that if you take steps A, B, and C, then what happens? It's almost a test of your imagination, because we don't know what's going to happen.

BERMAN: One last comment. I really think that we have to explore how this Flag or any of these standards are going to work and we have to get inside the game and inside the process, and unless people can ask questions, and not have their positions construed one way or the other.

SAMUELSON: So an alternative to the FCC or Congress doing mandates through legislation or regulation, is the private standards setting process, and I want to come back to a question Jerry [Berman] posed a little bit ago about the public interest and standard setting organizations in context, because very often the people who engage in these standard setting organizations tend to be big players with stakes. The question is: Is there a way for those processes to be open to public interest representation?

SIMON: Well, first of all, I have been involved in these standard setting bodies. The answer is that they are open, so any public interest group can show up, but what you are identifying is actually a tension in a hard question, which is how a public interest group may engage in an exercise that is expensive and time consuming and requires specific engineering skills and know-how. It's a hard thing to do. So if you are going have to a voluntary industry and private sector led standards setting body, for public interest groups to participate in, that is a tough thing. The alternative is to do it in a public interest forum, like Congress or the FCC, which then generates the alternative problem of legislation or regulation. So there is a tension between those things. For my money, it's still better to try to do this through voluntary efforts, and include whoever wants to show up at these meetings and speak their minds.

BERMAN: I really believe that my organization has fought against government mandates from the DEA and from export controls, and we

want to avoid as much regulation of the Internet as possible, yet the irony is that the only place where we have a voice right now is at the FCC, which is trying to regulate Broadcast Flags. Emery [Simon] raises a very serious question: if we want to participate in it, it's open, but it takes money, resources, and so forth. That barrier has to be crossed, because otherwise there is no chair at the table. But what is the other side? Let's say we can cross that Rubicon. There is a second point for consumer organizations: if you get into the process, you got to be in good faith, attempting to work on the standards, and trying to make it work; and there are a lot of people in this audience, who believe that if you get into the details, whether snippets for fair use, or anything else I can think of that you are on a slippery slope, and you are therefore going to end up endorsing the process. So if it's a zero sum game, consumers will not, they can't participate. If they are going to participate, they are going to have to get into the weeds.

ATTAWAY: Jerry [Berman], there is another safeguard that you are not addressing. Emery [Simon] is right, these standard bodies are open, but Jerry [Berman], I agree with you, sometimes it is inconvenient or even impossible for consumer groups to participate. But there is a very effective safeguard for consumers in place. It's called the marketplace. If standards are set that are unacceptable to consumers, they will be rejected; and they are, frequently. You see it every day. Technology is put out into the marketplace, consumers don't like it and it dies.

EPSTEIN: We are not worried about that. We are worried about the stuff that doesn't get out into the marketplace. The problem is I don't know who fills this chair where the public is supposed to sit? It seems to me you have large numbers of individuals, and there is an aggregation problem, and the traditional methodological individualist, as I am, says the only way you get to social utility is to sum individual utilities, such that the public is only coalitions and groups and so forth. And so hearing that there is some sort of mythical override leads me to fear again that there will be some sort of saving dictator who will be able to protect us all from ourselves, which will lead to our own ruination. The time to figure out how to work this process is going to be very, very difficult, given that constraint. I want to know whether you are strengthening markets or strengthening monopolies. There is a long history in the law, in every area from imports on down, where safety regulations are used, in my view improperly, to protect yourself from monopoly. I don't know whether that is happening here, and until someone answers that question, I don't know where to cast my ballot.

SIMON: Let me confuse things with the facts. So you say, where is the evidence that the marketplace will respond? The software industry has used DRMs for twenty-five years. It goes through a cycle. The software industry tightens up the DRMs and consumers scream, because they can't do very much with the software when it fails, or they want to reload it. Companies loosen up on the DRM, and the piracy goes way up, and then they tighten up on it. That has been the cycle, and that continues to be the cycle, and we're reconciled to that cycle. What we do in that cycle is we abandon technologies that consumers hated the worst. I'll give you an example. There is something called a dongle, a little piece of hardware that people attach to the back of the PC with which the PC has to shake hands in order to run the software. People hated it. Nobody uses a dongle anymore. So yes, there are DRMs that are hated by the marketplace, and are taken out of the marketplace in response to the market.

BLACK: To answer the question about standard-setting processes. First of all, there are thousands of standards created all the time. If the standard setting body tends to be dominated by a few very large players, the temptation to use the standard not to create an open standard, but to create a competitive disadvantage for potential competitors, looms large. I think with the Broadcast Flag we see this, I see that as part of the problem. But in general, I would love to see consumer interests able to be more vigorously represented more often. To the extent if we have a highly competitive group of players in the standards setting process, there is a certain amount of capability of the marketplace for the consumer voice to be somewhat heard, but when you have a smaller subset, when you have big players, that's when you have the potential for this.

HEALEY: Who should decide which programs can carry a flag? One might argue that the best place for those policy decisions isn't, to borrow the phrase from the Microsoft presentation a couple of days ago, "Isn't with the technologists, it's with the policymakers."

. . . .

THOMPSON: This is where I'm here to help you. (laughter) It is important to have, and this is something I've talked about that's involved technology issues, which may make this particular area a little different than some of the others that the government works in, that no one group has the answer. So it's important to have a diversity of views, and it's important to recognize that those views may not be fixed in stone, and they can change over time. Now, the marketplace is a great force but sometimes that market is not perfect. Otherwise, you wouldn't have people like us who are involved in antitrust issues, or consumer protection issues; and we are not regulators, we are law enforcers, which means that the market

works most of the time, but every once in a while you have to kick it in the butt, because there are some course corrections that are necessary. That gets us to standard setting. We have a presumption that standard setting organizations are good, to the extent that they can bring rationality to a given marketplace, and provide some efficiencies, so consumers benefit. The question is: Are there circumstances under which standards setting organizations become corrupted, by not full participation ?

I would also say that I would not be so quick to characterize public forums that are sponsored by government as simply those that wind up legislating or rule making. We at the FTC are having a workshop on spam in a few weeks. We had one on privacy technology. We had one on B2B marketplaces, where we take no action, and we took the step of saying we were taking no action, because we wanted to see it develop. So I think that we can actually form a place where we can talk very candidly, and perhaps get a little less positional, and perhaps more in the problem-solving mode.

BERMAN: That would be very, very helpful. In other Internet areas , the ball has been driven forward by the government providing a forum for getting people together. I think that would be a terrific role for the FTC, not a regulatory role, but just a convening role, a place to go. I understand, the consumer is a check, but there are certain things where the consumer is not dispositive, and the most important is in areas of free speech and privacy. Those are rights, which may conflict with majority opinion. The majority may love getting Harry Potter, but they may not care if all news and public affairs are flagged, and not available. I think that those issues have to be addressed, because if we are going to be in a closed system, and rely on future technologies, should some content be unflagged? On First Amendment rights alone, I think there is a serious issue about whether public affairs should be flagged.

ATTAWAY: Jerry [Berman], you once again mention the First Amendment and free speech, despite the fact that court after court after court has said that free speech does not mean you have the right to take someone else's speech and use it. The First Amendment has nothing to do with what we are talking about here.

SAMUELSON: I've read those cases and that actually isn't what they said. (laughter)

THOMPSON: This gets to the instance of the overbreadth that I've been talking about, in the sense that I've heard the same thing when we are talking about what constitutes commercial speech as well. So when the business community tells me that they can use information for whatever purpose, that's not true either. So it's important to try to get to the middle of what's reasonable. I always like people who cite the First Amendment

on the one hand and then on the other hand, at the same time say that's reserved for lawyers.

SAMUELSON: So I think it's time to go to a controversial subject, perhaps some discussion about the anticircumvention regulations, since Congresswoman Lofgren was here talking to us in part about that. As was mentioned yesterday, a preliminary injunction has been issued in the *Lexmark* case against Static Control's continued ability to sell their toner cartridges. That case, and the *Chamberlain* case and the universal garage door opener, are DMCA claims that I think are unintended consequences. The question of whether there might need to be some tweaking of the anticircumvention rules to exclude these kinds of cases from the scope seems like it might be worth talking about.

BERMAN: I think that there are several areas where the Congresswoman agrees that there needs to be tweaking, and we could maybe agree on some of the tweakings, but here is where I have to make two points. Unless consumers are really organized with the technology community, and get into the game, Representatives Lofgren and Boucher are flying alone, and they are not going to be able to tweak the DMCA. There are serious interests who don't want to open up the DMCA for very good reasons. It protects their software, it protects their content, and they are not interested in opening that to the political realm. Even if they agree that changes need to be made, they are not willing to take the risk. That has to be created by others, who want to make those changes, organizing, coming in and trying, and delivering political power, not market power, to put those issues on the table. I don't think we are anywhere near it; and when Larry Lessig says in the face of the Flag, the DTV bill, the need to wrestle with fair use, a standards body, and draw an X through Congress, and says, "Let's go somewhere else now because we lost the *Eldred* case"—I think that is a fundamentally wrong message. If you want to affect these policies, you have to organize, and you have to be in Congress, and they have got to hear your voices, because the reality is, the content people are well known, they have a lot of power, and they have a very good case. They are very worried, in particular the movie industry. They don't want what happened to the record industry to happen to them. They have an enormous amount of power, and I think they have a very good case, but the balancing of that case requires a lot of work by consumers, and the consumers, including us, are not sufficiently there.

EPSTEIN: I am a little bit mystified. What happens is you build up a huge head of steam, and you may take care of the garage door opener case, which does or does not matter, or these compatible systems, but any legislation you are going to enact will have massive movements in the opposite

direction. If this is the extent to which we have a problem, my own strong inclination is that I will listen to any side in the face of judicial format to see whether or not there is an implied exception, to see if the cases get reversed, but I don't think two swallows make a summer. There are billions upon billions of interests on the other side, and the moment you start to create a crack in the other side, you make a crack in the edifice of protection, and the whole wall comes crumbing down. The discontinuous nature of this business is something that leads one to think that they are attractive in principle, in an abstract way, but terribly dangerous when you are trying to implement them, because there is no way you could break the flow. The slope is simply too steep.

ATTAWAY: I don't want to sully Jerry [Berman]'s reputation, but I'm going to agree with him. Do you mind? (laughter). The bill that was introduced by Congressman Boucher is not tweaking the DMCA. It repeals the DMCA. The essence of the DMCA, at least for us in the motion picture industry, is the prohibition against trafficking in circumvention devices. We realize we cannot station a policeman in the home of every consumer to see if they are circumventing any particular technological measure. What we have to do is prevent the mainstream commercial availability of circumvention devices and that's what the DMCA gives us. Congressman Boucher has introduced a bill that says any device that is capable of allowing fair use is not a circumvention device. It totally repeals the essence of the DMCA. Burglar tools have legitimate uses. You can legally break into your own home, but if burglar tools were allowed in mainstream commerce, the predominant use of those tools would be to burglarize people's homes. The same thing applies with circumvention devices. So Congressman Boucher presented this view in 1998, and it was soundly rejected. He's presenting it again today, and I predict it will be equally soundly rejected.

BLACK: Let me talk a little bit about the history of the DMCA. First, we went back to WIPO, and White Papers before then, and there were many years of discussions by a lot of players, on how to structure this world. There were a number of people in opposition to certain proposals that wound up becoming the law, and believe me, I think the law was modified to a much more balanced position than it started out in some of the early drafts. But circumvention was used, because a decision was made in the process. Either you say fundamentally that everything is to be banned, and you make exceptions for some uses, or you do the reverse, and you say we won't ban stuff per se, but we will itemize and list all those improper burglar tools that can be identified, and create a rapid way to identify them. So it was really which side of the presumption and where

the exceptions were. Many of us argued that in a rapid and changing technological era, that it was really wrong to say that there was a blanket prohibition on devices, when we knew what was going to be out there, that anticircumvention tools that might inadvertently be structured in such a way, that totally innocent products could have an effect of looking like a circumvention tool. So facing that unknown world, none of us wanted that to be. We were going to be very liberal in identifying something that was going to be misused, we'll deal with it, we'll list it, but in fact, we had the opposite effect, and we basically are living this now. Even now with the exceptions, which are modest, were fought tooth and nail for. Research, and no one even thought of encryption research as an exception two months before the bill was passed, surfaced and it was fought for tooth and nail. I am in agreement with Emery [Simon]. There was no broad understanding in Congress with what they were doing. These were nitty gritty little debates that were fought out in the trenches, and the impact, we think, is as we predicted: Far-reaching consequences of people coming to use the anticircumvention provisions for anti-competitive uses, not for intellectual property protections purposes, and that's the danger.

. . . .

THOMPSON: I think that what was raised earlier about what kind of public voice there is, I won't diminish the value of that public voice. I mean sure, there is a lot of money, there are a lot of interests out there, but that's not to say that the interests of consumers or end users are not important, or to the extent that they are organized, that they may not be able to get at the legislative bits. But they sure can inform the legislature about what is going on, and they surely have a role in informing people like us, when people who legislate ask us what our opinions are. So knowing what happens out there on the ground, including what the side effects are, is important. For example, a lot of people don't know, and they should know, that one of the principle tools in antitrust are squealers, people who are competitors and who see things that are going on that we might not be able to see. Then we get a chance to sit down and think about what the impact is. I don't want to preach those issues, but that's why I would have some reservations about talking about what the scope of legislation might be, or what a fix might be because none of us have a total picture.

SIMON: Let me try to answer your question, which is about *Lexmark*. Whether it was an unintended situation under the DMCA or an unanticipated one, I don't know. What the DMCA is focused on is the piracy issues, and so it was not based on relationships between companies, competitors and the marketplace. So it was certainly an unanticipated situation. Whether the DMCA should be used in that way or not, I personally think

it should not, but whether it will or not, the courts will decide; and ultimately, if the courts decide this thing erroneously, there will be a role for coming back and looking at this thing again. On the things that Zoe Lofgren talked about this morning, I think one of the most revealing things was a question that was asked yesterday afternoon to a group of technologists: "Do you know, as a matter of technology, how to create a set of technologies that will permit fair uses without letting everything out of the bag?" The answer from three of that panel was no. I'm not diminishing the importance of fair use or private use or individual interests or anything, but if you don't know how to fix that problem with technology, if you fix it as a matter of law, what you have done is you have eviscerated the very purpose of the statute; and that seems to me a little bit of overkill.

EPSTEIN: This is a completely discontinuous problem. To think that what you would want to do in order to preserve fair use is to decimate an entire industry, or two industries as the case may be, strikes me as being an extremely odd kind of conclusion to reach. I don't see where the intermediate fix is, because once one pristine copy gets out, then there are a billion pristine copies that are out there, and one has to realize that there is this precipice, which I think determines the shape of the entire debate.

BLACK: The premise is industries are going to be destroyed. We've heard that over and over and over and over.

. . . .

EPSTEIN: It's not that the technology constrains the set of intermediate choices we have today. This is not fair use in the traditional sense of literary criticism that you need to make with somebody else's work. This is fair use in the sense of reproduction for private uses, and unless someone can explain how you can make one copy without making ten billion copies, then the issue becomes a very serious one. Is it Armageddon?

BERMAN: Richard [Epstein], there are ways to do that. You have not asked for explanations. You have just said it's not possible, therefore let's not explore it. But what Mozelle [Thompson] said is that whether it's the DMCA, or what can be done about fair use, the only way to get out of extreme characterizations—either legislative proposals—is to sit down and talk about the facts and how the technology works. You've made some assumptions about the technologies that are not true. You need to know that it would take 17 hours to put Harry Potter together. So those facts need to be discussed. The forum is missing. It is totally adversarial. One of the problems with Congress is that while they are holding hearings, the level of knowledge about the Internet—you can count on your hands the number of Congressmen who know that it is not similar to a television set—that is a serious problem because they will legislate. So creating

those forums, creating ways to bring the industry, the technologists and the consumers together, is absolutely critical to get out of this kind of problem we are having.

SIMON: Let's look at the fair use concept, and the fair use concept is a public interest, public policy balancing statute, which essentially says that if you are going to do something socially redeeming, like research or like education or like something socially redeeming, we'll excuse the fact that you've made unauthorized copies, and that's a good thing. So now we look at the overall context that the anti-circumvention rules appear in, and you do a balancing test again. On the one hand, you balance the potential threat, it's not an absolute threat, and probably Richard [Epstein] overstated it, but it is a serious potential threat. You balance against that the public interest that is inherent in the balancing of fair use, and you come up with an answer. The problem is that it is not going to be the same answer in every situation. I believe that the DMCA, for the moment, has gotten it about right, and I believe that doing what Zoe [Lofgren] and Rick [Boucher] and others propose would be a mistake. It's too early to make those decisions. Let's let it play out a little bit longer. Let's have some proof of the fact that there is really a lot of harm going on here, because frankly I haven't seen all that much.

BERMAN: I agree, I'm all for the documentation. Let's document and talk about the facts within a forum. And fair use is a balancing task, but within the constraints of DRM technology, where the possibility of exercising it, and then defending it in traditional fair use terms, may not be possible, so that you are on the end of asking permission for taking a snippet , that is a fundamental change in the way fair use works. If that's true, then you have to find a way, a forum, of how to rebalance those things, because there is no way to do the balance, if you turn it on its head and make it a permission.

HEALEY: Aren't we presupposing that the universe gets DRM? I mean, if there are non-DRM sources of content in the marketplace, and the public doesn't like the DRM sources, then you would think the non-DRM sources would win, and that would provide your outlet for fair uses and other uses that DRM content would not provide.

SAMUELSON: I think that is one of the things Larry Lessig was trying to envision with his Creative Commons initiative. I actually want to open it up to questions from the floor. Don?

QUESTIONER, DON WHITESIDE, INTEL: You might think of CSS as an imperfect solution that had great benefit for content providers and consumers six years ago. We are now at a point where we can actually expand CSS to enable portability. I am curious when we will see an update

to the CSS license to allow protected outputs to DRMs that exist and other protected environments very similar to what the cable industry just announced ?

ATTAWAY: Don [Whiteside], I wish could answer the question but those are decisions that are way above my pay grade. I agree with you that they need to be made. I am not involved in the negotiations aimed at reaching the resolution, but I hope that a resolution comes quickly.

. . . .

QUESTIONER, MARK LEMLEY, BOALT HALL: So, the consensus, to the extent that there is any consensus on this panel, seems to be, the Hollings bill is a bad idea. Why is it a bad idea? Because it mandates the way we build technology, and the market is generally the preferable solution. My question is this: Why then is the Broadcast Flag at the FCC? I would expect a market-based solution to be one in which device manufacturers, perhaps at a standards setting organization, but not uniformly, compete to make devices that do, or do not, encode something, right? And if they are in fact concerned by what Fritz said at the beginning, which is that we will not send content for free, unless these devices exist, I would expect the market to develop such a process on its own. The fact that we are not at the market, that we are instead asking the FCC, I take it, to mandate something along these lines, suggests to me that what's going on is not any kind of market driven, or even standards setting process in the classical sense, but instead regulation. Maybe there is a good reason for that, but if there is a good reason for that, then maybe we have to decide what that is. But we have to abandon this pretense that we are in fact doing anything different, and we have to come out and say that we are regulating technology, and this is why it's a good thing.

SIMON: Well, it is in fact a good thing; and the reason is that the marketplace way to solve this problem is for broadcasters to encrypt their signals and operate the same way that cable and satellite delivery systems do, where the broadcaster can control the types of devices that process their signals, and require those devices not to pass that content onto the Internet. However, the policy implications of doing that are rather extreme. It would immediately render useless every consumer digital television device that has been sold in the marketplace.

. . . .

LEMLEY: We don't want to do that because it would prevent a bunch of devices from being useful, but perhaps what is happening is that the market is solving the problem in a different way, right?

. . . .

I think you can make an argument for regulation, but I think you have to make an argument for it as regulation. You've got to abandon this pretense that Broadcast Flag is a market-based solution to anything. You've got to say, "we need regulation to solve this problem, government please help us."

SIMON: I'm sorry if I gave the impression that we don't think it's regulation. It is regulation, absolutely, of course it is.

EPSTEIN: But Mark [Lemley], I think the difference between this and Hollings is that in one case you are trying to control the show, and in another case you are trying to run the box. Therefore, the level of interference under Hollings is at least presumptively higher than it is under Broadcast Flag, and what one has to do is to go into the details to see whether or not that statement is true or false.

. . . .

QUESTIONER, LUCKY GREEN, CYPHERPUNKS.TO: I do have a question about the Broadcast Flag, and its potential anticompetitive consequences, not in the content space, but in the HDTV receiver space, and this question is really going to the FTC. There are currently HDTV receivers that are quite expensive. It's one of the many reasons why high quality television broadcast is not being received by many in the American television population. There are currently projects underway at present, software-defined related projects, that permit the receiver to get HD reception, and it is a fraction of the cost of any computer-based solution currently on which the market is based. Needless to say, this is all done with software, and since the software is all being given away in source code form, downloaded from the Internet, the robustness requirements that necessarily would accompany the Broadcast Flag cannot possibly be met. Hence a considerably less expensive technology would be of obvious consumer benefit, would be kept off the market, if a Broadcast Flag were to be implemented. So I'm wondering: Is this truly in the best interests of the MPAA, for HDTV receivers to be four or five times more expensive than they could be, and what does the FTC have to say about that?

ATTAWAY: HDTV receivers are going to have to be able to process protected content. That's totally separate and apart from the Broadcast Flag issue. People are not going to invest in an HD receiver only to watch over-the-air broadcasting. They are going to want to watch cable, they are going to want to watch satellite, going to want to watch DVDs, they are going to want to watch premium content that is protected. All the Broadcast Flag would do is to say that off-air content has to be routed through a protected interface that is going to be there anyway because it needs to be there to render all of this other content that will be protected; and consum-

ers will not be able to watch, unless they have a device that can handle this kind of content. So there is no additional cost. The protection has to be there anyway to receive the other kinds of content.

HEALEY: What about the professor's remark? Can you make, using software, an HDTV receiver that meets the robustness requirements of the Broadcast Flag?

ATTAWAY: I'm afraid I went to law school, not engineering school.

SIMON: Let me try to answer that, because I was involved in that process. So the answer is: we haven't agreed on what robustness rules should be. There is a proposal in front of the FCC, but that doesn't mean there is consensus on what the robustness rules will be. If we were to agree on what those robustness rules are, then our experience in the past has been that yes, we can deploy that software. I just want to come back to one important point raised. The right way to protect Broadcast is to encrypt it. The reason why the music industry has a huge piracy problem is because their product is out there in the clear. The reason why DVDs will go with CSS: it's not in the clear. When you put out free over-the-air broadcast in the clear, you are asking for trouble.

. . . .

SIMON: Do you know what percent of the American public who gets their television that way? Less than 20%.

EPSTEIN: Well, then you are telling me something which I kind of guessed, because I have cable and a dish at my house. I get anything I can get over-the-air, with those two things. So what we really have to do is to junk that technology, put everything through encryption. Once you encrypt it then you can monitor it, once you can monitor it; then you don't care about the assignment problem, and then we can all go home, including the FTC.

THOMPSON: With all due respect, a lot of people like me are among those 20%.

EPSTEIN: It's like Life Magazine, where it turns out that there was a time when picture magazines were great, but then television came along and they could never quite recover their market share. And what will happen is, if in fact we adopt the technology, you as a private citizen will adapt more rapidly than you as an FTC regulator.

SAMUELSON: I think this is an extraordinary moment to close. Thank you very much.

V. ANTICIRCUMVENTION REGULATIONS IN THE UNITED STATES AND ELSEWHERE

Panel:

Mark Lemley, Boalt Hall School of Law, University of California, Berkeley (moderator)

Tony Reese, University of Texas Law School

Graeme Dinwoodie, Chicago Kent Law School

Bernt Hugenholtz, University of Amsterdam, Information Law Institute

LEMLEY: Our final panel of the day continues what appears to be today's theme, of anticircumvention regulations and their relationship to Digital Rights Management. However, we are doing something shocking and novel for a conference based in the United States, which is that we will broaden the focus beyond the United States and actually talk about regulations and potential regulations in other countries. To lead us off, Professor Tony Reese of the University of Texas School of Law—and special counsel to the law firm of Morrison & Foerster—will talk about anticircumvention regulations in the United States, and their relationship to Digital Rights Management. He will be followed by Professor Graeme Dinwoodie of Chicago-Kent School of Law, and Professor Bernt Hugenholtz of the Institute for Information Law at the University of Amsterdam, both of whom will talk about anticircumvention regulations in European countries.

REESE: Thank you, Mark. My time is brief, but I would be remiss if I didn't take part of it to thank Pam Samuelson for inviting me, and to thank Pam and her colleagues and her students and the other co-sponsors for putting on this truly terrific and illuminating event.

I am going to be talking about a paper that I wrote that is available on the conference website. The paper raises the question of what incentives the legal protections for DRM systems that are in copyright law today offer copyright owners who are choosing which DRM systems to deploy. Now, I realize that legal considerations may be a fairly minor consideration in the choice by copyright owners of which technological protection measure to use. They are also going to be looking at how efficient and effective and costly those systems are. But I'm a lawyer, so I look at the legal regime, and I think that given the fact that copyright owners fought very aggressively for the anticircumvention provisions, and as we saw earlier this morning, speak very strongly about them, it is reasonable to think

that they will play some role in the choice of which DRM systems get deployed.

So, to remind you briefly of what Pam told us all at the tutorial on Thursday, the law in the United States protects two different kinds of technical control measures: access controls, measures that control access to a work; and what I call rights controls, measures that protect the rights of the copyright owner—the right to reproduce, distribute, publicly perform, publicly display, and so on. These two different kinds of controls get different legal treatment under the statute, and access controls seem to get more protection than rights controls. The clearest way that that is true is that access controls are protected against acts of circumvention, and rights controls are not.

Let me give you an example. The paradigm example of an access control might be something like the Divx system, where you buy a disk and the system allows you to access it only on a certain machine, and only for 24 hours, unless you contact the copyright owner and pay an additional fee. If Divx were still in existence, and you hacked around the protection in order to watch the film after your 24 hours had expired, that would be a paradigm instance of circumventing an access control. That act is illegal under Chapter 12 of the Copyright Act.

Rights controls, on the other hand, are not protected against acts of circumvention, and let me give you an example of how that might work. Imagine that I have a DVD player in my laptop computer, which allows me to play the DVD, see the film on the screen attached to my laptop, but doesn't allow me to send the output signal of the DVD to an LCD projector so that I can show it on a screen. That looks like a rights control. It's not controlling my access to the film, but it's limiting my ability to exercise one of the rights of a copyright owner, the right to publicly perform the film. If I were to circumvent that control (assuming that I had any technological ability, which I don't) in order to send the signal to the LCD projector to show the film on a screen, I would be committing an act of circumvention of a rights control, but not violating the law in any way with respect to the anticircumvention provision, because acts circumventing rights controls are not illegal. If I did that in order to send the signal to a screen in front of my class in Copyright Law at the University of Texas, I would also not be committing any act of copyright infringement, because the Copyright Act expressly allows teachers to publicly perform movies in their classrooms. So, that kind of act of circumvention would not be illegal as a circumventing act and there would not be any liability for it as copyright infringement.

For those reasons, access controls seem to get stronger legal protection in Chapter 12 of the Copyright Act, and that suggests that a copyright owner who wants to maximize the legal protection for a digital rights management system would be well advised to adopt access controls to get this additional protection.

Now, it turns out, if we look at least at the case law under the DMCA anticircumvention rules, copyright owners may not have to choose between these two types of legal protection. They may not need to choose because they may be able to merge access and rights controls into a single system. They may be able to protect against unauthorized exercise of the copyright owner's rights by using an access control.

What's the legal effect of merging access controls and rights controls? Well, so far, the legal effect has been that courts will treat a merged system as both an access control and a rights control, and therefore, entitled to both protections, that is, the stronger protection for access controls against even acts of circumvention. Indeed, in the DeCSS case, the decision of the district court was premised mostly on holding DeCSS illegal as an access control circumvention device. So, by deploying a merged control, the copyright owner gets the benefit of the stronger protection of the access control.

So what? Why do we care if copyright owners undermine this distinction that the statute draws between access controls and rights controls? Knowing whether we care depends on why we treat these things differently. Why do rights controls get less protection and access controls get more? And the legislative history of the DMCA, to the extent it is penetrable at all, is actually replete with statements. "We weren't going to ban the act of circumventing a rights control because that would allow the public to make noninfringing uses of protected works," . . . "If you circumvented a rights control, what you did would be illegal only if it violated copyright law, if it was infringing on its own." So, you could circumvent the rights control, you wouldn't face any liability under the circumvention rules, and if what you did subsequently was not infringing, you wouldn't face any liability under copyright law. So Congress said, "We're treating rights controls differently, giving them less protection in order to give breathing space for noninfringing uses of protected works."

Merging access controls and rights controls, and treating them as entitled to the protections of both, undermines this distinction. Users will have trouble circumventing the rights control, a perfectly legitimate act, without also circumventing the access control, and circumventing the access control is, of course, illegal. So the effect of treating these merged systems as

entitled to both sets of protection is, in effect, to suck all of the oxygen out of this breathing space that Congress tried to allow for noninfringing uses.

So, in the couple minutes I have left, how might we respond to this problem? Well, one response would be to do nothing. We could simply acknowledge that although Congress decided to treat these systems differently, it wasn't really a meaningful distinction. Why might it not be a meaningful distinction? Well, it could be that all the action is really in the device bans, and indeed Fritz Attaway said this morning, what really matters to us in the DMCA is stopping trafficking of devices. We realize that we cannot police these acts of circumvention. So, maybe Congress' intent to leave some breathing space for noninfringing uses by allowing the circumvention of rights controls was just lip service to get the thing passed, but all of the action is really in the device bans.

I am going to credit Congressman Lofgren's suggestion that Congress was in fact not just paying lip service to noninfringing uses. So, the suggestion is that instead of simply ignoring this, what we might do is say that acts of circumvention of an access control measure are not prohibited under the DMCA, as long as the person who circumvents the access control measure doesn't commit copyright infringement. You are free to circumvent them, and any liability that you face would be liability for copyright infringement, not for circumvention. Now, this wouldn't deal with some concerns that people have about the DMCA, which is that the device bans are really what matter, and those of us like me who can't engage in technological savvy circumvention, won't be able to do this even though it's legal, but it's at least a place to start to try and preserve the breathing space that Congress said it wanted to allow for circumvention of noninfringing purposes.

. . . .

DINWOODIE: When the organizers of this conference were putting together the program, a session on the implementation of the EU Copyright Directive seemed likely to be very timely, because the deadline for implementation of the Directive was December 22 of last year. You would think that therefore we would have fifteen or twenty-five national laws that Bernt [Hugenholtz] and I can actually talk about. In fact, two months after that deadline, only Denmark and Greece have actually enacted laws implementing the Directive. While this isn't an unusually tardy schedule, because the European Union Member States don't always implement the Directives on time, it does make what we are talking about a little bit more contingent. The good part of this is that, to the extent you don't like the shape that the proposals currently take, there is still an opportunity to influence the way that Member States implement the Directive in their laws.

The downside is that the Member States are under significant constraints from the European Union legislature itself regarding the choices that they can make about DRM regulation, because the Directive made a lot of those choices at the European Union level, and took away the autonomy from the Member States. That hasn't prevented, at least in the proposals that are out there at the moment, some Member States from trying some creative things, such as defining "technological protection measures" in ways that might exclude certain measures, like region coding and things like that, or adding alternative mechanisms, such as the German proposal does, that would require any product that has a technological protection measure on it to be labeled in a way to allow consumers to know about the content of those measures. The Directive does, however, constrain a lot of the choices, and as Pam [Samuelson] mentioned some of these in the tutorial on Thursday, I don't want to spend a lot of time on them. I should say, however, that like the DMCA, the European Copyright Directive is aimed both at acts and devices. Unlike the DMCA, it does not distinguish in the way that Tony [Reese] talked about between access control and rights control measures. Both are treated exactly the same, in fact, based upon the recognition that in fact these were likely to, at some point, work in combination. One other important difference from the DMCA is that there are no exemptions in the Directive itself to the anticircumvention prohibitions. That is not to say that the legislators were unaware of the potential that a broad prohibition might restrict the ability of the beneficiaries of exemptions under the copyright laws actually to exercise those exemptions; so they enacted a provision, Article 6(4) of the Directive, that really gives voice to that concern, or at least attempts to give voice to that concern.

Let me read the first paragraph. There are several paragraphs in this Article, and Bernt [Hugenholtz] at some step might talk about the second paragraph, but the first one reads as follows: Notwithstanding the prohibitions against acts of circumvention and circumvention devices, in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for a national law in accordance with—a whole bunch of Articles that permit exceptions—the means of benefiting from the exception or limitation.

My first reaction to reading that was that it must read better in French. But it doesn't have an awful lot more guidance or clarity in any language of the European Union. What I'm going to try and do is focus on that provision, which really is the vehicle for the infusion of balance into the Di-

rective, and suggest some of the ways in which it might operate, and the ways in which Member States are beginning to consider it operating. Before I do so, let me just mention however, that although it is potentially a very, very broad vehicle, in fact there are some limits built into it at the European Union level. In particular, it's only going to allow beneficiaries of certain listed exemptions to be able to take advantage of the potential 6(4) procedure; and those exemptions must exist in national law. The national laws of the European Union are not really harmonized on exemptions, because the European Union decided to make the list of exemptions in the European Union Copyright Directive optional. So there are significant limits on the ability of Article 4 to provide that balance; but notwithstanding those limits, it continues to operate.

Well, the first question is: What triggers the obligation on Member States to take "appropriate measures"? The provision appears to suggest that the need to take appropriate measures is brought into play by the inability of the beneficiaries of certain of those copyright exemptions to take advantage of the exemptions, because of technological protection measures. Some European commentators suggest that this trigger is unlikely to occur for a while because most works will be available in unprotected formats. If the scope of Article 6(4) was like the DMCA rulemaking, limited to adverse effects on "calluses of works", this argument would seem stronger. But it isn't. If you look at the exceptions that are in Article 5 that are incorporated by reference into 6(4), they refer to uses and purposes, not simply classes of work that are involved.

Perhaps normatively there should be some limit to this. That is to say, perceived unavailability of a single work for a single use might be insufficiently substantial a cost to warrant construction of an entire apparatus or mechanism contemplated by 6(4). Which I guess illustrates the point to some extent that Richard Epstein made this morning. But this depends on what's contemplated by the Member States as an "appropriate measure" in a response to the inability to exercise an exception granted by copyright law. If appropriate measures simply means grant an exemption, then there may not be any real cost to enacting a pretty low trigger level, a low threshold. If appropriate measures means, and this actually is possible and quite clearly contemplated by the Directive, mandating particular technological measures to be used by content providers, or establishing a complex quasi-judicial system for determining when such impairment of ability to exercise such an exception exists, then perhaps a higher degree of impairment should be warranted before that happens. I think the answer actually is that it's a little bit of both. That is to say, Member States should consider the combination of these different devices as ways of assuring

that beneficiaries of copyright exemptions can actually take advantage of those exemptions, and that a combined system using specific exemptions, and a quasi-judicial system not unlike rulemaking, imposing more intrusive or structural measures where classes of works are involved, might actually be the way of doing it.

This, I think, you might say, brings us then to the ultimate question of, what are these appropriate measures that states are obliged to take if, in fact, copyright beneficiaries aren't able to take advantage of exemptions. However, there is still another hurdle here. It's a little more complicated. The obligation of Member States to take these appropriate measures only arises in the absence of voluntary measures taken by rights holders. The recitals emphasized that some reasonable time is to be given to right holders to come up with the voluntary measures. Well, what are the voluntary measures and how do they affect the timing of Member State intervention? The only type of voluntary measure that is expressly referenced is agreements between rights holders and other parties concerned. But reaching such agreements is going to be a very difficult task because of the range of stakeholders with interests implicated by copyright law. To the extent that the exemptions are linked to particular purposes or uses, it is difficult to know who the different persons who potentially should be involved in negotiations are. The likelihood is therefore a complex web of agreements would have to be in place to give full effect to the different copyright exemptions. Rights holders might also consider modification of technological measures in ways that allow the beneficiaries of the exemptions to exercise their exemptions.

I think one of the more interesting things I heard on Thursday, though I think there's a lot of debate within the technological community, is the extent to which technology could in fact be developed in a way that reflects some of the nuances of legal exemptions. My sense was that to reflect the nuances of fair use is close to impossible, but someone made the point that in fact to write down in legal language how fair use applies in particular settings is very, very hard as well; but to the extent that particular exemptions that are actually much more like European exemptions, technology might be one of the appropriate measures that could be mandated by Member States (and which could voluntarily be adopted by rights holders).

The difficulty attendant to the process of voluntary arrangement also implicates the question of timing. Recital 51 imposes an obligation of Member States to promote the voluntary measures we've been talking about, but suggests that rights holders have a reasonable time to develop those measures. Well, what is a reasonable time? Some commentators in

Europe have suggested that such a reasonable period of time should only start to count, only start the clock going, the moment where "technological protection measures are sufficiently widespread and have a negative impact on the beneficiaries of exemptions." On one hand, it may not be clear what future effect the measure is likely to have and acting too quickly may be premature. On the other hand, there is a danger in building exemptions that will apply prospectively based simply on past practices. Those past practices may change. So I think the important thing for Member States to recognize is that there are two different acts involved here that affect timing. One is the obligation to promote voluntary measures, and the second one is Member State intervention by way of appropriate measures to remedy any imbalance.

The first obligation is immediate. As soon as the Directive is effective, that obligation exists. Only the second one is actually delayed. Some Member States in their proposals have understood that and have set up provisions that they think will help promote the development of voluntary measures. In particular, what several states have done is to establish a procedure that doesn't look unlike the DMCA rule-making procedure. In particular, the British proposal suggests that beneficiaries of exemptions who believe that they are not able to take advantage of them can apply to the Secretary of State for a direction to the content provider regarding ways in which the content provider should make the exemption available.

Now that direction may simply be that they have to obtain voluntary agreements with other interested parties. Let me just mention a couple of other possibilities in terms of appropriate measures that are suggested both by the recital and some of the commission officials. Recital 51 mentions the possibility of modification of the implemented technological measures actually being the form of appropriate measures that the state could direct. This interestingly inverts the "no mandate" debate in that content providers might suddenly be very interested in the notion of a "no technological mandate" philosophy. The other thing that I noticed was that one of the top commission officials suggested in a workshop this just last year that these means might include, and I quote, because I'm not quite sure what it means, "handing out the locking key." That's in a translation, so quite what he means I'm not really sure; but certainly the language of "right holders making available to the beneficiary" suggests affirmative conduct on the part of the rightholder, more than simply accepting the availability of the statutory exemption. The extent to which Member States are willing to push affirmative measures as one of the appropriate measures, I think will determine the overall effectiveness of Article 6(4) ensuring the beneficiaries are able to take advantage of their exemptions.

HUGENHOLTZ: I am under specific instruction from the Kingdom of the Netherlands not to make any jokes or other derogatory remarks about your President, so I will be brief. I would like to talk about something distinctly un-American, a typical product of old Europe, which is levies—levies for private copying —and the way the levy system in Europe is being affected, or will be affected, by DRM. Interestingly, while levies appear to be on their way out in Europe, there is increasing interest for levies here in the United States, at least in academic circles.

DRM and levies are from two different worlds. Reconciling them is like trying to square a circle. Indeed, this is what the European Copyright Directive attempts to do. Whereas DRM is based on individual rights management, reinforced by contract and technology, levies are a very crude form of collective rights management. DRM aims at keeping content exclusive, whereas levies operate under a statutory license. Users of DRM-protected content paid for what they get (or not get), whereas levies are something of a tax on equipment media, unrelated to the value of the actual content. Consumers pay providers of DRM based directly, whereas levies are paid by equipment manufacturers, or manufacturers of blank media. These costs then are passed on to the consumers. So, these are very, very different worlds.

Let me tell you a thing or two about private copying levies as we have them in Europe today. They are not the same everywhere. In fact, in the U.K. and Ireland, they do not exist at all. There are levies on equipment in a couple of countries in continental Europe. These levies traditionally apply to photocopying machines, fax machines, tape recording devices, and VCRs. More recently, and more controversially, levies have been imposed in some European countries on digital scanners, MP3 recordables, CD writers, and hard disks. Levies on blank media have also existed for some time: on blank audio and video tape of course, and more recently on minidiscs, CD recordables, CD rewritables, and even on recordable DVDs. So there are lots of levies in Europe today.

It is interesting to have a brief look at the history of the levy system. Levies were invented by the German Supreme Court in the 1950s and ’60s The Court on several occasions held that copying for personal use, using such “modern” technology as tape recorders or photocopiers, was not exempted from copyright protection. Manufacturers of such equipment were therefore held liable for contributory infringement. The Supreme Court, however, also recognized that enforcement of copyright claims against individual users would easily conflict with the users’ right to privacy. Thus a system of levies was suggested as a compromise between copyright and the right to privacy. This court-invented system of levies was

eventually codified, first in Germany, and later in many other countries in the EU.

Now, let's have a look at the EC Copyright Directive, and the way it tries to square this circle. In Articles 6 and 7 it promotes and protects the deployment of DRM systems, while in Article 5.2(b) it mandates private copying levies for analog and digital equipment and media. What 5.2(b) says is that insofar as Member States permit private copying, they should provide for fair compensation, i.e. levies, to the right owners. The amount of fair compensation, however, should "take account of the application or non-application for technological measures." The idea behind this rather opaque language is that if you would not take into account the deployment of DRM, consumers would end up paying twice: first to the rights owners, directly under the DRM system, and a second time indirectly through the levy system. So, to avoid such double payment, the Directive effectively sets out a track for the gradually phasing out of levies.

But what to make of that language in the Directive? How to "take account of the application or non-application of technological measures"? That's one of the many difficult questions that European lawmakers are facing today. Does it mean that national authorities are under an obligation to measure the actual degree of use of DRM systems? Does it mean they will have to measure what percentage of content actually is being protected by technological measures? And if so, what is the base line there? Should it be measured against a "perfect world" where 100% of content is securely delivered through DRM systems? And how should we measure that? If you think about it—and at our institute we have been thinking about it; we are actually finalizing a study which tries to make sense of this provision—you quickly come to the conclusion that this is not doable. This simply doesn't work. So, you have to look at other alternatives to give at least some meaning to this phasing out of levies. What we have come up with, a reading based on the recitals preceding the Directive, is that we should not look at actual degrees of usage, because that is an immeasurable and hopeless task. Instead we should look at the actual availability of DRM systems in the marketplace—availability, not simply as a function of the state of technology, but also in terms of economic viability. What are costs for content distributors, what are the costs for consumers, and particularly to what extent will consumers actually accept these technological measures, these DRM systems? In this respect, the very interesting discussion of yesterday afternoon will play a crucial role: what may consumers reasonably expect from DRM?

Last but not least, we should look at the legal side of the coin. Are there technological measures available in the marketplace that comply

with the law? Do they sufficiently respect privacy in such a way that the main reason for introducing levies in the first place, which was to protect the user's privacy, has disappeared? What all this adds up to is a process of technology assessment in a very broad sense, a regular (annual or bi-annual) rule-making procedure, to be conducted by the European Commission, national authorities or copyright tribunals. What it shows is that you might use the impending phase-out of levies as an incentive to introduce DRM systems that are socially acceptable. Until that happens, levies and DRM are bound to exist side by side for some time, as will, we all hope, "old Europe" and the United States. Thank you very much.

. . . .

QUESTIONER: FRITZ ATTAWAY, MOTION PICTURE ASSOCIATION OF AMERICA: A question for Professor Hugenholtz. Jack Valenti is frequently demonized for having suggesting back in the 1980s that levies be placed on VCRs. You may have heard that this morning. If this is such an absurd idea, why have so many of the world's great democracies in Europe adopted this ridiculous scheme?

HUGENHOLTZ: This is a trick question. I wasn't there when all of this happened, but I don't think if the choice had been between a prohibition on copying equipment and a levy, the choice would have been so difficult to make. But it all starts with imposing contributory liability. If that had not happened in Germany, I don't think we would have had levies in Europe.

LEMLEY: Let me just add one thing to that. You can look at a levy system in one of two ways, right? You might look at a levy system as a replacement for a copyright infringement system. That is, you can be sued for copyright infringement, but if instead you pay a tax that justifies the cost of the copying, then you can no longer be sued for copyright infringement, and your use is justified. Alternatively, you can look at a levy as a supplement to an existing system of copyright infringement, in which you say you will pay a tax and you will still be prohibited from making copies that violate the copyright law under the tax. It seems to me that how one feels about levies might differ greatly depending on what system a particular individual has in mind.

QUESTIONER, DON WHITESIDE, INTEL CORP.: I am curious what your view is of the efficiency of the levies infrastructure. The objective clearly is to provide compensation, and fair compensation, back to the rights holder; and I am curious what your perspective is on how the money is collected, whether the rates are done through a formal process, and how much of those funds actually make it back to the rights holders.

HUGENHOLTZ: There's indeed very little transparency in the way many levy systems operate in Europe. Tariffs are more or less randomly set, sometimes in negotiations between collecting societies and equipment or media manufacturers, sometimes ordained by government authorities or copyright tribunals. The transparency further decreases as you look downstream. The way levies are being redistributed, or "repartitioned" as they say, by the large collective societies to rights holders is murky, to say the least. It is a very, very nontransparent process.

LEMLEY: All right, please join me in thanking the panel.