21ST CENTURY COPYRIGHT LAW IN THE DIGITAL DOMAIN SYMPOSIUM TRANSCRIPT

UNIVERSITY OF MICHIGAN LAW SCHOOL
ROOM 250, HUTCHINS HALL
FRIDAY, MARCH 24, 2006

Cite as: *21st Century Copyright Law in the Digital Domain Symposium Transcript*,
13 MICH. TELECOMM. TECH. L. REV. 247 (2006),
available at http://www.mttlr.org/volthirteen/transcript.pdf

WELCOME AND INTRODUCTORY REMARKS

SHARON ARMSTRONG: Good morning. My name is Sharon Armstrong. I'm the Executive Symposium Editor of the *Michigan Telecommunications and Technology Law Review*. I'd like to welcome you to the University of Michigan Law School, and thank you for being with us today.

The *Michigan Telecommunications and Technology Law Review* began planning this Symposium about a year ago. At that time, the Supreme Court hadn't yet handed down its decision in *MGM v Grokster*, a case in which the entertainment industries sued yet another peer-to-peer file-sharing network.

After following the case as it wound its way up the courts, discussing the case in our classes, and learning about how Grokster's technology differed from its predecessors, we knew that whatever the Supreme Court decided, the *Grokster* case would have a significant impact not only on copyright law, but also on the people who use and create technologies that interact with copyrighted material.

We have a very distinguished panel of experts in copyright technology here with us today to explore many of these issues. They've traveled from across the country and I'd like to extend another very special welcome for being with us.

Now I'd like to introduce the Dean of the University of Michigan Law School, Evan Caminker.

[Applause]

DEAN EVAN CAMINKER: Good morning. In addition to being the Dean, I'm the father of a three-month-old baby, and so those of you who are parents or have had young children know that this is a period of time in which in the wee hours of the morning I am up and spending

many, many, hours pacing back and forth in the family room with a little infant on my shoulder, and there is one and only one thing that has kept me sane during the last three months, and that is TiVo.

[Audience laughter]

I am now a big fan of the digital revolution in technology. TiVo allows me to actually watch the entire session of March Madness, including this morning watching the last three minutes of the UCLA game last night 22 times.

[Audience laughter]

And I have to admit it, I had to keep waking my daughter up because, of course, the second she goes to sleep, I'm supposed to go to sleep, and I'm saying "No, no, you're not going to sleep yet."

[Audience laughter]

But it does remind me at this point in time about how so many things have changed in our world with respect to the presentation and articulation of ideas that come to us in a digitized form and as there is this continuing revolution in technology, as we all know, there will be a continuing butting of heads between existing legal forms and these new diverging technologies. And that's why it's really exciting today to have such a wonderful conference to look at this intersection between the revolution of digital technology and what I think will be a revolution in copyright law.

I want to second the general welcoming on behalf of the Michigan Law School to all of the wonderful participants in this conference. I'm particularly pleased that not only do we have distinguished academic guests, but we have distinguished guests from the world of law and the world of policy. In some cases, we have individuals who actually inhabit two or three of those worlds. I think it's going to be a nice mixture for those of you in the audience to see the interplay between the academic side and the legal and policy side.

Frankly, I also would like to start with a thank you to the *Michigan Telecommunications and Technology Law Review*. Obviously, the students have worked incredibly hard over the last year to put together this wonderful set of panelists, this wonderful day for all of you. So, please join me in congratulating and thanking them.

[Applause]

PANEL I
GROKSTER AND ITS AFTERMATH

KATE GUSMER: Now we're going to start our first panel. The panel is *Grokster* and Its Aftermath, and the panel is going to be moderated by Professor Margaret Jane Radin.

Professor Radin is the William Benjamin Scott and Luna M. Scott Professor of Law at Stanford University. During the 2004–2005 school year, she was a visiting professor at the University of Michigan Law School. In the fall she was visiting at Boalt Hall at the University of California at Berkeley and she is at NYU Law School right now.

Professor Radin is a co-author of *Internet Commerce: The Emerging Legal Framework*, which is the first traditional-format case book on E-commerce. Her research involves intellectual property, information technology and electronic commerce, and much of her current research is focused on the role of contract in the online world. In 2002, she founded Stanford's Center for E-commerce.

[Applause]

MARGARET JANE RADIN: Thank you so much. It is great to be back in Ann Arbor. I'm very happy to be here. The panel we have on this topic is the one that I would have chosen as ideal if I could've had anybody in the universe. I'm not going to read their bios to you because I don't want to take time away from what they have to share with you. Instead I'm going to say "Please read the bios." We have Michael Carroll from Villanova. He's an expert on copyright who has done important work on music copyright. And he's missing an important basketball game to be with us.

[Audience laughter]

We have Niva Elkin-Koren also a copyright expert, all the way from Israel, who has done seminal work on digital property and contract. We have Tony Reese, from Texas, whose work on the history of copyright is uniquely impressive, and then Fred von Lohmann, from the Electronic Frontier Foundation in Northern California, who actually litigated the *Grokster* case. Please promise me you'll read their bios!

Here are a few words of introduction. In this symposium we're talking about secondary liability. Secondary liability is widespread in U.S. law. But it's problematic because some other actor is actually performing the proscribed act. There's accomplice liability in criminal law, with the question of how far it should extend, and similar questions in tort; for example, whether auto manufacturers should be liable in tort if their car is likely to run off the road and hit somebody. There's the question of whether gun manufacturers should be liable if their guns are not as safe as people think they should be or whether they are primarily used by

gangs and the gun manufacturers know that. Secondary liability in copyright law refers to situations where an actor is held liable for infringement even though that actor did not perform the infringement. Secondary liability does rest upon a direct infringement being found—that is, someone did perform an infringement, and someone else is being held responsible.

You can see that secondary liability is both widespread and problematic. There is an important question that is now before us, which the *Grokster* case puts into focus, about how far secondary liability in copyright does or should extend. The underlying question is whether distribution of technology that can be used for infringement will make the distributor of the technology secondarily liable. This is a hot issue in copyright, but it's also present in trademark and patent law.

It's an important question especially in copyright. It is a bet-the-company question for distributors in the digital environment, because each and every unauthorized copy is subject to big damages. Every time a computer does anything it makes a copy, so in these situations there are millions of copies. And so, therefore, your company is over with if it is held to be secondarily liable. So, as this panel will be discussing, in practice this huge risk of secondary liability is driving innovation policy.

The plaintiffs in the *Grokster* case, the movie industry, really wanted to get the *Sony Betamax* case from the 1980's reinterpreted. The *Sony Betamax* case said you can't be liable for technology alone when it is being used for infringement by others, if your technology is "capable of commercially significant" (or sometimes) "substantial" non-infringing use. "Capable"—that's future oriented. It could be used for infringement today, but sometime in the future it can be capable of substantial or commercially significant non-infringing use. The plaintiffs in the *Grokster* case wanted to change this to look only at the present; if the technology is being used a lot for infringement now, then the distributor should be liable.

The defendants in the *Grokster* case wanted *Sony* to be upheld and be enforced. In the years since the Supreme Court decided the case, *Sony* had been weakened, particularly in the 7th Circuit by Judge Posner in the *Aimster* case, where the judge said that he was following the Supreme Court's decision in *Sony*, but instead basically followed the dissent in that case. He said, paraphrasing, "We need to look into the cost benefit analysis and see how bad the infringement in the present is today." This position didn't win in the original *Sony* case but it is a position that the copyright industries would rather have.

So what happened over time was that *Sony* had become weakened or ambivalent. In the 7th Circuit you have one thing; in the 9th Circuit be-

cause of Mr. von Lohmann's victory in *Grokster* you had another thing. Thus, what was at issue in *Grokster* at the Supreme Court was whether the Justices were going to affirm the original *Sony* rule, or revise it.

The numerous amicus briefs in this case, which I think are still posted at Fred's organization, [eff.org], show this as a battle between the content industries and the equipment manufacturing industries. Many, many amicus briefs were filed, by big players in the technology industry such as Intel. They were not trying to support infringers but instead trying to avoid having the copyright industries be able to control what technologies they are able to introduce. Nobody thought that these defendants should win, but, the equipment manufacturers didn't want their product design to be subject to control by the content industries. On the other side, the content industries don't want products out there that make it difficult to catch infringement. That is what the battle is about.

The Supreme Court in *Grokster* was split into three parts. There are nine of them and it was three, three, three. As I think this panel will further tell you, Justice Breyer, joined by Justices Stevens and O'Connor, wanted to maintain *Sony* and said the 9th Circuit was correct. Indeed, Justice Stevens was the original author of the *Sony* majority.

However, Justices Ginsburg, Rehnquist, and Kennedy do want to adopt pretty much the original dissent in *Sony*, which Justice Rehnquist was a part of. He too was consistent. And the third group, Justice Souter who wrote the opinion, joined by Justices Scalia and Thomas, say that *Sony* remains in force because this case isn't about *Sony*. It is about active inducement to infringe, not about facilitation of infringement by mere distribution of technology. So, what *Sony* actually now means remains shaky. Does it mean what the 9th Circuit says or what the 7th Circuit says? (Neither of the above?)

I think I'll stop there and let our panel just talk.

MICHAEL W. CARROLL: Great. Thanks. So I get to lead off, and I've just got to get onto first. I am not going to talk about *Sony*. I will leave that for my fellow panelists. I am going to focus on inducement. I want to start at a fairly high level.

Let's look at the legal and policy goals of two industries—the content industry and the technology industry—and then work through the case. So we've been told the threat of digital technology from the content industry's perspective is that it becomes one big copying machine. General purpose computers connected to the internet take away a substantial amount of control over distribution that was previously enjoyed.

So, their response is to try to staunch the flow of unauthorized files flowing across the network. And the way to do that, ideally—from the content industry's perspective—is to get to the design of these

technologies. So what these industries are looking for is a legal theory that will give them a legal threat over the design process. And you've heard this and you'll hear it again all day, but that's really the big problem with *Grokster*.

They also have fallback positions. If you can't control the technology design process, then you control the process of distributing new technologies. Finally, if that doesn't work, can you at least impose some liability if there isn't an attempt to filter—an attempt to use the technology once it is out there in some way that limits its capacity for infringing use? So those are the legal and strategy goals of the copyright-dependent industries.

By contrast, the technology industry wants maximum freedom to base design decisions on factors such as marketability, efficiency, and other criteria, without having to take into account the copyright industries' concerns. In the alternative, if those concerns have to be taken into account, their strongest demand is for a clear rule. The worst case scenario is fuzzy liability that can't be quantified and therefore can't be insured against. And, as a fallback position, liability would be not based on design choices or whether there's filtering or not, but would instead be based on some proportionality between infringing and non-infringing uses or some other test.

So, those were the opposing strategies going into the case. As Professor Radin just said, I want to reiterate that the parties were looking at this based on two doctrinal tools: contributory infringement and vicarious liability. That was the framework in which the case was presented.

Contributory infringement is fault-based liability. It had grown up in the lower courts as requiring some proof of knowledge of infringing use and participation in the infringing use. It's important that in the *Sony* decision, the Supreme Court mushed together contributory infringement and vicarious liability. It did not separate a fault-based and a strict liability regime. So from the Supreme Court's perspective, it was not bound by its own precedent with respect to the theories of liability analyzed by the Ninth Circuit.

The lower courts though, in going through the common law process, had created doctrinal rules, and these had started to ossify a little bit. So the evidence required for contributory liability in the lower courts was some form of knowledge about direct infringement and some form of participation in the infringing acts. We saw the lower courts relaxing the requirements to meet both of these elements under contributory infringement. Under the doctrine of vicarious liability, a defendant needed to have control over the direct infringer and receive a direct financial benefit from the infringing activity. And, we saw the courts relaxing the

requirements, so the measure of control could be a user agreement that says, "We can kick you off if we want." And, a direct financial benefit could include an indirect financial benefit, in fact.

The Supreme Court had not fashioned either of these doctrinal formulations of secondary liability, and in fact, I think the Court in *Grokster* reformulated both of these. So one of the legacies of *Grokster* will depend upon how seriously the lower courts take the Court's restatement of these doctrines. In the Supreme Court's words, contributory liability is now not based on knowledge, but on intent. So fault-based liability is now more directly proven by showing intent and contributory liability is intentionally inducing or encouraging direct infringement. Apparently, one reading of that is that there has to now be a tighter nexus between the secondary infringer and the primary infringer.

And, to my mind, even more important is the Court's reformulation of vicarious liability. It is questionable now whether secondary liability can be strict because, according to the Court, vicarious liability is now phrased as profiting from direct infringement, while declining to exercise a right to stop or limit it. Well, declining to exercise a right presumes perhaps a level of knowledge about the infringing activity, and therefore, it's not clear that there can be strict liability, although the prior case law has said knowledge was not required. So that is sort of a doctrinal hook that can be developed in a variety of ways. But now let's focus on what the Court did.

So that was a quick intro into inducement, which is now a new branch of contributory liability. It's got three elements. You are an inducer if you (1) distribute a device (2) with the object of promoting an infringing use (3) with the clear expression of promoting infringement or taking affirmative steps to promote infringement. Okay?

Now that sounds like a pretty limited source of liability, and a lot of the commentators have read the opinion that way. But in the common law, you can't just take the legislative part of the decision—the announcement of the rule—you then have to look at how it is applied.

When the court applies this rule to the facts, it says there are three pieces of evidence that show that there is inducement here. First, *Grokster* targeted a known source of infringement, that is, former Napster users. Then there was no attempt to develop filtering tools. Now wait a minute. Where did that come from? This statement is followed by footnote 12. I think from now on, *Grokster* discussions will talk of footnote 12 in the way that constitutional lawyers talk about footnote 4. Footnote 12 says, "But failure to develop filters by itself does not subject you to liability."

So, the court seems to be saying on the one hand failure to filter in this case is inducement, but this does not announce a general rule that failure to filter is evidence of inducement. Lastly, the defendants' software depends on scale and where infringing use is an important part of the scale for the business model that is evidence of inducement. So, it is not clear how those three pieces of evidence relate to the standard that was just announced. And I think that this disconnect sets the legacy of this inducement standard up for further development. And there's something in it for both sides.

My prediction is that the Court will have the experience that it had in trademark law and that it is having in patent law, where it thinks it's crafting a carefully balanced rule. It then sees the way that aggressive parties push that rule to its limits and then the Court is forced to revisit the rule.

So inducement now. Here's the narrow reading that the technology industry is likely to push for. Then I'll give you the broad reading and I'll leave it with the message that the battle to control the destiny of inducement liability is on. The narrow reading is that intent is now the name of the game. Knowledge of infringing activity by itself won't get you there and evidence of intentional acts to promote infringement is necessary to impose liability. And that is a more demanding standard that was previously required under contributory infringement. As long as your marketing materials don't show that kind of intent—as long as you don't take other affirmative steps—even with a sort of nudge and a wink, then one can avoid inducement liability.

So under this reading some of the first reactions were that this case is essentially limited to its facts because the Court punted on the *Sony* rule and the state of the law of secondary liability, is otherwise as it was. As I mentioned, I do think that the court intended to reign in the scope of the doctrines of contributory infringement and secondary liability as interpreted in the Ninth Circuit. I do think the intent was to shift emphasis away from the vicarious liability strain of strict liability that the 9th Circuit had developed, and to move to a fault-based regime, and to admit having a fairly demanding standard for what evidence would be evidence of fault.

I want to make sure we understand that although the Court was split into groups of three, Justice Souter's opinion was a unanimous opinion. So the unanimous court signed onto a statement that said, "We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential."

There is a need not to discourage dual-use technologies. It is a public policy that nine justices of the court signed onto. Dual-use technologies are an affirmative good that ought to be developed. All right? That point is likely to get lost in the shuffle unless the technology industries can develop it in litigation. Evidence that this is likely to happen is what the *Grokster* commentary has already found.

In contrast, I think that the legal strategy of the content industries will be to turn the inducement standard into the revision of the *Sony* standard they wanted. And I've got evidence for this in an article co-written by Professor Jane Ginsburg which essentially lays out the road map for how you do that. She walks through the *Grokster* opinion and suggests that the filtering requirement could in fact be drawn from the *Grokster* opinion and could be an affirmative requirement and the absence of filtering could serve as evidence of intent as a general matter.

Moreover, because intent is a slippery standard, I think the first strategy of the copyright-dependent industries will be to drive intent all the way into the design process because that process involves intentional acts. Can you prove that the technologists had a choice about whether to make the technology capable of filtering? Did they have a choice to build an opening for a plug-in that would limit the use of the technology? Did they choose not to develop that plug-in? So although the intent element, I believe, was introduced to limit the scope of secondary liability—because there are intentional acts back at the beginning of the process—the intent standard opens the possibility that the inducement standard can be driven all the way back into product design. If its intent does not cover product design decisions, then use of the technology and the choice not to filter will be the next argument over relevant evidence of intent.

I don't think the court intended that result. I think some of the lower courts will accept the content industries' interpretation, however, and I think the Supreme Court will have to come back and clarify that it really was trying to reign in the scope of secondary liability. But it is a common law process and I think it's game on. And whoever can develop the better record, the better cases, and deliver the better lawyering will win the struggle over the legacy of the inducement standard.

With that, I'll pass it off.

MARGARET JANE RADIN: Thank you. Professor Elkin-Koren.

NIVA ELKIN-KOREN: The optimism of some commentators who thought that *Grokster*, at the end of the day, was good news for the internet industry relates to the fact that the Supreme Court in *Grokster* did not overturn *Sony*. The Court, instead, introduced *inducement* as a basis for liability. What I'd like to do today is to examine this shift from *Sony* to

Grokster, from the substantial non-infringing use rule to the inducement doctrine, and to question whether it is indeed neutral on issues related to innovation.

In *Sony*, the Supreme Court established the fundamental framework for protecting copyrights in a dynamic technological environment. It sought to strike a balance between the demands of copyright holders for effective protection and the rights of others to freely engage in innovation and commerce. The Court held that a supplier of means that enable infringement could be held liable unless the supplied device has substantial non-infringing use.

The substantial non-infringing use defense was considered a key for keeping the courts outside the design room so that the law will not interfere with the freedom to innovate and would not stifle the progress. But the content industry felt that *Sony* no longer serves the interests of copyright holders, especially in light of increasing piracy and a growing difficulty to enforce copyright against individual infringers. Device manufacturers, they argued, should not stay clear of liability. If they enable infringement they should actively engage in preventive efforts. Copyright owners, therefore, asked the Supreme Court to limit the *Sony* exception.

In *Grokster*, the Supreme Court recognized that *Sony* secured some breathing room for innovation. Therefore, rather than overturning Sony, the Court opted for a new theory of liability—the inducement theory.

Inducement, as defined by the Court in *Grokster*, requires 1) the distribution of a device suitable for infringing use; 2) actual infringement by the recipients of the device; and 3) intent to bring about infringement.

Presumably, this new standard left the *Sony* rule untouched. It shifted attention from research and development related to new technologies, to commercial practices and intentions. What makes inducement so attractive to the courts is that it appears to have nothing to do with the technology itself. It is only the intention of those who use it that matters. The court could learn about this intention by examining market activities, promotion materials, and business models. If those reflect an intention to induce infringing activity, then defendants would be held liable, and the court would be exempted from having to balance copyright interest and freedom to innovate.

In my opinion, *Grokster* could, in fact, carry profound consequences for design and innovation.

First, inducement doctrine adds another layer of liability. It elevates the legal exposure for those engaged in designing new technologies. So now developers must consider legal exposure under contributory infringement, vicarious liability, as well as inducement.

Also, inducement doctrine does not stand on its own grounds. The elements of liability under inducement overlap with those required under contributory infringement and vicarious liability. Intent could be established by "gains that increase the more software is being used," which is one of the elements necessary to establish vicarious liability.

Inducement also requires supplying devices that would enable infringement which is one of the elements necessary for contributory liability. In fact, inducement repackages the same elements, only this time without the *Sony* non-infringing use defense. The same behavior that was considered legitimate under the *Sony* rule could now be unlawful.

The most important consequence of inducement doctrine for design has to do with *intent* as constructed by the Court in *Grokster*. The Court held that inducement requires the showing of intention to bring about infringement. The Court listed three types of evidence to support its finding of "unlawful intent." One type of evidence was aiming to satisfy a known source of demand for copyright. For instance, targeting former Napster users or naming *Grokster* after Napster was held liable for copyright infringement. A second evidence of intent was a business model: the more people use the software, the higher were the gains. Finally the Court found evidence of intent in the failure to develop filtering tools.

The court held that *Grokster* failed to develop preventive mechanisms against infringements and this failure shows its "intentional facilitation" of the infringements committed by its users.

This interpretation of inducement assumes an affirmative duty to develop the tools that would diminish infringement. Under *Grokster*, developers of technologies which are capable of non-infringing use could be expected to filter out infringing behavior.

The famous footnote 12 does not help much to limit the duty to filter. In footnote 12 the Court tells us that failing to actively prevent infringement would be insufficient for contributory liability. But this tells us nothing about inducement, right? Also, since other elements of inducement are relatively easy to establish, the stipulation in footnote 12 might not relieve designers of potential liability arising from the duty to filter.

The result is abandoning the *Sony* defense and requiring developers to cater the enforcement needs of copyright owners. In this sense, *Grokster* does follow, in my opinion, the 7th Circuit holding in *Aimster* which established a normative framework for determining the duty to filter. Here is how Judge Posner defines the circumstance under which a developer would be subject to a duty to implement preventive measures, "To avoid liability as contributory infringer the provider of the service must

show that it would have been disproportionately costly for him to eliminate, or at least reduce substantially the infringing uses." This is the good old least cost avoider rule: One should be held liable for hardship that she could prevent in a cost effective way.

What is wrong with that?

The first problem is analytic: Applying the *least cost avoider* approach in a dynamic technological marketplace leads to circular reasoning. We assume that parties should be held liable if they failed to employ cost effective measures. Yet, the cost and availability of such measures are themselves the result of a duty to employ certain measures. Liability rules could affect incentives to invest in research and development to produce specific technological solutions. If we hold suppliers liable for failure to implement preventive measures against hacking, we're likely to induce greater investments in efforts to develop such measures. This is likely to make such filtering available sooner and at lower cost. Therefore, the cost and availability of technologies cannot be considered exogenous in the liability analysis.

But the question is, of course, whether we want to encourage this type of technological development in the first place.

The *Grokster* interpretation of inducement invites legal intervention in shaping designs related to the standards. It is arguable that the Supreme Court in *Grokster* simply failed to stay away from design considerations, but still kept *Sony* untouched, and therefore, it really changed nothing in the status quo.

My concern is that the consequences of the duty to filter could be more profound. That has to do with the different assumptions underlying the duty to filter on the one hand and the *Sony* safe harbor defense on the other hand. The substantial non-infringing use defense assumed that it is impossible to tell infringing from non-infringing behavior, and therefore, that it is not justifiable to outlaw technologies simply because they enable infringement. A duty to filter, by contrast, assumes that distinguishing lawful and unlawful uses could be made possible.

A second issue is duration and cost. The substantial non-infringing use defense provided incentives at an early stage of the design. A duty to filter is enduring, and therefore, more costly. It requires suppliers to keep updating their system against new challenging efforts to hack and enable copying. You may recall the continuing effort by Napster to comply with the temporary injunction issued by the district court.

The last point has to do with design. The signals provided by the *Sony* defense encouraged the development of neutral platforms that could be used for many purposes in different ways. Consider, for instance, the shift from Napster's music service, the first generation of

peer-to-peer design, to the second and third generation of peer-to-peer networks. *Sony* also provided incentives to design systems that would allow more choice of the active users and would reduce central management and control.

A duty to filter may provide incentives for central management that would reduce the risk of infringement. Take ISP's for instance. Under *Grokster*, internet service providers could be held liable for infringing peer-to-peer traffic. First, they provide the infrastructure for infringing use by facilitating peer-to-peer applications on their network. Second, peer-to-peer is considered to a killer application which boosted ISP's revenues by increasing demand for broadband services.

Finally, intention could be learned from the failure of ISP's to implement filtering tools especially in broadband services. This potential for liability could affect incentives to develop solutions that would allow monitoring and filtering of peer-to-peer traffic, such as caching that is now emerging as a technical solution for managing peer-to-peer traffic.

Another example of how a duty to filter may affect design is attempts of file sharing networks such as eDonkey to follow iMesh and build a service that filters out unauthorized content.

To conclude, if we care about design we should worry about *Grokster*. If we believe, as I do, that the virtues of digital networks are vested in their decentralized nature which empowers end-users and minimizes control over the distribution of content, we should be concerned about the ramifications of *Grokster*.

MARGARET JANE RADIN: Thank you. Professor Reese.

R. ANTHONY REESE: Thank you. I think we're going to slightly shift gears now at this side of the panel away from the inducement aspect of *Grokster*. I want to think about one aspect of the *Grokster* aftermath, which is the avoidance by the *Grokster* court of the further development of *Sony*.

I want to adopt, at least for my purposes this morning, the reading of *Grokster* as saying inducement is a separate basis for liability, leaving undisturbed the existing set of standards under *Sony*. I want to consider a little bit the situation of the dual-use device maker who avoids inducement—who doesn't actively promote or do any of the express, overt acts that clearly constitute inducement under *Grokster* (putting aside the question of whether you can go behind that as the previous panelists have suggested).

So *Grokster* largely leaves the *Sony* standard in place with no further clarification of exactly what test a dual-use device has to satisfy in order to escape liability. *Sony*, of course, said the standard was that the device would be okay if it was "capable of substantial noninfringing uses" or

"commercially significant" non-infringing use. And *Grokster*, in my opinion, leaves that standard in place and requires us to keep thinking about what the substantial non-infringing use standard means. And in particular, this morning I'm going to talk a little bit about the temporal aspect of this standard. It is often thought of, I think, as a static concept, but I think it has a dynamic dimension that is worth considering.

So first I want to look at the dynamic element of what is a non-infringing use and then to think a little bit about whether there's a temporal aspect with respect to what "capable" of non-infringing use means. I'm going to leave aside the question of what is substantial or what is commercially significant.

First with respect to non-infringing use, the *Sony* case made it clear there are at least two primary categories of non-infringing uses of a device that are relevant: uses that are a fair use under the statute, and uses that are authorized—particularly uses that are authorized by the copyright owner.

So first, fair use. Here, I think we're becoming much more aware of the fact that there is a dynamic aspect to fair use and what's fair can change over time. We have a quite recent example in the form of the district court decision in the *Perfect 10 v. Google* case, which is about whether or not producing and showing thumbnail images as part of an image search engine constituted fair use. That recent district court case decided that because there was now a market for displaying small, low-resolution pictures on your cell phone and for selling people those pictures to put on their cell phones, the display by search engines of thumbnail images led to a finding of potential harm to the copyright owner's market—the market for tiny thumbnail images to be downloaded to your cell phone. And that weighed against a finding of fair use on behalf of the search engine. That decision stands in sharp contrast to a decision from only a few years earlier in which the 9th Circuit had said, "Well, there's really no real market for tiny little reduced resolution thumbnail images. So there's no real harm to the market in search engines displaying those images."

So clearly, markets can change over time. User behavior can change over time, and what is fair will change over time. *Sony* itself, I think, presents us with an example of this—and one that Dean Caminker with his new-found love for TiVo may not be happy about. The finding in *Sony* that seventy-five percent of surveyed users who time-shifted with their Betamaxes did not skip the advertising when they viewed the recorded program seems to be important to the Court's conclusion that time-shifting was a fair use.

When I teach the case, I survey my classes and I get a quite higher percentage than twenty-five percent who fast forward through the ads—I think, in large part, because at the time the survey was done, most Betamaxes did not have a remote control. So does the provision of a remote control, by changing the viewing habits, change whether or not time-shifting constitutes fair use?

This dynamic element of fair use, I think, means that today's fair use could be tomorrow's infringing use, thereby possibly reducing over time the quantity of non-infringing use that could be counted toward whatever is substantial or commercially significant use in evaluating liability for supplying a dual-use device.

A second set of non-infringing uses that comes out of *Sony* is a set of authorized uses, things that the copyright owner has allowed. The most famous example from the *Sony* case is Mr. Rogers and the evidence that Mr. Rogers was quite happy to have people tape *Mr. Rogers' Neighborhood* so they could watch it at a time appropriate for their kids. (It's great to teach the case in law school—how often do we get to talk about Mr. Rogers in the context of a Supreme Court decision)?

But the amount of authorization by copyright owners can obviously change over time as well. Again, we have an example directly from the *Grokster* case. Some of you may remember the lawyer for the recording industry saying in oral argument in the *Grokster* case that his clients—the recording industry—had publicly stated on their website that, of course, it was okay to take a CD that you owned and rip the songs on that CD onto your iPod for your personal use.

Recently, though, the RIAA, in a filing with the Copyright Office, indicated that yes, that was what they had said, but they didn't mean to say that that was fair use, only that it was *authorized* use by the recording companies, suggesting that the recording companies could tomorrow say, "We actually are not authorizing you anymore to rip songs from your CDs and put them on your iPods."

So authorization can change over time as well. But here I think it is possible to detect a general trend toward more authorized uses that would count on the non-infringing use side under the *Sony* test. In *Sony*, of course, we're dealing with broadcast television where we've got a relatively small number of copyright owners whose authorization is relevant, and who generally focus on commercial exploitation. But that has changed.

Let me ask you this. Raise your hand if you are a copyright owner. Okay—not very many hands. You're selling yourselves short. I'm quite confident that since 1989 all of you have fixed in a tangible medium of expression some minimally creative work of authorship, and you are,

therefore, a copyright owner, because copyright law has moved from an opt-in system where copyright owners were people who sought protection, to an automatic system where every creator automatically owns copyright.

As a result, we have a lot more copyright owners out there today than we did at the time of *Sony*. And because of technological advances, we have copyright owners who can produce pretty much every kind of copyrighted work. You could always have lots of people who produce literary manuscripts or musical compositions—all you really needed was a pen and pencil. But with today's technology you've got lots of people who can produce motion pictures and sound recordings and other kinds of elaborate works of authorship that used to be the province of the copyright industries.

Many of these new copyright owners—I suspect many of you who didn't raise your hands, and some of you who did—have much less interest in the commercial exploitation of their works than the traditional copyright owners did. They also—due to technologies like digital networks—have far more accessible means today to make those works available to the public at large. And, most importantly in thinking about authorized uses under the *Sony* test, they now have many more easy ways to indicate to the public their authorization that people can do many things with their works. I'm thinking specifically here about mechanisms like the Creative Commons licenses that allow people to release copyrighted works of authorship with express indication of permission for people to engage in lots of uses of those works. And we have millions and millions of works released under those licenses.

As a result of all of these trends, at least for general purpose digital devices, there's now a lot of copyrighted content out there for which the use on those devices is authorized by the copyright owner, and therefore, relevant in the non-infringing use analysis under *Sony*. Some channels of dissemination, of course, are not very open to this. There's still broadcast and cable TV, and broadcast and satellite radio, where you don't have a lot of small author-produced and distributed content becoming available. So if you're a technology producer who's creating a device that interacts specifically with a cable TV box or a satellite radio receiver, all of this additional authorized material may not help you very much if you're analyzing liability under the *Sony* test. But generally, I think there's been a shift since *Sony* to more authorization out there that can count as non-infringing use.

So that may be kind of hopeful about the non-infringing use possibilities and how they're changing over time. But now, having thought about what non-infringing uses are out there, I want to switch to thinking

about the question of how we figure out whether a device is "capable" of substantial or commercially significant non-infringing use.

I started off by saying the Court hadn't really given us any clarification of *Sony* in the *Grokster* case. That is true of the Court, but of course, four justices who still remain on the court did clarify their views about *Sony*—in Justice Ginsburg's and Justice Breyer's concurrences—and again I think these concurrences can be read to suggest a dynamic view of "capable of substantial non-infringing use" that changes over time.

Justice Breyer and Justice Ginsburg disagree about a lot in their concurring opinions, but while Justice Breyer seems to do various things at various places, it's possible, I think, to read the opinions as agreeing about what "capable of substantial non-infringing use" means.

Both opinions don't treat that question as a question about what uses the device has the *capacity* to make. They don't simply ask "What could this technology do?" Instead, they both seem to treat this question—the "capability" question—as a question of what uses a device can be shown to be likely to be *actually* used for in the future. Not just that it's capable of it, but will it likely be used in that way. They both have language that suggests the real question here is whether there is a reasonable prospect, or plausible likelihood, that these substantial non-infringing uses will develop over time. Not just can the device do them, but will they be adopted?

So, I think, they're essentially saying you're okay under the *Sony* standard if your device is widely used for legitimate non-objectionable purposes—language from *Sony*—or is reasonably likely to become so used in the future. And that view of "capable of substantial non-infringing use" as being about future adoption rather than the device's capacity has, I think, at least two consequences.

One, it makes me less optimistic about all this stuff that's out there that's been authorized for use as we just discussed because the question isn't just how many authorized uses are possible. The question is how many authorized uses are made or will be likely to be made in the future. So having a lot of content available under Creative Commons licenses isn't enough if people don't actually use the content that's available under that approach.

The other thing that it suggests, which I think is more worrisome, is that the answer to the question of whether a device is capable of substantial non-infringing use can change over time, even if what counts as non-infringing use doesn't change, even if there's no difference in what is fair use, and there's no change in the amount of authorization.

It seems to me that both Justice Breyer and Justice Ginsburg suggest that you could have a case where a court today says, "The distributor of

this device can't be held liable because there's a reasonable prospect of uptake by users of the device of authorized uses or fair uses of the work," and, that with respect to the same technology 10 years later—or 20 years later, depending on what the timeframe is—a court might say, "Well, that uptake hasn't happened. There could've been a lot of authorized and fair uses of this device, but it still looks like ninety percent, eighty percent of the use is for infringing uses. And therefore, although it was capable of substantial non-infringing use, it hasn't lived up to that capability. Nothing has changed to make us think it's likely to live up to that possibility in the next few years, and therefore, the distributor of that technology is now liable by distributing it for any infringing uses committed by the users."

So, I think that the aftermath of *Grokster* for the *Sony* standard, understood separately from the inducement standard, is going to potentially create (or preserve) problems for the courts and technology developers. This temporal dimension of how we figure out whether a device is capable of substantial non-infringing use is one that's going to bedevil us in future cases and the concurring opinions *Grokster* have only highlighted the problem.

MARGARET JANE RADIN: Thank you. Professor—Professor? No.

FRED VON LOHMANN: No. No.

MARGARET JANE RADIN: Not a professor. The non-professor Fred von Lohmann.

FRED VON LOHMANN: Yes, the non-professor. Because I'm speaking here to an audience of principally attorneys and people who will someday be attorneys, I feel confident that I can let on a little secret to this group here. As a practicing lawyer, you'll come to discover very quickly that practicing lawyers view litigation very differently from their clients.

And so, I remember quite vividly in the fall of 2001 hearing that a group of some thirty entertainment companies had brought a lawsuit against Streamcast, Grokster, and the makers of Kazaa. My first thought was this is going to be a blockbuster case. It's going to be the case that will test the scope of the *Sony Betamax* doctrine and will likely shape the scope of secondary liability in copyrighting for some time to come.

My second thought was that I hoped to be involved as counsel in that case. That worked out. I was counsel in that case. We at EFF represented Streamcast, one of the two defendants that were involved in the Supreme Court opinion.

We had very capable co-counsel representing Streamcast with us and referred our co-defendants at Grokster to excellent counsel, as well. We

thought it wouldn't be prudent to represent all the defendants given the differences between them. And so they, asked me for referrals for other counsel and I recall I referred Grokster to Michael Page who represented them throughout this proceeding. Later on I talked to Mike about this, and he admitted that as soon as he took that phone call, the first thing in his mind was—"We're going to the Supreme Court baby."

[Audience laughter]

I have to admit, I knew it would be an important case. I had no thought that it would go all the way to the Supreme Court. I mean, I thought it was possible it could go to the Court, but that certainly wasn't something I was taking for granted. Mike said he knew the moment he picked up the phone that we were going all the way. Now I have no way of disproving him because I didn't ask when I first spoke to him.

But let me tell you, from the client's perspective when you get sued by twenty-nine or thirty entertainment companies, the first thing in your mind isn't "Cool!"

[Audience laughter]

So let me walk through what I think that the post-*Grokster* world looks like from a client's perspective, because frankly, as attorneys, that will be the perspective you'll have to deal with on a regular basis in your practice.

So let me give you a hypothetical, and this hypothetical is not entirely hypothetical—that you'll recognize bits and pieces of it as having been drawn from real life—but let's imagine you represent a technology company that develops innovative technology and one of their products is a new digital mass storage device. It basically stores large amounts of digital data. Sort of the next thing beyond hard drives. This new mass storage device is particularly optimized for the storage and playback of digital video. Demand for such a device can certainly be imagined, given the increase in interest in digital videos in recent years.

So your client has developed this great new technology. It's showing great success in the marketplace. It's selling like gangbusters and then over the transom comes a letter from the Motion Picture Association of America. The letter says, "Dear Storage Co. It has come to our attention that your technology is being used principally for infringement of our copyrights. We know this because we have commissioned surveys in the field of your customers. Please find attached as Exhibit A to this letter the results of said survey, including responses from some 3,000 or 4,000 of your actual customers illustrating that in fact some seventy-five percent of them are using your technology to infringe our works. Moreover, we know that your works are being principally used for infringement because we have found many, many reports in the press from reviewers and users celebrating how well your product works for making unauthorized copies

of our high-definition movies. Please find attached hereto as Exhibit B a number of such articles, including the extensive threat of Slashdot people saying, 'Boy, oh, boy, this is really the way that you should be archiving your movies you've downloaded from BitTorrent.' " This bit, by the way, is the bit from real life. The number of times I've seen copyright owners cite Slashdot as evidence.

[Audience laughter]

It is really quite stunning for anyone who actually reads Slashdot regularly. The MPAA letter continues, "And moreover, we believe that there are very easy and inexpensive ways that you can modify your technology to reduce this popularity for infringing uses. Please find attached hereto as Exhibit C a detailed description from our retained technology experts explaining things you can do to change your technology that would make it less useful for copyright infringement. We, for example, think watermark detection would be a wonderful thing you could add. Moreover, we also think in future iterations of your product, you should include a tether whereby you can go back and update that product and users in the event new and better forms of technology should develop that would make your product even more resistant to infringing uses."

The term, by the way, in the movie industry field for this is "revocation." It is something that they're very serious about. The notion is that they don't want to see products that go out the door that cannot be subsequently modified. That way, if a device is cracked or otherwise altered, the technology vendor will be able to reach out and "update" the entire set of products in the field.

So your client comes to you. And as I said, your client is probably not thinking to him or herself, "Cool!" The client asks, "What am I supposed to do? Am I liable? What are my rights? Please advise me." So let me talk a little bit about what that session—for which you will be charging several hundred dollars an hour—might look like. Frankly, this is I think an echo of some of what we've heard earlier here today, I'm not principally worried about inducement. Inducement is the least of my concerns advising a client because I actually think I know pretty well how to advise a client on inducement.

If that client has been wise and has secured my counsel throughout the process of developing and launching the product, that client will already have been careful not to say anything stupid in advertising material—not to say anything stupid in instructions or in customer . . . or in other material, and hopefully, that client will have been careful to keep their customer service representatives on a very tight leash so that when the archives of e-mails from customer service to your customers comes out, there won't be anything in there that will be incriminating.

In fact, I've often thought that for a number of technology companies giving up customer service entirely may, in fact, be a sensible thing to do.

[Audience laughter]

After all, these days as a user of new technology devices, I get much better support from user forums than I do from companies anyway. So why not just make that the policy?

So inducement doesn't worry me so much because that portion can be contained. And here actually, I have to somewhat disagree with Professor Elkin-Koren and with some others who have suggested that intent is so scary because it's so amorphous. There is always evidence of intent. My answer to that is, "Of course there is." I'm not going to urge you to try to win on the inducement claim on intent, right? You're screwed, right? You're never going to get out on summary judgment on an intent question.

The way you're going to get out is by demonstrating that you took no affirmative acts to encourage or induce infringement. You didn't actually communicate a message to anyone that encouraged them to infringe. That's something that as a company you can and should be able to control. So inducement worries me not so much, especially if the company's been well-advised from the outset.

Well, now, what about contributory and vicarious liability? What do we do about that? Tony has given a very able description of the substantial non-infringing use standards. I agree with folks who have said the Supreme Court's opinion certainly doesn't give us crystal-clear guidance.

So my question then is "Well, what do you do on that? How do you win on *Betamax*?" Well, I think this client may have some relatively good stories to tell about non-infringing uses. I mean, clearly, a large capacity digital storage technology just like hard drives, just like floppy disks, and blank DVD's, and all the other storage technologies that have come before is certainly capable of substantial non-infringing uses: backing up files, backing up your home movies.

One can imagine there are probably many actual instances of non-infringing uses. I am going to say to my client, "We need to develop evidence and emphasize the authorized uses of this technology," and I'm not going to want to go into court and say, "It's a fair use for you to make backups of your DVD's on this technology, right?" I don't want to have that argument in court. I want to say, instead, "People have lots of home movies. They are backing up their home movies with this product." Clearly, not infringement. I don't have to have a fair use debate.

The authorized uses are the easy ones and the ones that are going to be clearest for you as a client.

So, the question then becomes, well, what is substantial? What does that mean? The MPAA in the hypothetical cease and desist letter described a moment ago, have obviously come forward with what they hope will be evidence that the overwhelming use of your product is for infringement. If they come forward with that evidence, does that get them past summary judgment? Because for you as a small startup company, frankly, whether you win or lose is only distantly relevant. What's relevant is: can the copyright industries drag you through millions of dollars of litigation before you can obtain an answer? They could starve you to death for funding, for example, if you're a venture-funded company, long before you actually get to the final answer.

I always remind people that there has still never been a final judgment in a peer-to-peer file sharing case involving technology. *Napster* was [a] a preliminary injunction case. They disappeared before final judgment was entered. *Aimster*, was the same—a preliminary injunction effectively ended the matter. And even in the *Grokster* case, we have a situation where it was a partial summary judgment—no final judgments. These are very expensive cases to litigate, and the expenses often drive companies out of business before a court is able to render a final judgment. We'll never know if *Napster* or *Aimster* might have prevailed after a trial.

So is the evidence contained in our hypothetical MPAA letter enough to get plaintiffs past summary judgment? The survey, the reporting from Slashdot and other news sources? And how much infringing use is too much? They came forward with a survey that said seventy-five percent of the users surveyed were using it for non-infringing activities—presumably making copies of movies they were not authorized to make copies of. Is that enough? I don't know, how to advise my client on that issue. I would say it's uncertain. We have a three-three-three split in the *Grokster* case. We have a 7th Circuit ruling. The law is unclear.

Vicarious liability, which has been spoken about least so far today, in my view is actually the single most dangerous and frightening doctrine in secondary liability, precisely because that is the theory that the entertainment industries have consistently argued creates a duty to redesign your product. It hasn't been through inducement. In the *Grokster* case from day one, the copyright industries said that the ability to have designed the technology differently should be viewed as satisfying the "right and ability to control" element of vicarious infringement. This stemmed from the irrebuttable fact that P2P software vendors were not able to actually control the activities of end-users, any more than Xerox

can control how its machines are used. The entertainment industry ultimately admitted that this P2P technology does not give you the ability to control how people use it.

So their answer to that was, "Yes, but the reason you can't control what people do with your technology is because you made a deliberate design decision to create a system where you could not control what the user is doing." So the argument is that if you could've designed your product to have control over your users and you failed to do so, you should be deemed to have control of your users.

Where does that leave our hypothetical Storage Co. client? Could the client have designed its product so that it could have asserted more control over what its users did with the device? Well, sure, it could have, right? What realm of possible design options is a court going to look at? You could have designed a very different product. instead of having people have a storage device that sits on their desk, you could've stored a system that stored all that data in a server somewhere on the internet. Had you designed that product, you would've had very good control over what your customers were doing with your product, but of course, that wouldn't look much like what you actually built. Will that be held against you?

My answer is, I don't know. The Supreme Court left vicarious liability entirely unaddressed in the *Grokster* case. The case law below is not terribly clear either. The Solicitor General's brief was kind enough to reject this argument in a footnote. So that's good. I'll cite that if this ever comes up again. The Solicitor General of the United States thought it was crazy. Of course, he came out the other way on the rest of the case. But I don't know the answer.

So here's the point where my client gets frustrated and says, "You're telling me there are no clear answers." The next question a typical business client will ask is, "Well, what is my downside? If you can't tell me whether I'm going to win or lose, tell me what my maximum downside risk is so I can try to build a business sensibly around that risk." And there I'm going to tell my client, "Well, there are three pieces of bad news that I think you should know about. One, statutory damages as was mentioned earlier creates a situation where you would be liable for a minimum monetary amount of roughly seven hundred dollars per work your customers have infringed, if you're found liable."

So you pull out a pocket calculator, you run a few numbers, and you deliver the bad news, "So you'll be liable for . . . let's say you have 400,000 customers each of whom have made at least a hundred copies of works on their very large capacity drives. You're looking at a minimum statutory damage amount of five hundred billion dollars."

[Audience laughter]

Let's do the math. It adds up real quickly. And on top of that, copyright owners have a very easy time getting injunctions. Copyright law has a number of features that favor preliminary injunctive relief for rights holders as witnessed by Napster and Aimster and others who found themselves in this position. So your product could—if we go to litigation—find itself yanked off the market within a matter of weeks depending on the timetable, certainly, within a matter of months, depending on how quickly they file for an injunction.

Now the client is getting very unhappy, and I say to them, "Oh, and by the way, given the nature of these risks, there's no insurance policy in the world that you can buy that will cover these risks. This is not the kind of thing that your insurer is going to be eager to cover. Oh, and finally, in copyright law, we really don't have such a thing as the corporate veil. So they're going to sue you in your personal capacity and come after your house and the house of each of your board of directors personally." And by the way, in the course of this litigation, my fees are probably—depending on the size of your company—going run about a half-a-million dollars a month, for as many years as it takes."

[Audience laughter]

So now my client is saying probably "Okay. We need to call the guys in Hollywood and work something out. Whatever they want, let's find a way to give them what they want because we can't go to the mat on this."

So that, I think, is the scary picture presented by secondary liability in the post-*Grokster* world. It's not inducement that's the problem. It's the rest of the secondary liability, in my view, that is the problem for innovators.

This leads to a few likely implications. First, I think you have to think about the implications that this legal structure has for different kinds of innovators in the market. The Supreme Court didn't know, or perhaps didn't think, that this decision was going to restructure innovation markets. You don't see a lot of that addressed in the opinion. You see some in Breyer's concurrence, certainly, but not in the unanimous opinion. You don't see very much about this.

I would suggest this new arrangement of secondary liability principles creates some very interesting incentives for innovators.

Imagine you're a very, very big company with lots of resources and lots of money for whom a half-a-million dollars a month in litigation costs is not such a big deal. For example, Microsoft. What are your incentives? Well, the problem for you is if you lose on this one product, due to the nature of statutory damages, the odds are pretty good it'll take the rest of your company with it. Any loss in the courtroom is the boat

anchor that takes the whole company to the bottom. So for you as Microsoft, do you really want to bet the whole company on this one new technology? Probably not. So you have very strong incentives to go negotiate with Hollywood. You actually have also better access to go negotiate with rights holders, as well. When Microsoft picks up the phone and calls the people at MGM and Disney and Universal, and wants to sit down and talk about how we should redesign our technology, that call will get answered almost immediately and they can afford to have the lengthy negotiation. And, perhaps if they're thinking strategically, Microsoft may say to itself, "And that gives me an advantage over my smaller competitors, because my large size, and privileged access to the entertainment industries, will allow me to cut deals that the small fry won't be able to cut." And so great, the big guys have incentives to negotiate and perhaps an ability to create new barriers to entry.

On the other end of the spectrum, you have what were earlier called the hackers. The hackers, frankly, don't care. The hackers are individual programmers scattered throughout the world who are going to design the technologies they think are interesting, that people want. Many of them don't know anything about the law. Many of them who know something about the law don't care. Their attitude is, sure fine, sue me. You can have my 10-year-old car and my collection of outdated software, and fine, we're done. Unless you've got a criminal claim against me, you really don't have that much to threaten me with.

So those guys will keep innovating. You're going to see more Napsters. You're going to see more DVD ripping tools. You're going to see more of the kinds of tools that small groups of innovators can create kind of non-commercially as a hobby.

The thing I worry about most is the guys in the middle. If you are a small company, if you are venture-financed, and you want to build a technology at the leading edge like the technology I describe, you are going to have a real bad time of it because your venture capitalists are not going to be thrilled to pony up millions of dollars to do work that could be sued out of existence at whim of the entertainment industries. So that's my view on that.

Now, I will note some interesting counter-examples just to point out that life is more complicated than it first appears. I will note that BitTorrent managed to net eight million dollars of funding after the *Grokster* case came down. Well, now that's sort of interesting. Who are those VC's and what were they thinking? So the uncertainty regarding secondary liability may not dry up all innovation among small companies. Just because the lawyers think your risk profile looks one way doesn't necessarily mean the entire venture community views things the same way.

That being said, I think on the margins, one would imagine more reticence among innovators than would've existed before. I think we have to worry about ways in which case law like *Grokster* creates this distortion in our national innovation policy.

MARGARET JANE RADIN: Thank you. If you folks are amenable, perhaps we could go directly to audience participation so we can hear what people respond to this.

AUDIENCE MEMBER: As a computer scientist, whenever I hear people talking about filters, I cringe, and I hear that Ed Felten will be discussing some of the technological problems with writing filters. But let's just assume for the moment that it is impossible technically or mathematically to write a filter to detect copyrighted material being sent over the net.

This is the process of the law. You might talk about approximations. Well, maybe we can capture fifty percent of it or something like that. Where's the reader in this? That's what I want to know, the technical reader?

[Audience laughter]

FRED VON LOHMANN: Rather than answer that question because I think it's begging for technical rigor among lawyers it sort of answers itself, doesn't it?

[Audience laughter]

If we had to have we would've gone into computing and gotten engineering degrees. But I will say this. I think the focus on filtering is far too narrow. The legal principle that the entertainment industries are seeking here, is not an obligation to filter. That the shorthand with which this concept has been tagged.

Rather than limiting themselves to "filtering," the entertainment industries are really seeking precedents to support their view that technology companies should have a duty—a general duty—to design their products to minimize infringing uses to the extent reasonably possible.

So, if filtering doesn't work, then fine, let's talk about something else. This is why I mentioned revocation and the ability to update the products. Maybe it's not filters. Maybe it's some other mechanism that might work better. So, from the rights holders' point of view, they're not wedded to "filtering" or any one particular solution. They want the technology companies to solve this problem for them and pay for the solution.

AUDIENCE MEMBER: But don't you think that there should then be some discussion of what these things are because when you talk about monitoring, for example . . . ?

MICHAEL W. CARROLL: So, I want to make two points. One, how to answer your question, I think, is really that the entertainment industry wants to get discovery. That is, they want to be able to use a lawsuit to get the information about all of the choices that were made in the design process. The rigor then would be simply what did you look at, what could you have looked at and chose not to look at in designing this? And, I think, Fred's exactly right. It's not really the filtering. It's about what elements of control did you choose to build in? What elements of control did you opt not to include that you could have?

To Fred though, he said, "I'm not worried about inducement, I'm worried about vicarious liability." I think you have to worry about inducement. I think the strategy is to repackage all of the vicarious requirements into inducement and draw with that and say, "I want discovery about all your design choices because I want to see if you have engaged in an intentional act to induce infringement."

So from the technologists' perspective, you want rigor as to whether you made a rational choice or not, but from a business perspective, the business doesn't want to have to give discovery. The business doesn't want to have to litigate that question at all. The *Sony* rule provided a safe harbor that the question of product design wasn't relevant to the legal issue. And if inducement gets developed the way it might, that question becomes relevant and then it's going to change the practice of innovation.

NIVA ELKIN-KOREN: Assuming that no filter is perfect, and that it is absolutely impossible to prevent copyright infringement by technological means, a duty to filter still matters. That is because it affects design and cost. From a legal perspective the question is who should bear the cost: the cost of copyright enforcement, the cost of filtering, the cost of developing preventive measures against infringing materials? That is similar to a duty to comply with DRM's. It does not have to be a filter. The question is whose responsibility it is and who has to bear the cost of implementing technological measure and keeping it updated so it can effectively address forthcoming technological challenges. If there is a duty to filter, regardless of whether it is feasible, then it is likely to affect the type of technologies that would become available.

MARGARET JANE RADIN: Let's say one more jurisprudential thing, too. If the doctrinal issue is could you have readily done this, and you failed to do whatever this is, judges are not very good at figuring that out. Occasionally you get somebody like Judge Posner who is perfectly willing to say judges should figure out what could have been done and they should figure out how much it is going to cost. So they should

be economists. Although Judge Posner's perfectly willing to say courts should do this, that's not a thing which judges are good at.

So when you're talking about rigor . . . you saw a bit of it in the *Napster* case. They called people to the stand and experts in this and said, "Okay, how seriously could you have done something or other?," and the court was ready to give them some leeway on that, but they had lost the case already because it made them go broke. But as Fred was saying, that's the type of stuff that you get into if you have legal documents that make this relevant.

So the whole debate about *Sony* is partly driven by the fact that many people think that you should be able to formulate a legal doctrine that doesn't make so much of that stuff relevant. So, the dangerous thing right now that's out there from my point of view is when you have Judge Posner saying, "Well, I'm following *Sony* because I have to, because I'm not the Supreme Court." But, he re-reads it to make that stuff relevant, then all of a sudden, we're in that phase that you're questioning, I think.

R. ANTHONY REESE: And Judge Posner would be quite happy to say, "Sure, fine. It's not perfectly possible. You can only filter out fifty percent. Great. All we say in *Aimster* is 'could you have eliminated or significantly reduced the amount of infringement activity?' So, sure we'll take into account how effective it is. But if it's possible to do it at some effective level, then you're going to have to run the cost benefit analysis."

FRED VON LOHMANN: I don't think secondary liability in copyright imposes any obligation whatsoever on technology companies to design their technology to do the job of we saying for infringement. I don't think the inducement *MGM vs. Grokster* changes that for companies who don't take affirmative acts that encourage or induce infringement.

As I said, although the entertainment industry has continued to press the same view under vicarious liability, it has so far been rejected by every court to have looked at the argument. So I don't want to concede by any means that the question is simply who pays for the redesign. My opinion is that technology companies should have no obligation under secondary liability to do that. Now, if Congress wants to legislate a regime that requires them to design a certain way, well, then obviously that's Congress's prerogative, but I don't think it should be done via judge-made secondary liability principles.

MICHAEL W. CARROLL: So, if I'm a business person sitting in the audience, I have to say that I would think that there's a whole lot of uncertainty actually about the impact of *Grokster*. I think quite clearly, a difference of opinion, which may help explain why some VC's are will-

ing to fund. Why, we haven't seen more cases yet. So none of that really scared me so much. But what did scare me has nothing to do with *Grokster* because my risk profile was all the stuff Fred started talking about in terms of statutory damages and injunctive relief and personal liability. I want to say that it seemed to me that of all those other legal issues you can always try to find a way to win an argument one way or another. But, when you come up with a risk profile, it's the five hundred million dollars or whatever and the fact that you might take my house that's actually really got my attention. At the end of the day, it doesn't matter how you interpret *Grokster*. If you've got a series of rules that ensure enforcement even before you actually get to the trial then I just can't take that risk, and that's the practical reality folks.

FRED VON LOHMANN: Right after the *Grokster* case came out, I wrote an article in which that was exactly the approach I took. It is critical that we consider the chilling effect that these legal norms can have on innovation. We also made this point in our briefs to the Supreme Court, where EFF was joined in making that point by Intel, the Business Software Alliance, and from sixty law professors. It appeared from the oral argument that the justices also agreed that the chilling effect on innovators is a worry. Then another way to approach the problem would be to fix the remedial structure such that it is not so thermonuclear to people who are in this field. So, I have suggested that one good first step would be to eliminate statutory damages for secondary liability claims. If you can prove that I'm liable, then you also should have the proof that I did you some harm, and maybe I'm liable for that. But that's very different from the kind of statutory damage multiples you see in the existing remedial provisions of the Copyright Act.

Another place I think some sense would be in order is the ease with which these claims can be used to pierce a corporate veil, which I fully agree is incredibly chilling. For those who don't know, the principal investors in *Napster* are still being sued for Napster's activities from 1999 through 2001, and they are being sued in their personal capacity. The word on the street is that lawsuit is all about sending a message to the venture capital community that if you touch these companies, we will come for your house.

R. ANTHONY REESE: Actually, on the worries about statutory damages being reinforced by *Grokster*: although they don't address it directly, Justice Breyer's concurrence does throw out the possibility of a statutory damage award. But of course, there's nothing in the statute that expressly says that statutory damages are available in cases of secondary liability—because, of course, there's really not anything in the statute that says anything much about secondary liability at all. So, it's at least

possible to think that you could have a court that says, "Okay. There are these secondary liability doctrines. That doesn't mean all of the remedies in the statute for direct infringement automatically flow." But the fact that off-handedly an opinion in *Grokster* refers to statutory damages may make that more problematic for the lower courts to do.

KATE GUSMER: We have time for one more quick question before we break for lunch.

AUDIENCE MEMBER: What about the distribution networks? For example, if we're designing things that are hard drive manufacturers, computer manufacturers, software manufacturers along the way, ISP's in transmission. I mean, one also could cover, I think, the whole computer industry. Is there any way to kind of limit it?

FRED VON LOHMANN: That's sort of the driver behind this whole secondary liability debate. Nobody wants to make the entire technology sector liable for every bad act committed by a customer. The harder question is how in the h*** do you draw the line that makes sense? I don't think the Supreme Court did a very good job. I had a view of what I thought a sensible line was that prevailed in the 9th Circuit, but in the end, didn't prevail in the Supreme Court. It's a hard question.

I will note though, the extent to which this debate begins to drive toward a focus on obligations to design and as Professor Elkin-Koren suggests and I think as Judge Posner suggests, these are least-cost-avoider kinds of discussions. Like who in there is it best positioned to most cheaply solve the "social problems" caused by the new technology? That, I think, leads to chilling conclusions when taken to its logical conclusion . . . because the reality is Microsoft is in a better position to solve these problems than anyone. I mean by virtue of having ninety-seven percent of the desktops at its control. ISP's are also incredibly well positioned by virtue of sitting astride the principal distribution channel.

I worry if we start going down this road to find the person who can solve the problem most cheaply, you end up untethering these liability doctrines entirely from a fault-based conception. This is the point in torts, for those of you who remember this debate. It is an old debate in torts. In torts, even though law professors wrote articles urging courts to put the liability on the person who can most cheaply solve the problem, the courts have never adopted that kind of broad conception. And so, I think, there is something we can learn here from torts about why that may not be the ideal option.

MARGARET JANE RADIN: Yes, and you're the last person before lunch, so make it delicious.

[Audience laughter]

AUDIENCE MEMBER: All right. The court describes the *Grokster* software as a device and by doing that was able to sort make a device . . . There's a lot of interdependence and interconnection between the players. And if you think about the *Napster* case—that Napster was a service that rode on top of the growth of public internet and included all of the people who contribute to the provision of that service and roped into that lawsuit.

So, I think, it remains to be seen what the court does when it's faced with something that is much more integrated, much more interactive, and how this inducement standard or the *Sony* standard will play out in that. But, of the many questions the court ducked, I think by characterizing *Grokster* as a device, it managed to leave for another day a lot of questions about interdependent technologies and companies that have those kind of relationships.

SHARON ARMSTRONG: Thank you everyone on Panel One. We're going to take a break for lunch now. We'll be breaking until 1:45.

[Applause]

PANEL II
IMPLICATIONS FOR TECHNOLOGICAL INNOVATION

KATE GUSMER: Good afternoon. We're going to go ahead and get started with Panel Two which is called Implications for Technological Innovation. As you will hear, this panel will discuss the tradeoffs between protecting content owners and fostering technological advancement.

We are privileged to have as a moderator of this panel Professor Susan Kornfield. Professor Kornfield is a partner in Bodman LLP and has been an intellectual property attorney for 24 years. She handles transactional litigation matters involving technology development, commercialization infringement, copyright, trademark, trade secret, and unfair competition, competitive intelligence, conflicts of interest, and post-employment restrictions.

Her clients range from small startup high-tech companies to nonprofit museums and foundations to local corporations. Professor Kornfield is an adjunct professor here at the University of Michigan Law School, and has also taught at Michigan's Ross School of Business and the School of Information. Professor Kornfield has been an expert witness, a mediator and arbitrator in a variety of intellectual property disputes, and serves on an advisory committee at Stanford University on matters involving libraries and active information resources.

Professor Kornfield, I'll turn the panel over to you at this point.

SUSAN M. KORNFIELD: Good afternoon. First I'm going to say how grateful I am to see my current and former copyright law students. I don't have my teaching iPod with us today because we have a panel of true experts, and I'm going to tell you a bit about them and also I wanted to add a personal comment about each.

First, to my left, Edward Felten, who is a Professor of Computer Science and Public Affairs at Princeton, and I think even that name—Computer Science and Public Affairs—is a very interesting title. For those of us who have been following his exploits, we think of him as a folk hero since a few years ago, he received a cease and desist letter from the Recording Industry Association of America he and some of his graduate students were threatened if they were to go ahead and publish and speak on certain information they had determined about security flaws in encryption methods. He's going to talk about a number of issues and, we learned last night that over the last few years, digital rights management technology has merged with the attributes of spyware.

To his left, Barbara Simons, who is an expert on electronic voting. I learned last night that hanging chads are the least of our problems. She's an expert in internet voting. She has worked on matters with the Clinton Administration, with the U.S. Department of Defense. She is the first woman to receive the distinguished Engineering Alumni Award from the College of Engineering at UC Berkeley, and she's a Fellow with the American Association for the Advancement of Science. She's going to talk a lot about security issues and technology issues involved in voting.

And to her left is David Sohn, who is at the Center for Democracy and Technology as staff counsel, and for law students who might wonder what their professional path might be, he started out practicing law at Wilmer, Cutler & Pickering. He went on for five years to advise as Commerce Counsel, Senator Ron Weyden, and he joined the Center for Democracy and Technology last year.

And I know that all of you read the front page business section of the Ann Arbor news last night and there was David's group, the Center for Democracy and Technology is employing a new technique in its fight against software service. One of the solutions and to skirt pop-up advertising—public shame. So he's going to talk about the use of public shaming, perhaps, as an aspect of the technology management.

So we're going to turn it over to Professor Felten first.

EDWARD W. FELTEN: Thanks. About six months ago, Alex Halderman, a grad student who was working with me discovered something really interesting. He discovered that certain compact discs from Sony BMG, the world's second largest record company, installed on people's

computers a piece of software that is generally known as a rootkit which inserts a kind of security hold into the computer.

This was part of a longer ongoing investigation of the latest generation of CD copy protection technologies that Alex has been working on for about the last year. When Alex discovered this, we thought it might be pretty important and we thought it was certainly very interesting. So we did what we always do when discovering something important in our copy protection research. We called our lawyer.

[Audience laughter]

In fact, lawyers were involved in the planning and design of this research program from the beginning. We went right away to our University's general counsel, we talked to other people outside the University trying to figure out what we could do safely in this area; trying to figure out how we should structure the research program; which kinds of experiments were safer to do than which other kinds, and so on—whether we had a path to publishing the information at all once we found it.

And, in fact, after discovering this, we spent about a month talking to counsel at different places, talking to our University's general counsel, talking to people at the Samuelson Clinic at UC Berkeley, and talking to others, some of whom would rather not be named.

And while we were talking to counsel and deciding what we could do about publishing this information about how millions of consumers were being put at risk by this seemingly harmless product. While we were doing that after about a month, someone else discovered the same thing and not being experienced in the field, just went ahead and published it.

This opened the floodgates that ultimately led to a bunch of revelations about what Sony was doing. To cut to the end of the story, we eventually, after this information had come out, and after it became clear that we were not going to face litigation and so forth or indeed threats from Sony and others, we went ahead and we wrote an academic paper describing all of what we had found which is now available on our website.

And if you flip to the end of that paper and look at the acknowledgments section, you see that we acknowledge a number of computer scientists for their helpful advice and comments on the paper. We then proceed to acknowledge a larger number of lawyers for legal support. In fact, it's become a fact of life in this area of research that if you're going to do work, if you're going to be talking to lawyers from day one, for every two hours you spend in the lab, you're going to be spending about

an hour dealing with the legal implications of what you're doing, making sure that you stay clear of the possible negative consequences, and so on.

It's also a fact of life that when you write the paper describing the research you have done, that you will leave certain things out. You will self-censor up to a point in order to make your legal position stronger should anyone act against you. And, I can say that of the papers that I have written about copy protection technology, there's really only one that did not involve at least some modest degree of self-censorship in the writing of the paper, and that ironically, was the one that was described before which led to a threat to sue us and ultimately a federal lawsuit.

This was a paper relating to the secure digital music initiative and the watermarking technologies that they were thinking of deploying. So the story is that we wrote the paper and we left out some things and we wrote it sort of carefully to try to reduce our legal exposure. Then they threatened to sue us anyway. So, as long as they were threatening to sue us, we figured why not put all that stuff back in?

[Audience laughter]

If we put that stuff back in, there would be a declaratory judgment action to try to put the issue before the court. So, ironically, the only paper that we ended up publishing with which we haven't self-censored at least a little in this area was the one that actually did involve federal litigation.

Many of my colleagues in the computer science research community and computer security research community just won't put up with this stuff. Many of them say they're allergic to lawyers. They don't want to have to learn what's in the DMCA. They don't want to have to meet with their general counsel. They don't want to have to understand what the case law is. That's not why they went into this field. So to a large extent what had been a reasonably robust research effort in this area has now shrunk down to relatively few people who are willing to put up with it.

This is a very real story about the impact of this area of the law and technologists, and the people to look at are not the people like me who are just too stubborn to get out of the area. It's the people who are not there—the students who are not studying this area because they are worried and they just don't want to put up with the hassle.

Now we heard this morning about the *Grokster* case and we heard some very nice analysis and reading of the Supreme Court's opinion. Questions about what the rules are and so on. It's worth also saying that it's not just a question of where the legal boundaries are. Questions of politics and public relations, in fact, matter as well. And I should tell you that before we publish a paper, we don't just call our lawyer. We also call our university's public relations person, and we learned to do this be-

cause we found that occasionally, we would publish a paper and some congressional staffer would call her up and yell at her about why was the university letting their people do this terrible thing. So we learned that we needed to send her a copy of the paper in advance and have a little phone conversation so she'd be ready to answer those questions. And now that's again a regular part of the process that we go through before we publish a paper in this area.

Because, in fact, even if we're careful about the legal factors and we make sure that what we do is absolutely lawful, we can still cause trouble for ourselves and for the rest of our community if we do something that can be painted as harmful; can be painted as something a hacker would do. And so in order to work in this area, you have to be quite careful, and intellectual property law and regulation and sort of the penumbra of politics and public opinion that have grown up around it are certainly limiting factors.

It's worth thinking, I think, about how things got this way, about how what ten years ago would've been considered absolutely mainstream computer security research is now something that some people consider legally edgy and people suggest that we're somehow rebels to be doing this. This is, in fact, mainstream stuff in our scientific community, and the papers that we write are, when they're good, published in the most mainstream and stodgy of research venues.

Part of the problem, I think, that has caused intellectual property to reach so far is something that I call the regulatory rationale. This is the idea that it's the job of law and regulation to stop infringement. Therefore, if infringement is still going on, the problem must be that the law doesn't reach far enough. And the solution being to increase the scope and reach of intellectual property law and to continue to do so until infringement is halted. Given that law is not really in a position to stop infringement in today's world, this is a recipe for increasing overreach.

There's also a technical version of this rationale which says that as long as infringement is going on, the solution must be to develop and deploy technology that reaches farther; technology that's more intrusive in an attempt to stop it. And this is part of the story that led to the Sony CD copy protection technology that I talked about before which did really quite astonishing things in reaching into people's computers: ejecting security holds, installing software without consent, and so on.

A lot of this was the attempt by the designers of this technology to do more when they found that the technologies that they had designed so far were not going to solve the problem. And in fact, given that technology is not going to solve this problem, this also is a recipe for stepping farther and farther over the line until you get into trouble. Because if

you're going to regulate in this area or you're going to design technology in this area, you have to base your strategy on a realistic understanding of what it is that the regulation of the technology is actually trying to prevent and what it's possible for it to do. It's not necessarily the case that the failure of law or technology to achieve some result means that more law or technology is required.

And on this particular topic, there's an enormous disconnect between the policy makers and technologists. I mean, there's always some kind of disconnect between scientists and technologists on the one hand, and the people who are making policy relating to that science and technology. That's sort of just a fact of life.

Whenever there are two different communities talking about a topic, there's going to be some level of disconnect. But here, the level of the disconnect is astonishing in the sense that assertions about technology which are considered laughable in the technical community are not only considered respectable, but are actually considered true beyond dispute in some policy discussions. It's quite amazing.

For example, in the computer science research community, the idea that any technology could have a meaningful impact in reducing peer-to-peer file sharing is almost considered a crackpot view. That is a topic which has been well discussed over the years, and the debate over that is essentially over. No one would seriously get up on the podium at a computer security research conference and claim to have a technology that would stop people from file sharing. It's simply not as bad as, but in the same category as arguing, that the earth is flat at a geology conference. It's simply an outrageous view.

Nevertheless, in policy discussions, it's often taken for granted that it's reasonable to expect technology to make a significant dent in this problem. And we saw this in the *Grokster* discussions and in the Supreme Court's opinion. As we heard this morning, the opinion of the court asserted that the lack of filtering in the design of the *Grokster* technology was evidence of inducement. That this is essentially a finding that a reasonable technologist who actually cared to prevent infringement, would have, gone down the road of filtering.

Now, the interesting thing about this is that the court really did not have much in the way of evidence to base this on. What they had were a few friend of the court briefs from companies that sell filtering technology arguing that the court ought to require technology like theirs to be bought by the people like *Grokster* on the one side.

On the other side, you had a brief by seventeen computer science professors including some of the real giants in the field like David Clark, who's considered as much as anyone the father of the internet, saying

that filtering is not only unproven technology, but unlikely to work if it were tested. And also arguing that a well-intentioned engineer could rationally choose not to pursue filtering given that it was unproven and unlikely to work.

Now the interesting thing is that in discussing it essentially is saying that, *Grokster* should have filtered. Not only did the court disagree with the brief of the computer science professors, it didn't even bother to mention it. Imagine if you will, that seventeen distinguished economists had filed a brief asserting that as a matter of economics, something was true. And then imagine that the court had asserted the opposite and not even sort of mentioned or explained away why the economics professors were wrong. You wouldn't expect that. And the most disappointing aspect of the *Grokster* decision really, to many technologists, was that the brief of the computer science professors was more or less ignored.

It's also interesting to note what the court said about filtering because, if you read it carefully, what the court said was this. This is from page 22 of the *Grokster* opinion. "Second, this evidence of unlawful objective (that is objective to induce infringement) is given added significance by MGM's showing that neither company," (meaning neither Grokster nor Streamcast), "attempted to develop filtering tools or other mechanisms to diminish the infringing activities using their software." The court is talking not about whether these companies made a rational decision; they're essentially criticizing them for not trying to develop filtering technology that would work.

To me it is very interesting that it's the lack of effort rather than the lack of—even of deployment of the technology that might work—that the court is criticizing. It's as if it's unknowable, whether filtering technology would work and the companies had an obligation to try and find out.

And we see this kind of disconnect in a lot of the policy discussions that go on where copy protection or infringement fighting technologies that are as a technical matter just dead on arrival are promoted as solutions and are proposed as mandatory.

We see this in the broadcast plight, for example, and the technology which really is as a technical matter completely dead on arrival. Nevertheless, there are serious proposals to mandate it, and as a result of this disconnect, a lot of people in the technology community, a lot of researchers and educators have simply sworn off the public discussion on this matter saying that folks in Washington are just too clueless to, to even talk to, and that's, I think, a very disappointing result. There are some of us who have not given up talking about it, but nonetheless, I think this disconnect is a very serious matter unless—and unless this

changes, we're going to I think continue to have pretty bad policy in this area. Thanks.

SUSAN M. KORNFIELD: Barbara Simons.

BARBARA SIMONS: I'm going to talk about a slightly different topic. As you said, I was for many years working in copyright and database directive. When Pam was writing about some of the crazy pre-DMCA proposals, USACM (the U.S. Public Policy Committee of ACM—the premier Society of Computer Scientists) was addressing computer related policy issues such as the anti-dissemination provisions of the DMCA. We were saying that the DMCA would criminalize some computer security R & D which, in fact, it technically does.

I thought I'd tell you an interesting little story. As many of you know, the anti-dissemination provisions of the DMCA were delayed until the year 2000. A few years ago when I was in Washington, I discovered that the reason for this delay was that people knew about the Y2K problem. They realized that some of the reverse engineering and other work that needed to be done for Y2K would technically be illegal under the DMCA. So they delayed the implementation of the anti-circumvention and anti-dissemination provisions until 2000. The fact that the Y2K problem is not the only computer related problem that might require reverse engineering somehow didn't dawn on the folks who drafted the DMCA.

One of the things I'm hoping to accomplish is to convince some of the folks here that voting machines, voter registration, and other aspects of voting are of great relevance to this community. Of course attacks on fair use and first sale, combined with all of the efforts to restrict speech, are very important and deserving of attention. But if our votes are stolen or lost or manipulated, then the game is over. When you start studying technical and legal issues relating to computerized voting, you find yourself in an Alice in Wonderland world where common senses and technical expertise become irrelevant.

The testing of voting machines is a joke; the rules relating to the testing are a joke; and the oversight of testing and machines is a joke. But today I'm going to focus on the legal aspects of voting and voting machines. If you have questions about the other areas that I'm skipping, which of course are very important, please ask me during the question period or afterwards. I'll be around all day.

The Help America Vote Act (HAVA), passed in 2002 as a result of Florida 2000 and Florida 2002, allocates almost four billion dollars for states to upgrade their voting systems. HAVA also mandates that (all) people with disabilities should be able to vote independently by 2006 or 2007. There is some ambiguity.

I support the idea of providing accessible voting systems for people with disabilities whenever possible. (Some people may be so seriously disabled that there is no way using current technology that they can vote independently). But the 2006 or even 2007 deadline for providing systems that allow people to vote independently is a serious problem, because there is far too little time for the research, development, and testing needed to develop new voting tools. 2006 is also the HAVA-mandated deadline by which every state must have a statewide database of all registered voters. At least 20 states don't yet have the statewide databases. There are no rules, no regulations, and no standards for the databases. I would bet a lot of money that in November 2006 you are going to see massive meltdowns when these databases don't work.

If anyone is interested in problems relating to statewide databases of registered voters, USACM has just produced a report that contains 99 recommendations, all quite obvious when you think about them. The full report or just the list of recommendations can be downloaded from http://www.acm.org/usacm/VRD/. The report contains recommendations that I'm sure most election officials haven't even thought about, such as the need for good audit trails, so that it's possible to determine who made particular changes. Is anyone here from New York?

AUDIENCE MEMBER: Yes.

BARBARA SIMONS: I don't know if you know about this, but there was a ruling yesterday by a federal judge that gives the State of New York until April 10th to come up with their plans for implementing the statewide database and for purchasing voting machines. New York doesn't have anything yet, and they have until April 10th to devise a plan. As a result of a lawsuit by the Department of Justice, many groups, such as the New York State League of Women Voters, are concerned that New York State is going to be forced to purchase really unsafe, insecure voting machines because of time pressure from the DoJ.

There are some huge problems with many of the voting machines, including secret software, secret testing, secret test results, and no possibility of a recount or an audit of the paperless Direct Recording Electronic (DRE) voting machines that are being widely used in this country. Voting machine vendors have been retrofitting DREs with paper that is supposed to make a record of the voter's ballot that the voter can either accept or reject. This is called a Voter Verified Paper Ballot (VVPB) or Audit Trail (VVPAT). Unfortunately, really bad engineering has been used to retrofit the DRE's. The continuous rolls of thermal printer paper that vendors added to the DREs have created a whole new set of problems.

Because votes are stored consecutively on the continuous rolls, there are privacy concerns. There are also problems with storing the thermal paper so that it doesn't fade, such as can happen with the receipt you get from the gas station.

There are also serious concerns about how to conduct audits and recounts. You want to count ballots the way we count money, by sorting the ballots into piles according to the vote and then counting each pile. This can be done very publicly, very visibly. Unfortunately, with continuous rolls of paper someone has to read the information off the paper roll and someone else has to record what was just read. It's a really bad system. If I had wanted to design a system to make recounts as difficult as possible, I might have chosen a continuous roll model.

While some states have good voting laws, many states do not. In some states, it is almost impossible to get a recount or to conduct an audit. California has a very good law that mandates that one percent of all precincts randomly selected be recounted for every election. Such an audit is one way to check on some of these voting machines.

Amazingly, when California allowed paperless voting machines, the audits were conducted by first printing out copies of the votes from the computer's internal memory and then manually counting the print-outs. This is a joke, because there is no way to know if the results stored in the internal memory accurately reflect the will of the voters. Fortunately, in California we now have a law that no longer allows paperless voting machines. Unfortunately, many California counties will be deploying badly retrofitted DREs. The only positive thing you can say about the retrofits is that they're better than DREs without retrofits. At least there is the possibility of a recount.

I'm going to quickly review some interesting legal stories to try to whet your appetite without going into much of a discussion about overall voting machine issues.

An illustrative example from the 2004 election of how the law has not kept up with technology is what happened in Carteret County, North Carolina. Carteret County used a paperless DRE for early voting. Unfortunately, somebody forgot to change the capacity of the memory. After 3,005 votes had been cast on the DRE, the rest of the votes went into a black hole.

Now losing votes is never a good idea, but in this case it was especially disastrous, because over 4,500 votes were lost. There were no records of the votes, because there was no paper backup. Furthermore, there was a statewide election—in this case for Agricultural Commissioner—where the difference between the two candidates was less than 4,500 lost votes. So, what to do?

First, the State Board of Elections ordered a revote for Agricultural Commissioner to be held in Carteret, County. That was thrown out by the courts. Then, the Board of Elections ordered a statewide revote. That, too, was thrown out also by the court. Finally, the leading candidate obtained 1,352 affidavits from people who swore that they had voted for him and their votes hadn't been counted. Since it looked like the judge was going to accept the affidavits, the losing candidate conceded. That's how the election was decided.

What happened in Carteret County is an example not only of problems with voting machines, but also of inadequacies of our election laws. There is no law in North Carolina to deal with a situation in which paperless voting machines lose a significant number of votes. A legal problem with rerunning an election is that the people voting the second time will not necessarily be identical to those who voted the first time. So, how do you resolve this mess?

I'm going to discuss Diebold in the time I have left. I don't mean to say that Diebold is especially worse than any other vendor. We are, however, very grateful to Diebold because Diebold has been of the poster child for everything that is wrong with DREs. But I want to emphasize the fact that most other vendors' machines have not been subjected to the kind of scrutiny that Diebold DREs have received. The lack of scrutiny does not give us confidence that other vendors' machines are any better than those produced by Diebold.

Diebold became famous in part because Walden O'Dell, the then CEO of Diebold's voting machine division, said in a 2003 letter sent to Ohio Republicans that he was committed to helping Ohio deliver its electoral votes to the president next year.

[Audience laughter]

So some Democrats woke up and said—

[Audience laughter]

—"My goodness, this doesn't look good. If he can manipulate the voting machines, he could swing the election."

On February 2003, shortly before the O'Dell letter, a journalist named Bev Harris found Diebold software on an open FTP website and downloaded it. Among the files she found was one called Rob-Georgia. Some people assumed that Rob-Georgia was related to 2002 when the entire Georgia election had been conducted on Diebold paperless DREs, and the major Democratic candidates all lost. That's when Senator Cleland lost, although he was favored in the polls. The governorship of Georgia also was won by a Republican for the first time in many years. However, it turns out that a programmer named Rob Behler was working on the Georgia file.

Bev Harris also learned that there were last-minute software patches being put onto this software before the election. This is completely illegal. These machines are supposed to have been examined and tested, and only the software that was examined is supposed to be used in an election. However, because of their last minute nature, there was no testing done of the software patches. So in fact nobody can say for sure whether or not malicious code might have been inserted into the machines which self-erased afterwards. And no one can prove by a recount or audit that Sen. Cleland was actually defeated, because there is nothing to recount.

The story continues with Avi Rubin, a computer science professor at Johns Hopkins, being given the software by Bev Harris. Rubin, together with colleague Dan Wallach and graduate students Tadayoshi Kohno and Adam Stubblefield, wrote a paper based revealing many security vulnerabilities in the Diebold software. Now what's interesting is that the Hopkins scientists first had to consult attorneys, in this case the folks at EFF. Furthermore, there was a file that the researchers did not examine, because it was encrypted using a key that was available on the Diebold website. The researchers were concerned that if they viewed the file, even though the key was easily available, they might be in violation of the DMCA.

The *Hopkins Report* exposed some very disconcerting security flaws in the software, including a hard-wired key that was used to encrypt all the data on the storage device. If you could access one of these machines and you knew this key, which incidentally was F2654hD4, you could have manipulated the election.

[Audience laughter]

While Rubin and his colleagues analyzed Diebold software security in 2003, in 1997 a computer scientist name Doug Jones, who was also on the Iowa Board of Examiners for Voting Machines and Electronic Voting Equipment, had warned Diebold against hard-wired keys. Yet, in spite of the advanced warning Diebold had received, they had not changed their software. In fact, the man with whom Jones talked had never even heard the phrase "key management." These are the people who are running our elections. (A subsequent analysis of security problems with Diebold software, the *RABA Report*, revealed yet another case of identical keys).

Diebold's response to the *Hopkins Report* was to deny that the code had ever been used in an election. However, there was a wired news article that appeared on August 4th, 2003, in which a Diebold spokesman Mike Jacobsen "confirmed that the source code Rubin's team examined was last used in the November 2002 general elections in Georgia, Maryland, and in counties of California and Kansas."

It's interesting that on August 11th the Jacobsen quote was modified retroactively. If you look up the article on-line, you will find the more cautiously-worded phrase that says that the code examined by Rubin et. al. "on the whole is not the same" as the production code. The careful rewording suggests that, except for minor changes, the code examined for the *Hopkins* paper was essentially the same software used in the elections.

The State of Maryland was about to buy Diebold voting machines for the entire state when the *Hopkins* report came out. Maryland delayed the purchase and commissioned another report from SAIC. When the *SAIC Report* was released, two-thirds of it was redacted. Attempts to obtain a copy of the redacted portion via public records requests have failed. That's an area in which I'd like to see the legal community get involved. By the way, the *SAIC Report* was redacted by the State of Maryland, not by SAIC. In fact, the *SAIC Report* concurred with the *Hopkins* study. In the unredacted portion, the report refers to Diebold by saying "the system as implemented . . . is at high risk of compromise." So you can only imagine what was contained in the part that was not released.

In spite of some very negative content in the unredacted portion of the *SAIC Report*, Maryland and Diebold claimed victory. Maryland bought the machines, and then the *RABA Report*, which was also negative, came out. Each time a new negative report was released, Maryland election officials and Diebold have said, "Well, we'll fix it; everything's fine." But every new study that's done of Diebold code, every new examination, finds more problems.

In 2003 there was another interesting intellectual property dispute that relates to the DMCA. In the summer of 2003, a hacker broke into Diebold website and obtained e-mails dating from January 1990 to March '03. The e-mails, which were quite damning, were originally posted by Bev Harris on her website. While refusing to acknowledge that the e-mails were theirs, Diebold forced Harris's ISP to remove the emails because of copyright violations.

So of course the e-mails popped up elsewhere. One of the places they were posted—by a group of undergraduates—was Swarthmore College. Predictably, the college received a threatening letter from Diebold demanding that the e-mails be removed. Again, Diebold did not acknowledge that the e-mails were theirs. Rather, Diebold said that they were going after the emails because of copyright violations. Perhaps someone could explain the legal logic to me afterwards. I still have trouble understanding it.

The college removed the e-mails, but that did not solve the problem for Diebold. Instead, e-mails were posted on at least fifty college and university websites and even on a high school website.

In November, 2003 the Swarthmore students announced they were bringing suit against Diebold for abusing copyright law and that EFF was handling the suit. On December 1st, Diebold withdrew their complaints against everyone who posted the e-mails on a website. That happened around that time that representative Dennis Kucinich posted links to the emails on his website.

So, here's another question I have. Can you go after a member of Congress under DMCA violation?

PANELIST: Yes, you can.

BARBARA SIMONS: —You can?

PANELIST: So long as he doesn't shout out the URL on the House Floor.

[Audience laughter]

BARBARA SIMONS: But if he doesn't, okay?

PANELIST: He's okay if he does that.

BARBARA SIMONS: Okay. In October 2004 the U.S. District Court for the Northern District of California ruled in favor of the students, and Diebold had the honor of being the first company found in violation of the DMCA. Diebold was fined $135,000 damages and fees. Is Diebold the only company to have been found in violation of the DMCA? I don't know, but it's certainly the first.

Next I want to talk to you about Alaska, because there were some bizarre occurrences there in the '04 elections, held on Diebold voting machines. For example, in some districts the reported voter turnout was more than 200 percent.

[Audience laughter]

A district by district tally of the totals for Bush resulted in a total of 292,267 votes. But the official total was only 109,889. So there seemed to be a bit of a discrepancy.

That made the Democratic Party curious to see what was going on. They made a public records request to get the election database. Initially, the State Division of Elections refused to turn over the electronic voting files to the Democrats, arguing that the data format belongs to a private company and could not be made public.

Diebold claimed that it owned the structure of the database. Although the data is public, the company claimed, the format is a company secret. (Meanwhile, the format was available on the Web, where it had been posted by activists). The Elections Director supported Diebold by

saying that the state contract with Diebold forbade the release of the data.

Because there was a lot of bad press, Diebold subsequently waived their claimed rights. However, Diebold cautioned that there was sensitive information in the files, including encryption passwords, users IDs, and phone number used to load in the results. "Therefore, in order to provide the specific information you're seeking in the specific form requested, the Division," (this is from the Alaska Election Officials), "the Division is looking into the feasibility of changing the encrypted information as well as changing the voter numbers for future elections." Well, I'm not quite sure what all that's about.

So the state continued to delay, even though under Alaskan law they had 10 days in which to provide the files. Initially, the files were supposed to be released by January 4th. Then the deadline was extended to January 19th, when the proprietary assertion was made. Next, on February 3rd Diebold said they waived their rights, and the deadline was extended to February 27th.

On February 27th, the chief security officer of Alaska refused to release the data because, "Release of any security-related information creates a serious threat to our ability to ensure confidentiality, integrity, and enable the leave [sic] of our systems and services."

So from what I can find out right now, the Democratic Party of the State of Alaska is currently deciding whether to file a lawsuit or to make an administrative appeal of the denial. [Note: After filing a lawsuit, the Alaska Democratic Party finally received the voting database in September 2006. The Democrats claim that audit logs in the database were accessed as recently as July 2006. They are now trying to obtain a copy of the database as it existed just after the 2004 election.]

I only have like a minute-and-a-half, so I'm going discuss Florida really quickly. In 2005, Ion Sancho, who was the Election Supervisor of Leon County, Florida, invited Harri Hursti to test the security of Diebold precinct-based optical scans voting systems. Hursti had a copy of the Diebold software and other documentation that had been downloaded in 2003. Hursti discovered some serious security flaws that he was able to manipulate to produce false election reports.

Optical scan voting systems use paper ballots, but if you don't look at the ballots after the election, if you depend only on the election reports, which is what many states do, then you can manipulate the election reports to steal an election. That is because elections are not routinely audited in most of the country. What happened was that Diebold, which had a contract with Sancho, refused to deliver the machines. Since there are only three vendors certified to sell voting machines in Florida,

Sancho then attempted to purchase machines from Sequoia. Sequoia initially agreed to sell machines to Sancho, but they backed out of that agreement on January 1st, 2006. Sancho then attempted to purchase machines from ES&S. They also subsequently refused to sell machines to Sancho.

Now, Florida is threatening to take back the HAVA funding from Sancho, because he has not satisfied the HAVA requirements and has not obtained machines by the 2006 deadline. Meanwhile, no company that can legally provide Sancho with voting machines will sell them to him. Consequently, Sancho has instituted his own lawsuit for breach of contract against Diebold.

There are a lot more interesting happening in Florida and elsewhere, but I've got to stop. It's a crazy situation, replete with legal issues. We really need your help. We really, really, really need your help.

SUSAN M. KORNFIELD: And here to help her is David Sohn.

[Audience laughter]

DAVID SOHN: Well, I'm a member of an organization called the Center for Democracy and Technology. I guess I'll start by saying a couple words about who we are. We're a nonprofit public policy organization. We characterize our mission as defending and promoting civil liberties and democratic values on the internet which means we get involved in issues like free expression, privacy, as well as some of that stuff that we see happening on the internet like spyware and the article that Susan mentioned in the newspaper that has to do with some of our efforts to expose companies that are advertising with spyware/adware providers.

We're Washington-based, so we try to be engaged and provide a public interest voice in some of the technology policy debates that are going on in Washington in front of the government.

I thought what I would do is two things. Basically, talk a little bit about our general approach to the issue of copyright and how copyright protection relates to innovation and the internet, and then offer a specific example of one case where we looked at government intervention in a particular instance and tried to document the impact that had on innovation.

So, our general approach. First we do think that rampant infringement is a real problem. We don't want to see an internet that's characterized by an accepted practice and culture of mass infringement with little to deter it. There's a couple reasons for that. One, certainly, is that copyright is supposed to give an incentive for creation, and we take that seriously. It's a problem not just for the large media companies that are often the face of this debate. More and more on the internet, smaller

players are able to use digital technologies to make types of creative works that they probably couldn't have made previously, and to find ways to disseminate them. And so the community with some interest in copyright not being overrun by the internet is actually pretty large.

But even setting aside the incentive issue, it does seem to us that if copyright infringement does just become widespread and rampant on the internet and there's not much to check it, the kind of responses that we're going to see to try to keep it under control (and we already do see some of this) are very dangerous. I think they fall into a couple main categories.

The first category is the kind of response that the copyright holders themselves might take. They may try to limit the delivery of content to closed systems or devices and electronics boxes that don't connect to the internet, and therefore, don't take advantage of all the neat things that the internet can do.

They could achieve to some extent the same effect by trying to use really, really restrictive digital rights management technology. There clearly are questions of DRM's effectiveness, but as you know, it certainly is the case that when content owners use digital rights management technology, they're backed up by the legal hammer of DMCA. So that is a powerful tool that they have.

In our view, if they use that tool extensively, they are certainly swimming against the tide. There's no question that consumers want to be able to get the flexibility and the types of uses that the internet and digital technologies permit. And, if companies try to stymie that at the outset, the practical result is probably going to be to drive people to more infringement. That just creates a cycle that basically fuels the problem.

The risks that we see there—if content owners try to only release content in ways that are narrowly locked down—the risk is not just that consumers don't get the kind of uses that they want. There's a real innovation impact as well because an awful lot of innovation that we see around the internet has to do with companies figuring out interesting and exciting new ways that people can use and manipulate content. Things like MP3 players and podcasting. Someone this morning mentioned the Slingbox as a new technology that lets people enjoy their televisions in a different way. It's a really fertile field for innovation. But certainly if content owners are trying to release content only in ways that are narrowly locked down, you have a real possibility that you preclude uses that people haven't dreamed up yet, and you prevent innovators from figuring out new devices and ways to use that content.

The second category of response—and the one that we probably focus on the most, being in Washington—is government responses. And there's a variety of types of possible government responses. The most obvious one is technical design mandates where the government will basically try to mandate the inclusion of specific technology solutions designed to fight piracy.

We think that trying to lock in specific technology approaches at the government level is certainly a bad idea. It's not helpful for innovation. Closely related to that would be government efforts to not necessarily mandate a specific technology solution, but rather to give the job to a government agency—say, the Federal Communications Commission. (I cite the FCC because there's a specific example of that, which I'm going to talk about at the end.) But basically, give a government agency some sort of gatekeeper role where it gets to scrutinize new technologies coming onto the marketplace and see if they look like they incorporate sufficiently strong technologies to achieve whatever kind of content protection the government has deemed appropriate. Also a very bad idea for innovation.

There are other kinds of government responses. One, certainly, would be overbroad secondary liability. There was a lot of discussion this morning of *Grokster*. Before the *Grokster* decision came down, Congress was debating a possible legislative effort to flesh out secondary liability and to try to create some kind of inducement standard.

CDT was participating in those talks and was not at all happy at the time with the direction things were going. And I note Professor Samuelson said that had *Grokster* come out the other way you probably would've seen this issue back in Congress and again, possibly gotten a very bad result out of that. I think that's exactly right. There's certainly some benefit to clarity, but having worked on some of those talks during the congressional efforts to define inducement more clearly, it really didn't seem like the kind of standard that was going to come out of any legislative negotiation there was going to be as good as what the court did.

So those are the risks that we see. I guess the way that we would like to see copyright policy proceed—basically, an approach to try protecting copyrights without having these negative impacts on innovation—would involve three main things.

One certainly is enforcement against infringers. So that means things like the lawsuits, frankly, that the content companies have been pursuing against infringers. We think those do have some deterrent effect. They definitely send a message about infringement being a problem and some-

thing that isn't just okay. It's obviously important to target that kind of behavior.

We also think secondary liability is an important tool. So in working out the balance with *Grokster*, we certainly want to protect innovation, but also need to have a rule that when a company really is purposefully taking steps to promote infringement, that does seem like the appropriate case to have some enforcement possible. Congress has actually gone a long way down the road in providing all sorts of avenues for enforcement. So this is not an area where we see a lot of need for new legislation. Just back in 2005, Congress passed a law creating tough new penalties for camcording of movies in movie theaters and for infringement of pre-release works. So there has been this constant addition of new tools to the enforcement arsenal. The tools are basically there, but certainly enforcement on an ongoing basis is one thing that we think can productively be done.

The second thing—and this is probably the most important of all—is that the industry has got to roll out legitimate online services. Legitimate online distribution of content that is attractive enough and convenient enough and attractively enough priced that it can really convince people to go ahead and use those legal services rather than trying to engage in piracy. And iTunes has led the way here, showing that if you offer an appealing enough product, you actually can compete with the peer-to-peer networks and infringement options.

I think it's fundamental to all of this to recognize that the ability of consumers to obtain infringing material on the internet is not going away. It's here to stay, and none of this effort is ever going of put the infringement genie entirely back in the bottle. But the goal has to be to have both a sound legal structure for enforcement against infringers, and legal options for obtaining content without infringing.

And the third thing, I'm not going to say much about, but I'll just say that it's public education—to send a message that infringement is a problem that society takes seriously.

The goal would be that with the right balance of those three things, you try to make infringement relatively unattractive and you keep the level of it manageable. If you try to set a more ambitious goal than that of preventing all infringement or coming up with technology that's going to end all infringement, it's never going to succeed.

So let me just turn quickly then to the specific case I mentioned. Ed, I think, mentioned the broadcast flag. He didn't say much about it, so I'll say what it is. He also referred to it as a technology that's dead on arrival. I'm not going to get into the technological aspects of it so much as the procedural aspects. But basically, the idea here was that movie companies

and other content companies are concerned about piracy of television programs—that people will copy programs off TV, particularly as TV goes digital; upload them to the internet; and leave television facing the same kind of piracy problems as music faces.

So the idea that they came up with to try to stop this was to have something called the flag. The flag itself is just a marker that would be attached to the programs that the broadcaster is sending out over the airwaves. And the marker would basically mark the content as something that is supposed to be protected. The hard part is, how does downstream technology—the TV receivers and the other devices—how do you ensure that these devices know how to treat the marked content? Well, the answer under this scheme is that you have the Federal Communications Commission basically serve as a gatekeeper for technology and say that they have to approve television receiving devices and that those devices, in order to get approval, have to show that they have some way of preventing flag-marked television programs from being uploaded and distributed on the internet.

The FCC went quite a ways down the road of doing this scheme but ultimately got struck down in court. The court ruled the FCC didn't have authority to do this. But the issue is very much live; it's back before Congress, and there is some substantial support in Congress, so this could come back. What CDT did was we took a careful look back at what happened during the FCC's process, and the interesting thing that we found was this. The FCC had an initial round where it looked at technologies to comply with this flag regime. Thirteen applicants came forward. All thirteen were ultimately approved.

So in a lot of ways, we feel like from an innovation-friendly perspective, the FCC could've done a lot worse. They actually weren't rejecting technologies left and right. They actually approved everything that came their way. Even so, when you take a careful look, four of the thirteen applicants had proposed a technology that had pro-consumer features that really should have been perfectly permissible under the scope of flag regime as it was set out. What they basically proposed was to provide a secure way for people to transmit a flagged program over the internet to a limited number of recipients. So you could send it from your home to your office, for example.

That was opposed by the content industries who said that they thought there should be a localization requirement—in other words, that the flagged content really shouldn't be able to transmit anywhere outside your immediate home network. What ended up happening during the course of the process was that once it drew strong opposition from the content companies, three out of the four technology companies that had

proposed the feature elected to withdraw it and basically imposed a localization requirement—the design specs of which were drawn directly from a memo that MPAA had provided to them telling them what they wanted.

It's understandable from a business perspective why the companies might have done this. The process was fairly uncertain. They weren't really sure how the agency was going to rule on this new technology. They were worried about the delay in getting their main product out to market. But the end result is that in three out of the four cases, they withdrew this consumer-friendly feature that was basically a way to use some of the location flexibility that the internet provides.

The FCC ultimately approved, in the end, the one technology that didn't capitulate and that stuck by its guns in keeping this feature. So that's some good news. But the lesson that we drew is this. We've been arguing throughout the debate on the broadcast flag that having governments in some kind of approval-of-technology role like this is itself dangerous for innovation and poses some real risks. Proponents of the flag have said that they don't think those risks are very serious. We see this example as pretty concrete evidence that simply having the government in an approval role like this does indeed create risks.

The other lesson that we draw is that if government is going to go down this road at all—and I noted that one of the topics in the description of this panel is how do you craft legislation that protects both copyright and innovation—if they're going to go down this road at all, the way that the approval process is structured is crucially important. The more discretion the agency has, and the more unguided discretion it has, the more uncertainty there is, and the more pressure there's going to be on every applicant to try to make sure that there's no potential objection to its technologies. And so the more it's likely to try to cut deals with the established companies that have a particular interest in this area.

So certainly, if you're going to go down this road at all, very clear standards, set timeframes for approval decisions, and similar procedural safeguards would be needed. And that's certainly an argument that we've been trying to make to folks on the Hill as they consider doing legislation in this area. So I'll stop there.

SUSAN M. KORNFIELD: We saved a lot of time for questions from the audience, but I first wanted to ask the panel speakers whether there might be some follow-up comment they had to the comments of others and I do want to actually take the moderator's privilege here and pose a question to Professor Felten.

Last night, he mentioned that even if there were pure heart and good intent in using digital rights management technology, in fact, to prevent

infringement, that it was doomed to failure. And I wondered whether you might speak from a technologist's point of view why you think DRM is in fact doomed to fail.

EDWARD W. FELTEN: Sure. There are several arguments here. Let me say first that there is really no technical evidence in support of the proposition that digital rights management can stop peer-to-peer infringement. There's no theoretical basis for believing that it could ever work. There's no practical evidence that it might work. No digital rights management system has ever succeeded in keeping any content off computer networks ever, and there's no reason to expect that that will change.

Now I could talk about why that's fundamentally true, but it basically boils down to the fact that if something is represented digitally as digital bits, it can be copied. It is sort of the definition of digital information that it's by definition copyrighted, and it's by definition transportable across the internet. The internet can transport any information from point A to point B. That's what it's designed to do, and fundamentally, it's not possible to change that nature of modern communication technology. It's fundamentally possible to communicate cheaply from anywhere to anywhere.

Now there are different strategies that people have attempted to use to make digital rights management technologies work. Let me talk just about two of them and how they get into trouble.

One approach is the approach followed by DVDs. For example, to tape the content of the case of a DVD—a movie—and encrypt it and put the encrypted content onto the disc. But the problem with that scheme is that the DVD player has to have the decryption key.

You think of encryption as being like locking the content in a safe. Every DVD player has to know the combination to the safe. And so if your business claim is to have this secret combination to the safe and then to build that combination into hundreds of millions of devices that will be shipped to everyone in the Western world. The failure is pretty obvious that someone's going to take apart their DVD player and get the combination out and publish it, and then that's going to be the end of the story, which is exactly what happened.

Whenever you have one of these encryption-based schemes, the information is encrypted, but it's always the case that all of the information needed to unpack it is there in the consumer's house. It's there in the house, or in the lab of the person who wants to analyze the technology. And you can unpack all of the different approaches to digital rights management, and it's always fundamentally the case that all of the information that's needed to actually unpack the content and getting into

the eyes or ears of a viewer or listener is right there in the viewer's or listener's home or in the device that they have access to. Someone will always be able to take that device apart and get the content out or simply wait until after it's been decrypted. After all, encrypted videos aren't much fun to watch. They have to be decrypted and sent via light into your eye, and light is fundamentally a capturable, measurable thing, just like in the same way that anything you can hear with the ear you can capture with a microphone. There are fundamental problems with digital rights management that make it unlikely to work. So when you take the fact that all of these methods are leaky and will leak somewhere and combine that with the fact that once the information leaks anywhere, it can spread everywhere by internet technology cheaply.

You have a fundamental failure to be able to control the spread of this content. So as long as two things are true: (A) people have access to a fast, general purpose internet, and (B) people choose to infringe, you're going to have a lot of infringement. You have to change one of those two things to stop infringement, and it seems to me that the one that's more likely to change is that people choose to infringe.

SUSAN M. KORNFIELD: Questions from our audience to our speakers? Yes?

AUDIENCE MEMBER: There is some empirical evidence that export control regimes in the '90's pushed offshore some software development. I wonder if there's empirical evidence yet to suggest that higher education, research, or innovation is moving offshore in response to DMCA or what other sorts of heavy-handed content actual moves by content members?

EDWARD W. FELTEN: There is some modest evidence of researchers choosing to go to other countries because of these restrictions. Probably the bigger effect is American researchers being deterred and that creating a vacuum that researchers from other countries can fill.

Increasingly, research in these areas related to security is international in scope, and different institutions, different countries do tend to specialize in different areas. And you're seeing, I think, an increasing fraction of the research related to copy protection taking place outside the United States. This, of course, at a time when the U.S.-based music and movie industries want more than ever to have a good handle on this technology.

AUDIENCE MEMBER: Yeah. I was actually looking for empirical studies. Have there been any yet that can be cited back to policy makers?

EDWARD W. FELTEN: No, I think there's only anecdotal information. It's hard to tell because you have to compare it to a hypothetical

world where we are not subject to results. Other than that, you're just asking people what they would have done.

SUSAN M. KORNFIELD: Fred.

FRED VON LOHMANN: All this introspection, I wonder if there's also a part of that question that goes to the issue of whether more researchers are becoming black hats instead of white hats. It's becoming lucrative to be a researcher in Moldova or Romania or a number of places. You'll get paid a lot more to do the work in the black hat community potentially, and I always worry from a security point of view. We should never deter the best people from working on the white hat side because there will be people who will always be working on the black hat side.

But my question actually goes to something David Sohn raised: the idea that if *Grokster* had come out the other way, Congress would've gotten in the game and the outcome would almost certainly have been worse. I actually take the opposite position. I think that's incorrect, and I think that it's empirically and demonstrably incorrect because in the discussions that the CDT and others were involved in, there were a number of drafts exchanged in an effort to craft a compromise version of the INDUCE legislation. Although the two sides never came to an agreement, the copies I've seen lead to sort of the last position that the content industry was willing to sign off on. A position which ultimately the technology sector wasn't willing to accept, but that last position, it seems to me as I read that measure, is much better than what we got in *Grokster* if you're taking the point of view of a person who wants to create an environment for innovative technology.

In other words, it was clearer. It created some exceptions for ISP's and for others that obviously we don't enjoy in the *Grokster* context. So I wonder why do you think Congress would've done worse given the legacy of trouble that the Supreme Court left us with?

DAVID SOHN: Sure. So the answer to this question does depend partly how you feel about the *Grokster* case. I guess I'm a little more optimistic about how that case came out. I think you're right that there were some exceptions that were drafted into the two versions of legislation that might have been useful. I still know that there was a lot of unease in the technology industry overall about the shape of those bills, and I think that the way I've heard some people put in reacting after the decision is that the *Grokster* case, in part because it's a court decision, it has this kind of sheen of culpability to it. The court was really looking at the fact that these guys seemed to be bad actors. The Court wanted some kind of evidence of active steps to induce infringement, and it is maybe

easier to demand that in a judicial context than to actually spell out in legislative language precisely what we're looking for.

SUSAN M. KORNFIELD: Okay. Barbara do you have follow-up comment?

BARBARA SIMONS: Yes. Regarding the black hat/white hat issue that you raised, I may not have been clear about some of the issues that I am very concerned about. The fact is that the software in voting machines is secret and people are afraid to look at it. That seems like a situation where white hats can play an important role, because we want to find out if there are security issues. We want to learn if the software has been rigged, but we can't legally do so. When it comes to voting machines, copyright and trade secret law is being very much used in an anti-democratic way. The reason that I discussed Sancho is that he brought in a white hat researcher to examine the voting machine. Because the researcher found serious security problems, Sancho is being prevented from buying any voting machines. And because the vendors won't sell Sancho any machines, the state is going after him because he's not adhering to the 2006 deadline in HAVA.

KATE GUSMER: There were some questions in the back.

AUDIENCE MEMBER: You say that you think the DRM will never really be fully effective. It's obvious that no matter what's going to happen, there's still going to be some isolated darkness. There's still going to be content traded if there were some copyright holders. But I just sort of looked at some of these things happening on the public policy front, DMCA, and some states adopted a Super-DMCA of sorts. Michigan is one of them that has things similar to the national level. Isn't there some point in which the controls become so onerous that people will actually choose the illegal route rather than continue to use the legal alternative?

EDWARD W. FELTEN: Well, I think certainly the controls can become arbitrarily onerous. The question is whether doing that will actually stop the infringement and I think not. Certainly, the DMCA has not succeeded in doing so. That's been demonstrated over and over, and again as long as eyes and ears insist on receiving analog inputs and the internet can trade this material, then people will be able to do it.

I don't believe that the trusted computing technologies will change that fundamental fact because in order to get to the state of sort of techno lockdown that some people say will flow from those technologies, many, many other things have to change. And in particular, the systems that people use are going to have to become a lot less useful for a lot of the things that they want to do in order for them to lockdown to have them, and I just don't think that the market will accept that. I think that a

locked down operating system will be perceived as essentially useless by end users not doing many of the things that they want to do and won't be accepted. And so, I still think that any technological scenario that seems realistic is going to feature the possibility of infringement.

Now I do think that there is a possible future in which there are attractive to consumers ways of paying for and using copyrighted content in ways that people like. And, if those attractive services are available and they're priced right, I think people may pay for them. But it's not because technology stopped them from infringing: it's because they made the choice that they wanted to live within the authorized ecosystem of authorized products instead of the other way.

But I think that, that alternative of infringing rather than paying for it and living within the authorized system will always exist. It's just a question of making an alternative that's good enough that people will choose it. I don't think you can take away that choice.

AUDIENCE MEMBER: This question is for Dr. Simons. You paint a pretty dismal picture of electronic voting and its state in the United States and I was just wondering—especially with the massive meltdown that you predict—will there be any pieces for those of us who are to be future attorneys to pick up and help fix this area?

BARBARA SIMONS: Oh, yeah. I think there's a lot of work that current and future attorneys could be doing right now, which is why I pleaded for your help. The EFF has been doing a great job, but there are only so many people at EFF and they can't handle all the cases. I think there are a lot of open record requests that need to be filed around the country, so that we can learn about the contracts that have been signed, as well as relationships between election officials and vendors. There are many instances, unfortunately, in which election officials subsequently go to work for vendors. There are also cases in which the vendors seem to be working far too closely with election officials.

It would also be really useful if legal experts could help computers security experts legally obtain voting machine software. Many states have the software, but they won't let outside experts examine it.

A few months ago California tested ninety-six Diebold machines under Election Day-type conditions. There were twenty crashes and fourteen printer failures. It's clear that the private entities that do the testing do an amazingly poor job. There is also the questionable practice of having the vendors—not the state—pay the testing organizations.

I also hope you will encourage states to conduct realistic testing, as California has done. Even more important, states should be prevented from signing contracts that allow voting machine companies to keep

their software secret. There are no trade secrets in these codes. All they are supposed to do is record and count the votes.

[Audience laughter]

Really the trade secret argument is a canard and even Michael Shamos—those of us who are working this area know Shamos, because he's one of two computer scientists who sometimes support these machines—even he will say that the trade secret argument is absurd. The only trade secrets they have are the software bugs.

[Audience laughter]

So please help us. Challenge election officials and vendors. Talk with Cindy and me afterwards, and we'll give you lots of things you could work on. Right, Cindy?

CINDY COHN: I'm Cindy by the way.

BARBARA SIMONS: There she is.

[Audience laughter]

CINDY COHN: Barbara's one of the technologists and I'm one of the lawyers who are trying to push more lawyers into this. There is a lot to be done. In fact, I think that actually we need a huge revolution in the way that election laws work. We need to think about election administration not only from a perspective of actually creating a digital secure environment, but also creating a procedural and legal framework that supports the technology. That is a huge job, and one that could be many people's life's work.

I think what we saw, as Barbara says, when we started looking at election laws, was that outside the context of traditional equal protection and apportionment-type issues, when you actually start to think about elections as administrative systems. From that perspective, we saw how truly inadequate the law is currently. It's going to be a lot of work to try to clean up something of this magnitude. It's really fascinating and fun and it's interesting litigating policy or procedural or administrative-type work.

BARBARA SIMONS: I have a really quick comment. We need new laws in this country. We need to have random manual audits conducted in every state for every national election, even if the election is not close.

SUSAN M. KORNFIELD: Robert?

AUDIENCE MEMBER: This is particularly a question to Professor Felten. The term fair use hasn't come up as much in this conversation. It strikes me that regardless of how effective or ineffective DRM's use has been, those of us who have to crack them to exercise our fair use—I confess, I use videos in my classes which is clearly protected under the fair use, but in order to exercise my fair use rights as a professor in a classroom, I have to break that code. I have to use the D sets, and that leaves

me criminally liable for the reverse engineering laws used today. I guess what I'm saying is from that perspective, it doesn't really matter whether the DRM actually works. What actually matters is if anybody tries to break it they are in violation and it's a unilateral action on the part of the content provider, it can actually lockdown content that is not even copyrighted in cases. Do you see any way that we can get around that?

EDWARD W. FELTEN: Technologically, apparently, you can get around it.

[Audience laughter]

Legally, it's just a matter of changing the law. But this is actually, I think, an important point about these DRM technologies because although they're not effective at controlling this sort of widespread P2P infringement that their advocates are always talking about they do have some effect in controlling how the average users who have paid for the content use it within their own local library. That's an area where DRM can have an effect on average, and there is revenue in that control for the copyright owners. So, there's a certain cynical view of this debate that says that while we have all this public rhetoric about P2P infringement, everybody who's sort of behind the scenes really knows that that's not the effect that this technology will have.

The effect of the technology really is to give copyright owners more control over the uses that purchasers of the content make, and I'm not going to say that I always subscribe to that cynical view of the debate, but I think it's a perspective that's worth bearing in mind. That there's more at stake here than just the P2P issue, and often the P2P issue is really a red herring. Even if some of the people in the debate do believe that they're controlling people from infringement, it's worth bearing in mind that these other effects are the real primary effects that DRM actually has.

SUSAN M. KORNFIELD: And Robert, you can consult with any of my copyright law students who will tell you that there's some good recent case law that's come down saying if you're not otherwise committing infringement, it's not a violation of the DMCA. So my students, raise your hand to be able to consult with Professor Frost.

[Audience laughter]

We have time for one more question and then our panel time is over.

AUDIENCE MEMBER: It seems that one of the major problems is getting people involved and interested in this area of the law. One of the fundamental problems is that it's such a small percentage of law students have difficulties going into this field because of the lucrative careers elsewhere. So how do we get more technically proficient people engaged in this area? I know that Professor Felten presumed that a lot of professors don't want to deal with it. How do we change that?

EDWARD W. FELTEN: Well, our students are still young and naïve and still want to change the world. I think there are opportunities to get involved. I do think that the younger generation of lawyers and law students are more tech savvy than their elders. That's true in almost every field including computer science, that our younger students are more tech savvy than we were at their career stage.

There's also a surprising number of technologists who are becoming lawyers. At Princeton, it's now the case that about ten percent of our computer science bachelor's graduates go straight to law school.

[Audience laughter]

AUDIENCE MEMBER: What a waste.

[Audience laughter]

EDWARD W. FELTEN: He says "what a waste." It may be a waste, but it is happening. And those people, I think, will make a difference on the legal side even if it if they're not living up to their full potential.

[Audience laughter]

SUSAN M. KORNFIELD: Ed and I were talking about this last night. I guess earlier it was the P2P stuff, then the Digital Millennium Copyright Act, and now bogie, these are all topics that have brought computer science into the political world—like it or not. So, I think our community's become more aware and as you say there are young, idealistic students who decide the only way they can deal with this is to also get a law degree. I've had students do that, too.

EDWARD W. FELTEN: The other sense in which this can happen is through large technology companies. There you have a lot of engineers and you have companies whose phone calls will get returned to Washington. And that matters a lot to be able to get your phone calls returned and to be able to get yourself invited into the room where the deals get made.

An ordinary technologist has no hope of doing that, but the representative of Microsoft or Cisco or Google, maybe can do that. And they do have a technology viewpoint. Although it is the viewpoint of the technology company.

DAVID SOHN: I just wanted to follow-up on that. Working in Washington, that's absolutely true. Those companies play a really important role in a lot of these debates. But their interests can be different sometimes than the interests of a small start-up who is just getting going.

SUSAN M. KORNFIELD: I'd like to thank our panelists for traveling such a distance and being here today.

[Applause]

KATE GUSMER: We'll, we'll take a short recess. We'll reconvene for Panel Three at 3:30 and there are refreshments in the hallway, so help yourself.

PANEL III
INTERNATIONAL ALTERNATIVES AND ENFORCEMENT

KATE GUSMER: Now we're going to start Panel Three which is INTERNATIONAL ALTERNATIVES AND ENFORCEMENT. This Panel is being moderated by Richard Owens. Professor Owens is the Executive Director of the Centre for Innovation Law and Policy in Toronto. Before entering academia, Professor Owens was a partner with Smith Lyons LLP, where he led the firm's IT and IP practices. His teaching and writing interests include intellectual property, financial services, privacy, e-commerce, biotechnology and the law of the cyborg.

Professor Owens is the Director of the International Technology Law Association and teaches courses including the Law of Information Technology and Electronic Commerce, Innovation Law and Policy, and Policy of Biotechnology, all at the University of Toronto Faculty of Law.

RICHARD OWENS: Let me start by congratulating the organizers for bringing together such an interesting and expert roster of speakers in such an in-depth and well-prepared conference.

I am delighted to be here. The Centre for Innovation Law and Policy, which I represent here, is a multi-disciplinary centre for the study of all aspects of innovation law and policy, located at the University of Toronto Faculty of Law. We have many programmes including graduate degrees, for those of you inspired by the parade of luminaries to continue your scholarly endeavors. More information can be found at the Centre's web site.

In my role as moderator, I have been asked to provide some context on the issues for the panel, so I will say a few words and then introduce our speakers.

We are all here because of the internet. *Grokster* and the whole file sharing project are, of course, artifacts of our digital interconnectedness.

And it is a trite observation that this interconnectedness need not observe national borders. To this trite truth, however, there is a growing list of exceptions such as the French Yahoo case limiting the ability to sell Nazi Memorabilia in France from outside the country.

Our panel addresses itself to this annoying aspect of the Internet; the frustration of rights holders who, in spite of being able to pay the exorbitant fees of powerful lawyers like Fred von Lohmann—not, admittedly,

that they would choose Fred, of course—finding that their pit-bull lawyers are on jurisdictional chains that don't reach the pirates baiting them from outside the nation's borders.

FRED VON LOHMANN: I would agree.

[Audience laughter]

RICHARD OWENS: A response to this conundrum is international lawyer deployment; to take the war to the location of the infringer or circumventer, whether that is Norway or Amsterdam or the United States. In the case of Canada, it turns out to be effective to sue in Philadelphia, as happened in the *iCrave TV* case involving a Canadian web site's unauthorized use of American broadcast signals.

These tactics are expensive. They depend on the vagaries of local jurisdictions—like Canada, for instance, which has not updated its Copyright Act to bring it into compliance with the WIPO Copyright Treaty and which has a blank media levy which, in one instance, was found to legalize unauthorized music downloading. Each piece of litigation only provides a remedy as far as damages in that particular country. Now if that country is the United States, it might effectively rob the enterprise of its economic rationale, and thereby stop it; if it is an insignificant market like Canada, it won't. If an injunction issues and access to the network can be geographically controlled, then only local use will be affected; if access cannot be geographically controlled, as was found to be the case with iCrave TV, then the enterprise will be shut down.

Long-arm jurisdiction is a partial answer. But efficacy of long-arm jurisdiction ultimately hinges on the willingness of other jurisdictions to recognize it, or on a defendant's connection with—preferably assets in—the U.S.

In the British Columbia internet libel case of *Braintech v. Kostiuk*, the B.C. Supreme Court refused to enforce a Texas court's exercise of jurisdiction over a B.C. resident. In another example of ambitious exercise of jurisdiction backfiring, extensive rights of access to data under the Patriot Act has created political pressure resulting in effective limits on outsourcing of data processing to U.S. companies.

The ability to protect intellectual property in foreign jurisdictions improves with strengthening local laws and their enforcement. So rights holder jurisdictions like the United States pursue the harmonization of intellectual property protection through instruments like TRIPS, and elevation and modernization of the standards of IP protection through instruments like the WIPO copyright treaty.

Still, these international agreements are subject to variations in local implementation, and even non-implementation. The recent announcement

by France that it will introduce legislation to require Apple to abandon its TPMs in order to ensure multi-platform operability of its iTunes downloads is a particularly apposite example.

In any event, internet challenges to intellectual property rights inspire new energies in legal reform. Policies like the requirement for service provider filtering of content lurk in the wings after *Grokster*. These kinds of policy initiatives gain momentum from P2P networks tainted by illegality. One source of such taint is the traffic in child pornography over them, a reality to which rights holders are alert and in which they may find polemical advantage. So too P2P network operators seem shady not only by adopting the –ster suffix, but also by hiding their operations from the effective exercise of jurisdiction, as Kazaa went to great lengths to do, or as Earth Station 5 has by locating in the Palestinian territories. So, in the fora of public and judicial opinion, the equities are not with the P2P networks.

These networks do represent technological innovation and they benefit from policies promoting innovation. From a public policy perspective, then, arguments for controls on networks and devices are met by national innovation policies to encourage social wealth creation by technological discovery. But these national policies are notoriously vague and their effects unquantifiable, and will likely bear less political force than arguments about theft of IP and protection of children.

Peggy Radin set a great precedent for introductions by suggesting you read the biographies of the panel in your materials.

Our speakers will be brief to allow lots of time for audience participation.

MICHAEL GEIST: Thanks, Richard, and let me add my thanks to the organizers both for the invitation and for a really interesting day. Richard just presented the internet and the jurisdictional issues as a problem. I'd like to present it in a little different way by describing why sovereignty is really great.

As I was flying in yesterday, I noted that it was literally only on approach that I left Canadian air space and landed at the airport in Detroit. While geographically we're very close, there's a significant distance at least for the moment between Canadian law and U.S. law. And so when we're talking about international approaches to these issues, I don't want to talk so much about enforcement. Rather, I want to talk about choices and different choices that some countries want to make.

I need to give you five backgrounders about Canadian law, and then tell you where it is we may be going. First, we don't have a DMCA. Yes, you can applaud.

[Audience laughter]

We did sign the WIPO treaties back in 1997, but as I'm sure you all know, signing the treaty doesn't create any obligations on a country. Obligations only arise from ratification.

[Audience laughter]

It's only when you ratify it that you're required to do something, and we have yet to ratify it, and in fact, we're very unlikely to ratify even if we implement. There's now "bureaucratic speak" in Canada that we might implement the treaty, but we won't ratify it because we will take on additional obligations that would largely involve transferring large amounts of royalties south of the border here to the United States and that doesn't really benefit our artists. That's part of national cultural policy. We'd rather show that our royalties are paid to Canadian artists—Avril rather than Britney.

[Audience laughter]

So we don't have a DMCA. We do have a private copying levy, and so in Canada those that download for personal noncommercial purposes do so at least arguably lawfully. The private copying levy, which is a levy that is placed on blank media, such as blank CD's, has generated more than $140,000,000 over the last five years in Canada. That's a small amount by U.S standards, but we're a small country. So $140,000,000 is actually pretty sizable amount of royalties to be generated, particularly given that they go directly to, by and large, the artist. And so when we talk about peer-to-peer, the debate is a somewhat different one because, by and large, much of the activity could be argued to be lawful. We haven't had anywhere near the 17,000 or so lawsuits that the RIAA has launched in the United States. We've had one series of lawsuits involving twenty-nine alleged file sharers, and that lawsuit was unsuccessful. I should note that we, too, have a public interest technology law clinic in our law school—CIPPIC—and it involved itself in this case. Those lawsuits were launched by the recording industry against these twenty-nine alleged file sharers, and they were unable to get to stage one because the ISP's were not required to disclose the identity of the alleged file sharers.

For one thing, the evidence the recording industry provided seemed to be faulty, and for another, we have national privacy legislation that the judge didn't think should be eliminated because the recording industry decided to sue. Moreover, there were questions about whether or not this constituted an infringement of Canadian copyright law. That decision was ultimately appealed, and while the decision itself was upheld, the appellate court certainly created a road map by which we could see future lawsuits, but as of this date, we haven't seen any.

It's also important to note that we don't have copyright within our Constitution the way that you might, but we have had a very active Supreme Court of Canada, at least in recent years. Up until fairly recently, it was the view of the court that copyright law in Canada was an artist-focused statute. So the purpose was to ensure adequate compensation for artists. Yet, in a trilogy of cases handed down by the court over the past four years, the court has really re-focused the copyright debate making quite clear that copyright law is all about a balance.

Articulating the need both for compensation for creators, but also the importance of users, the court has gone so far as to characterize the exceptions that exist under copyright law as user rights, arguing that those user rights must be set up against the creator's rights and that there must be a true balance.

One final thing, we don't have fair use. We have fair dealing, which sounds similar, but it's not entirely the same. The Canadian Supreme Court has granted a very broad and liberal interpretation to fair dealing. For example, full articles may be permissible for copying purposes as fair dealing, but it is limited just to a series of categories. So the categories that we have, things like research and private studies, criticism and news reporting, are exhaustive. I believe we would do far better by adding two words to our statute, "such as," to make those illustrative rather than exhaustive.

Anyway, that's the background you need to know. It won't come as a surprise to learn that there has been mounting pressure in Canada to adopt WIPO-like standards. We don't have a DMCA, but many people will say we don't have a DMCA *yet* because it is seemingly, in the view of some, only a matter of time.

The government last consulted on this issue several years ago. In 2001, it asked questions about digital copyright-related issues, primarily any circumvention questions, making available right type issues, as well as the role of internet service providers and what kind of liability ISPs might face in those takedown-type systems, as well as whether or not they ought to enjoy some sort of exemption for some of the activity that takes place on their systems.

In 2004, a Standing Committee on Canadian Heritage—the equivalent of a Congressional committee—issued a fairly important report on copyright reform in which it embraced DMCA-like provisions. Just last year, the government finally did move on copyright reform, introducing Bill C-60, which was our first major piece of copyright reform legislation in about seven years. I'm not going to go through the whole bill, in part because the bill has now died. We've had a change in government and the bill didn't make it past its initial introduction. But it is worth not-

ing a couple of things because when we talk about choices, these are the kind of choices countries can make. On the issue of internet service providers, you may note that in the United States, you have a notice and take-down system which a copyright holder can send notification to an ISP alleging that there is infringing content on their system or being posted by one of their subscribers and ask them to take it down. Notice and then takedown.

Simply put, that system doesn't work. It certainly doesn't work in a peer-to-peer environment where there is nothing for the ISP to take down because it's residing on the individual's computer. That doesn't stop people from generating literally tens of thousands of these notifications.

In Canada, we chose not to follow the notice and takedown approach, at least under Bill C-60, but instead adopt a notice and notice approach. A notice and notice approach would involve a notification from a rights holder to an ISP. The ISP would be obligated to simply notify the individual subscriber that they had received this notification. If the rights holder wanted to go further, they could go to court and actually seek some sort of remedy to actually order the ISP to remove the content.

Supporters of this note for one thing, it's a better system because a notice and takedown doesn't work. For another, Richard mentioned child pornography on peer-to-peer.

We actually do have a notice and notice system in place already. It exists for child pornography under our criminal statute, and so ISP's are not required to take down child porn based merely on notification. So, if it is good enough for child pornography, one might think that it would also be good enough for an allegedly infringing song.

We also introduced fairly limited anti-circumvention provisions. The new anti-circumvention provision ensured that any circumvention would only become an infringement where it was done for the purposes of copyright infringement. In other words, if you circumvent it for another purpose, let's say for privacy for example, that would not be an infringement. There's actually a limited exception for private copying, but I don't need to get into it.

We also didn't include anything on devices—no ban or criminalization of devices whatsoever. That, too, I would describe as an innovation strategy. Bill C-60 has died and we've had a change in government. I want to very quickly tell you about where it is we may be headed.

First, we've had this change of government. We had a Centrist party switch to another Centrist party which is seen as a bit more right-wing, but in Canada, everybody's sort of in the mushy middle. This new government is expected to take a more market-oriented approach. Now I

don't know what that necessarily means. CATO came out with a study just this week which would be seen as more market oriented. Their argument is that, from a market-oriented perspective, the DMCA is not particularly a good thing. So we'll have to see whether or not the government adopts seriously its notion that it wants to take a market-oriented approach. Note that we do have iTunes and the new Napster and the like right now absent a DMCA.

In Canada, as in many jurisdictions, the stakeholders are getting ever louder. The copyright lobby is getting very vocal and just over the last few weeks, for example, they've brought in a series of experts, including the Registrar of Copyrights here from the United States and one of Canada's leading computer law experts who is now a lobbyist for the recording industry. They came together and put together a show for government officials, then they went to the Canadian Music Week, put on the same show, and then, I think, they were part of another event at the University of Toronto. So, there is certainly a fair amount of activity that's taking place from the lobbyists who argue that C-60 didn't go nearly far enough and that Canada really needs more.

At the same time, users are becoming far more vocal and there's been a recurring theme about what can individuals do about these issues. I actually think that as much as it's great to get involved in clinics, you can do an awful lot without a clinic. You can do an awful lot just on your own. Blogs and other new technologies give people the power of voice that they didn't have before and users are speaking out. In our last election just in January, I got involved in a fairly public debate that started from through my blog and then through a lot of other blogs with the person who actually chaired that standing committee on Canadian heritage that developed that report that I just described. She then became the Parliamentary Secretary for Canadian Heritage and the lead person on copyright. It turns out that the recording industry, the movie industry, and the software industry was holding a fundraiser for her four days before the election. I didn't think that was so good.

[Audience laughter]

So I posted something on my blog and some other people, Boing Boing, posted it on their blog and lots of bloggers started picking up the story, and people started raising it at candidates meetings. Those meetings were soon after posted to YouTube, with video in which the candidate said she wouldn't be intimidated by Michael Geist and his pro-user zealous and EFF members.

[Audience laughter]

The issue generated considerable discussion and the Member of Parliament actually lost her seat. There was a swing of a fair number of

votes and whether the impact that the bloggers had, nobody knows for sure, but this was by far the biggest swing of any riding in the City of Toronto. People have a voice—as many local bloggers noted, pro-user zealots are voters, too.

[Audience laughter]

I think there's a tremendous opportunity for everyone to speak out if these are issues that concern you. That must be set up against growing pressure from the United States, quite frankly, for a change in Canada, a change that follows more particularly the U.S. style approach. Part of it comes from the copyright lobby associations like the Canadian Recording Industry Association, the Canadian Motion Picture Distributors Association, who are by and large U.S. organizations in Canadian camouflage. They put the name Canada in front, but answer to their sister organizations in the United States. I think even more important is the pressure that comes directly from the U.S. government. The Section 301 report that comes from the USTR (the United States Trade Representative) regularly puts Canada on the list. Frankly, just about everybody's on the list, so we're in good company.

[Audience laughter]

I expect that Canada will get particular mention this year as being an egregious example of a country that hasn't done enough on the copyright and there are certainly those that will take that very seriously. Of course, people pay attention when this issue escalates up to a trade level issue. There are many countries including Australia, Singapore, and Morocco, that have signed trade deals with the United States that include numerous provisions that deal specifically with copyright. To read just how extreme, in fact absurd, it gets—if you take a look at the Morocco deal, there is something like a 30-page side letter that talks about what an ISP in Marrakesh must do if it receives a notification from a rights holder.

I think that my country is probably going to join that list. We already have the free trade agreement, so we can't be threatened with free trade, but we do have trade irritants, such as lumber and fishing.

The counter to this is that there are, of course, global changes that are happening all around the world, and we've heard a lot today already about the changes in France.

Just a few weeks ago, Australia came out with a unanimous parliamentary committee report taking a look at TPMs and the implementation of anti-circumvention legislation. For those of you that don't know, they did create anti-circumvention legislation back in 2000. They then signed a free trade agreement with the United States in which the U.S. said, "Your anti-circumvention legislation isn't good enough. Here's the additional

stuff we'd like you to include," and Australia is now in the process of doing that.

Well, their parliamentary committee came up with an incredible report in which there are literally dozens of recommendations about the kinds of exceptions that are needed so that if you are going to have a cultural policy, if you're going to have an industrial policy, if you don't throw all of that out the window for the sake of creating ever stronger copyright protections that send most of the royalties that are generated outside of the country.

And then even at the international level, WIPO is engaged in an absolutely fascinating debate right now as part of the development agenda where large numbers of countries from South America, from Asia, from Africa are beginning to question many of the kinds of agreements that we've seen in the past, and starting to push back. So, the question from the old Canadian parochial perspective, of course, is what impact will that have? We had for a long time people arguing that Canada must meet international standards. Well, if international standards mean the French iPod legislation and all the exceptions that Australia's talking about and the exceptions that Chile raised at WIPO, I'm all for international standards.

And so this is, I think, the kind of international framework that Canada is facing, but it's not just Canada. It is many other countries that are in similar situations. Thanks very much.

RICHARD OWENS: Thanks, Michael. Professor Oswald.

LYNDA OSWALD: Thank you. As the moderator said, I come from the Business School right across the street, so I think I won the award today for coming the least distance to the conference.

Since I teach in a business school, my perspective on this, I think, is very different from those of the other presenters today. I approach the topic as a law professor who teaches primarily MBA students—future clients, not future lawyers. And that different orientation, I think, causes me to come at these issues from a slightly different direction.

I teach IP law each year to about one hundred-thirty graduate students, and these are the people who in ten or fifteen years are going to be the leaders in their industries. They're going to be the ones out there managing the rampant technological changes that are certain to sweep over us in the coming decades.

One-third of these students are international students. They're primarily from China, India and Southeast Asian nations. All those countries who, if you believe the accounts that are given, are going to be eating our lunch in a decade or two. They have a very different perspec-

tive on how the world looks, how the business environment should look, and how the legal environment should look as well.

Now, the students I teach amaze me because they're so much more sophisticated, both the American students and the international students, than the students of my generation—which we won't talk about how long ago that was, but it was a while. They're far more widely traveled than we were at their age. They're far more technologically savvy as one of the other presenters mentioned. This is a point which I will confess to you: I have never even so much as held an iPod in my hand, but I kind of know what they are.

They have a much better understanding, I think, of the diversity of the international political, legal, social, cultural, and economic norms, and they have an ability to adapt that is so quick and so agile that sometimes I am just stunned at the things that they can do.

These are the managers in training. I think they are the wave of the future. They are going to be the ones developing the technology and businesses that are going to be driving new IT products, and ultimately, the types of IT global activities that we'll see in the future. And I think they see different challenges posed by the environment that we face, the legal and the business environment, but they also see unlimited opportunity.

They're also the ones that are going to demand that we, as lawyers, figure out a way to develop an IP legal regime that will be flexible and sophisticated enough to handle these technologies that we don't even know about yet today. We know the technologies are coming, but we don't know yet what form they'll take.

I don't want to talk today really about specific legal regimes that countries have developed for handling digital products in particular, but I do want to share some general thoughts on the types of issues that we face in this digital arena, and the effect that those issues are going to have on American business, on global business, and on the domestic and international legal regimes that we're going to have to develop for those businesses to operate within.

These are issues being debated already, of course, in the international arena by legal commentators, by legislators, or the policymakers, by organizations like WIPO, and IP rights holders, and of course, by the end users of the products as well. There's a long list of stakeholders in this debate and they're a diverse group. They have a lot of different interests, and they often have conflicting goals and objectives at stake as well. What that means, of course, is that the international legal issues that we are going to face in the digital environment will indeed be very, very difficult to resolve.

Now, we often talk about globalization, and we talk about the global economy in which we all live, operate, and work today. Fifteen years ago when I was a new professor, business schools were very much focused on what they called "internationalizing" their curriculum. They wanted to prepare these future business managers for this global phenomenon that everybody knew was coming.

Well, today, internationalization doesn't even really show up in the debates that we have. It's not really on the radar screen of the business schools anymore because we think globalization has occurred; it's inherent within business activity today, and it's inherent and embedded across the business curriculum as well, and I think that's the point that we need to get to as lawyers.

Digital copyright issues, I think, are globalization taken to the nth degree. Digital copyright is borderless. It's ubiquitous. It's difficult to regulate (if you can regulate it at all). Yet these digital products are also a tremendous source for growth in capital. They're tremendous magnets for creating new wealth, new opportunities, new types of businesses that we can't yet fathom.

So we need to figure out a way of getting copyright law to the same place that business education has reached: where internationalization is so inherent it can go virtually unspoken; where it's so embedded and so inherent in how we talk about these issues that you don't need to focus on it anymore as a specific topic; where it's automatically part of the dialogue whenever we talk about these things.

Now, I think there are a number of systemic reasons why we have not yet reached internationalization in digital copyright law, and why it may never even fully occur. And it's interesting, the debate I get among my students within the classroom, since they approach this topic from so many different perspectives.

There is this fundamental tension in the international digital copyright area. A conflict, on the one hand, which leads some people to think, well, the internet is a mechanism for the free sharing of information unless we're told better; and on the other hand, those people who say, well, the internet is just one more mechanism in a whole host of tools that we have for disseminating authorized information to authorized individuals—usually, of course, for a price.

In the international sphere, I think those differences—that conflict—gets magnified because you do have these different kinds of social and economic, political and legal differences all coming to the fore. It's hard to sort out what the ramifications of those differences actually mean to countries with weaker notions of private property rights, especially IP rights. Would they favor digital copyright as well? Would content pro-

viders continue to innovate and create if they faced less legal protection or would we see a decrease in their creative output—which I think none of us would want to actually see. Conversely, would a weaker international digital copyright system actually promote creativity and decrease inappropriate types of monopoly?

I would confess I personally believe in a very strong private property rights regime, and I think that Hernando DeSoto and researchers who have followed him have done an admirable job of showing that a strong private property rights regime in real and personal property can indeed support the growth of capitalism and development of wealth by even the poorest members of society. What I think we need to figure out is, are digital products somehow different than traditional property interests? Would weakened property rights in them actually foster more growth or would they actually inhibit growth? It's hard to say.

I think the opportunities for empirical research in this field are limitless to try to tease out some of these potential consequences. I think until we look at some of that work and do some of that empirical research, any of our efforts to try to legislate in this area are necessarily going to be fumblings in the dark. We can't really be sure of the effects we'll have until we know how the system views those products.

There's also, of course, the issue of IP rights in the digital environment just being very different and more complex than IP rights in the traditional non-digital environment. We've talked about the ease and the speed of replication today, the difficulty of identifying an infringer, of halting their activities once you have identified them, of trying to obtain or enforce a judgment. All of these types of things are multiplied in the international environment.

We've talked a little bit today about the fact that technology is probably not the solution, that as fast as we can develop technology to try to protect digital products, hackers—or whatever term you would prefer to use for those people if that's now a pejorative term—are behind us, right behind us, working as fast as we develop the technology to develop ways to get around that technology. The other mechanism that we have, of course, is the law. But in the international digital copyright context, the law is not a simple solution. Even just the logistics of trying to enforce your rights in the digital world can be overwhelming. Just think of the complexities that are involved and the inherent global reach of the internet.

If you think about, if you're a rights holder in the global digital environment, how do you protect your copyrighted products? How do you identify your infringer? Once you do identify your infringer, what country's law is applied? Who has jurisdiction? How are you going to deal

with things like forum shopping? Can you enforce a judgment abroad? All of those things are very, very complex issues. To a large extent, your ability to protect your property—your digital product property—is going to depend upon the efficacy of those national laws that you face in those countries in which you operate.

Of course, there's the other side of the coin, which is if you're operating in the digital environment, how do you make sure you're not subject to the laws of other countries, which you either might not know or might find unfavorable? Once your product is out there on the internet, of course, you can't control where the reach extends, or the countries in which you are subjecting yourself to jurisdiction.

So, as I tell my students, it really doesn't matter whether you are the plaintiff or the defendant in these disputes. Either way, there's just inherent tension out there between the traditional, territorial approach of IP law versus the international or even stateless nature of the digital environment.

So the question, of course, then becomes, what do we do? How do we create a playing field where the rules of engagement are clear and fair, and they're easily applied even in this very complex world that digital copyright creates?

Now, of course, as we talked about today, here in the United States we've already been pretty active in that area. We've got our DMCA that creates this very broad range of legal protections for digital copyright holders. Some would say it's too broad. Some say it's ineffective at what it attempts to do, but nonetheless we've got it out there.

And we also, I think as Michael alluded to, we have been pretty diligent about trying to export our view of the perfect digital copyright regime to the rest of the world as well. We can and we do, encourage or pressure, depending upon your view, our trading partners to adopt U.S. IP rules, including with respect to digital copyright protection. We're pretty unrepentant about what we're doing. The acting general counsel for the U.S. trade representative recently said, "The rules we apply around the world are the rules that are needed throughout the world." Well, that works as long as we're the 800 pound economic gorilla in the room, which we currently are.

Our trading partners today may well gain by adopting the US standards because it might give them more access to foreign trade and foreign investment, but I think we need to recall that our IP system is unique. Few other countries have our system of very strong IP rights coupled with really extremely weak IP responsibilities. We've got a legal regime, here, where copyright protection extends for seventy years past the life of the author and compulsory licensing is a dirty word. Where

courts offer very extensive enforcement protection for IP rights, with the enforcement power and legitimacy to make those things stick.

But can we or should we really expect countries with a different world view, a different view of IP rights, and different judicial backgrounds to adopt similar schemes? Will the international harmonization of digital copyright law require changes in our own legal regime as well?

As the global economy changes—(and it is changing)—and non-western participants like China and India play a larger and larger role, we're going to increasingly hear voices that will come from very different cultural, political, economic, legal and social backgrounds. And their views of how digital copyright issues, or even IP in-general, should be managed are likely to be very different from our own.

I think we need to ask ourselves, how willing are we to be open to dialogue on these issues and to new approaches to these ideas and rights? How well will we flourish in the new global economy if we refuse to participate in this new dialogue that is inevitable? It will come.

I think to a very large extent, digital copyright creates issues of international and political economy—not just law. And as non-western nations start to play a larger and larger role in that global economy and they have a louder voice in setting international policy and standards, we here in the west need to think very carefully about what it is we value what it is that we're trying to protect—and what mechanisms we can effectively use to reach those goals.

Now something great about being a professor: You can ask questions, but you don't necessarily have to have the answers! I'm going to stop right there.

RICHARD OWENS: Well, the table may be turned on you, Lynda, when this is over.

[Audience laughter]

MICHAEL W. CARROLL: All right. So, I'm going to put my Creative Commons hat on in a minute, but I'm going to keep my Villanova hat on for the moment. I have the challenging job of keeping you awake. I see a lot of you struggling with this.

A couple of points in my professorial capacity that I want to make. One is the premise of today's discussion: is that law matters and, in particular, copyright law matters. But we should think about what we have heard today and ask, Does it really? There are two ways in which copyright law might not matter. One is that a DRM regime combined with a licensing regime could render the copyright entitlement irrelevant. We've heard from the technology panel that, in fact, the effective combination of these regimes is a false hope. So law might matter, but we've also heard that law is irrelevant if the behavior you're worried about is peer-to-peer

file sharing. (the behavior which gave rise to the *Grokster* case). That behavior will not stop no matter what the law is, whether it's standardized or tailored by jurisdiction.

But law will matter when used against people who create businesses around technologies that facilitate the communication of copyrighted works across this global network. So then we should care about legal entitlements, at least, but we should focus on the likely defendants, the likely folks against whom these entitlements will be used. And we have heard essentially two competing visions of how this entitlement should be shared.

One is that standardization and uniformity is what we need because the internet is a global medium. But that means that, as Professor Oswald closed with, it might not be so easy. The U.S. should be careful for what it wishes. Professor Geist says there's an easy way out of that, and it's through a laboratory approach with multiple jurisdictions experimenting with different entitlement designs based on local conditions. I think I'm with him on the entitlement design question. But the push for standardization, the demand for standardization in intellectual property law is strong.

I am now putting on my Creative Commons hat, and I'm going to talk a little bit about a standardization effort that I've been involved in. So let me just ask how many people in the room have heard of Creative Commons? All right. Good. So there are at least a few who haven't, but it's grown. That's good.

So Creative Commons is an organization that does a number of things, but primarily what we do is create and distribute free copyright licenses that are standardized across the jurisdictions of the world. These licenses essentially flip the presumptions of copyright law. So I want to close, actually, on the alternative side of the panel.

The whole discussion's been premised on how people use the copyright system to enforce their rights in order to extract a profit. The control granted by copyright law is premised on the need for economic incentives to create, but, as Professor Reese has suggested, once you get into a world of automatic copyright, you've now lumped together different kinds of copyright owners with different kinds of interests. Some of them have a much stronger interest in having their work shared than in controlling how it's used and in obtaining a royalty from such use. And that's the premise behind Creative Commons. Set up royalty-free uses that go above and beyond fair-use that you permit, and express it in simple terms that people can understand.

So in December 2002, we set these licenses loose on the 'Net and had very little idea of what the uptake would be. But our vision of how

creativity works suggests that there should be a population out there that would be more interested in sharing their works over the network than in controlling distribution.

We don't have a perfect way to measure how many licensed objects there are but, at last measure, there were fifty-eight million objects on the web that link back to one of these licenses. And the number keeps growing at a rapid pace.

Briefly, what you do is, if you have a web page or something on the web, you answer a couple of questions about what conditions you want to put on the uses you are willing to allow. Are you willing to allow commercial use or not? Are you willing to let people modify your work or not? And then what jurisdiction are you in? Right? Because copyright law is territorial.

And so what we've had to do is translate the legal code of the licenses to comport with the language and the law of all of these different countries, and we have a number of projects ongoing in a number of jurisdictions that are reflected on the screen. So part of the Creative Commons response is that this is not limited to a U.S. perspective. This is not a U.S. problem. This is a global response to global copyright, and there's demand for having creative works shared.

Some of the interesting applications of the licenses include Flickr. Flickr is a website that will host your digital photos. Flickr's Creative Commons search engine, which sorts photos by license type, is evidence for my argument that copyright status is a new relevant dimension to measure things that you find on the web. We started dealing with the web in terms of topical relevance. You went to the search engine and said show me information that's relevant to the subject matter that I'm searching for. But that doesn't tell you anything about what you can or can't do with the objects that you find, right?

So now copyright becomes a new relevance dimension. I don't just want something that's topically relevant, I want something that I can use for a specific purpose. So if I'm a teacher looking to create a PowerPoint slide that I'm going to put up on the web, I want a nice background—and I'm tired of Microsoft's Powerpoint templates. I might go to a website like Flickr and say, well, maybe somebody's done some photos of abstract kinds of things and I'll use that as my background. Well, will I have permission? Do I have to negotiate? No. If I choose something under this Creative Commons Attribution license, all I have to do is give this person credit. They've already given me permission to use their photo. They've said go for it, just give me credit. So the transaction cost for that transaction dropped to almost zero, and to the copyright owner it's great that the photo will be shared.

So the presumption that the international and alternative discussion is supposed to be just about enforcement, I think, is too narrow. I think we're in a world where the Net is not only being used for copyright infringement, but also for licensed or authorized sharing of copyrighted works—and this is just one use case.

Now these are licenses, and they are legally enforceable agreements. Just recently, Adam Curry, a former MTV DJ who now podcasts, hosted some of his photos of his 15-year-old daughter up on Flickr under a Creative Commons license. A Dutch newsweekly printed one of these pictures for commercial use, but the photo was under a Creative Commons non-commercial license. Curry has sued successfully in a Dutch court and enforced the non-commercial restriction of the license.

Separately, there's been an issue with musicians trying to share their music under Creative Commons licenses, but being told by European collecting societies that you must assign your copyrights to us. You can't have it both ways. If you want to get paid for your music being played in bars and on the radio, you've got to license all of your music to us and you can't choose to hold some back and share it under a Creative Commons license.

A Spanish court just this week disagreed with that. A bar was playing only music available under a Creative Commons license. It was not paying the collecting society any money. The bar was sued by the collecting society and the court said, no, your claim is based on unauthorized performance of music. This is authorized by the copyright owner, and therefore, there's no infringement here.

So there's an alternative copyright economy growing up, and the Creative Commons phenomenon is just an example of it. I think it's bigger than this. Yahoo! just bought Flickr. Right? Yahoo! had a business model and Yahoo!'s a global media company competing and trying to figure out how to make money as digital video and other forms of media become more and more popular. Yahoo!'s initial bet was we're going to be the platform for professionally created video content. We are going to be the extension of the television networks. We're going to be the video broadcasting platform, and they brought in the network executives to help develop this professional media platform.

After having bought Flickr, the culture of Flickr basically infected the culture of Yahoo! I'd say. As the young senior executives started to see the power of what they call user-generated content (what other people refer to as social media), they've changed their bet and have now bet that this is the future of where you're going to make money at least in an ad-supported business model on the Net.

This is the big year for copyright owners. It's not just peer-to-peer file sharing. It's competition from amateur-created content against professionally-created content. So when we talk about alternatives and enforcement regimes, that's within one version of the copyright model, but there's an alternative copyright model that's emerging on the Net. Creative Commons licenses are part of the infrastructure for that model as well as websites like Our Media or YouTube. Digital video is the next big thing.

I want to close by going back to peer-to-peer. If digital video is the next big thing, and there's a market for user-created content, there's a problem. Digital video is expensive to host and to transmit. The bandwidth is an order of magnitude above what is required for music files even after it's compressed.

In Creative Commons' submissions to the Court in *Grokster*, we tried to make this point. We tried to say the user-created copyright environment is going to need technologies like BitTorrent. It's going to need technologies to distribute the load allowing users to share and participate in the ecology, and copyright rules that make those technologies illegal make this form of social media in the video context very hard to sustain.

Now that may be part of the strategy of the professional media content owners to use those rules to undermine this competitive ecology, but I think from the Creative Commons' perspective, it's essential that when they create the copyright regime, leave space for this alternative relationship with copyright. And it's always been the Creative Commons' position that these two uses of copyright are not mutually exclusive. In fact, we would anticipate that professionally-created content would survive—thrive in fact—on the internet and co-exist with the social media universe, which is an underappreciated and growing phenomenon.

We started with music, so I want to close with music. Some MIT students started, as a project, a piece of open source software that we helped finish developing at a site called CC Mixter. The idea is you can go on this website, you can post samples. So if you have a great voice, nothing else, just sing the melody. Digitally record it. Put it out there, and say put this in your mash up. Do something with this. And a community of re-mixers has emerged out of this.

On the screen, is the South African version of Mixter. We now have a contest. I don't know if you've heard of the band Linkin Park? Well, they have a side project called Fort Minor. Fort Minor actually has a hit called "Remember My Name," and for those of you who watch the NCAA on ESPN, that's the tune you hear. Right? Well, Fort Minor, Warner Brothers, and Arista agreed to license "Remember My Name," for mixing and mashing up on CC Mixter, and so we're now having a contest that just

started. So they've taken apart the pieces of the song and you can remix it any way you like.

So we talked earlier about filtering. How you might implement a filtering regime, right. You're supposed to look for a file name called "Remember My Name," and now you will find that CC Mixter hosts a file called "Remember My Name Latin Version," which is an authorized Creative Commons licensed remix. But if the filter says that's an illegal song, then there's a problem. Right?

So the large copyright holders are beginning to participate in the user-generated, the social media universe, and I think this complicates some of the questions you talked about, but at this point I'm going to hear what you say. You've been very patient. I appreciate it very much, and would like to hear questions. Thanks.

RICHARD OWENS: Thanks. So we have indeed reached the opportunity to turn the tables on all of our panelists, not just Professor Oswald. If there are questions in the audience, please let's hear them.

AUDIENCE MEMBER: Could you touch on the politics of piracy in Sweden with Pirate Bay?

MICHAEL GEIST: I'd say I can't. Any of you know anything about it?

LYNDA OSWALD: No.

MICHAEL GEIST: Well, no. Pirate Bay was like a BitTorrent node.

AUDIENCE MEMBER: A tracker.

MICHAEL GEIST: Tracker? Okay. They have faced regular takedown notifications, yet they post all the various claims and say ha, ha, ha.

[Audience laughter]

Swedish copyright law so far hasn't done much about it. I think that reflects in parts of my comments today. Countries want to make choices. There are those that would argue that a U.S. approach that exports U.S. copyright law to other countries is a perfectly rational thing to do given that it may lead to a net economic gain, though we can argue as to whether or not that's true given what we've just seen about the amount of content that is created that doesn't rely on copyright incentives. But certainly from a Canadian perspective and perhaps from a Swedish perspective and many other countries, the reality is that we're net importers of culture. If you're a net importer of culture creating ever-stronger rules then you are likely to lead to more dollars being sent out of your country.

What you're mainly concerned with is ensuring that you've got a vibrant national cultural policy where you want to ensure that your own artists get airtime. We have Canadian content rules for radio, for televi-

sion, and there's lots of countries just like it. Why? Because we're awfully close, as you just heard, to the United States. If we didn't have some of those rules, we would only get U.S. content, very little Canadian content because the economics wouldn't make any sense.

This arises in the context of the IP choices that you make as well. Where if you make an IP choice that mirrors the U.S. approach, you've got to recognize that the economic impact may be a negative for your country at least with respect to royalty distributions. Although, of course, if it's traded for something else, that should make generally a benefit which is what we see happening in a lot of the other countries who are willing to enter into trade deals with the United States.

RICHARD OWENS: Yeah, but just one quick point on that. A net difference in intellectual property trade at any given point in time will only be sustained if levels of protection do not increase in the nation in deficit, and so forever ensure that it will be a net deficit in intellectual property trade. Right?

Without encouraging local creation, you're not being able to redress that imbalance. So it's also a part of the national division policy to try to redress the imbalance by copyright?

MICHAEL GEIST: No. Actually, a lot of countries can encourage the creation of national culture without buying into the notion that it's IP rights, stronger IP rights, that actually accomplishes that. You can, for example, ensure that smaller Canadian artists get more air time if there are incentives from radio stations to give more air time. You could take the money that would otherwise be transferred out and literally just hand it to the artist, if you like.

There's lots of different cultural choices that you can make that I don't think necessarily include stronger IP rights, but of course, that could be one. I think the kinds of examples that we're seeing with Creative Commons and others actually suggest that it is one of the least effective in terms of creating more cultural interaction.

AUDIENCE MEMBER: It seems to me that international IP treaties are not a new phenomenon. I was wondering how much you could address whether there is really a matter of new media, and how much it's a matter of increasing the strength of U.S. copyright laws—thus becoming a driver for other countries touched on this with trade treaties to support economic pressure. But the thing that made me think of this was Charles Dickens and that he talked about international piracy rights, and so it's been around for a while.

MICHAEL GEIST: Well, it has been. The U.S. domestic strategy of using both bilateral trade treaties as a way of upping the ante is a relatively new phenomenon. One way to test that is to go to the U.S. Trade

Representative's website and take a look at the various trade treaties, and you can see the evolution over time. You can, if you'd like, just read the Canadian free trade agreement, and you'll find there is very little in there that has to do with IP. In fact, there's even a provision that Canada insisted on that allowed us to protect our own culture. So culture's actually exempt from the trade treaty and the U.S. was willing to agree to that at that point in time.

Over time we began to see a shift. It happened in two ways. One, it happened at the international level and of course Pam's written about this, how there was an attempt to get DMCA-style legislation within the U.S. which proved unsuccessful. Instead, the U.S. went to WIPO, obtained the WIPO treaties, and brought it back to the United States, with new "international obligations" to fulfill.

And at the same time have a parallel trap at a domestic level where when you're entering into these kinds of negotiations, it increased the kind of pressure the countries are facing. Peter Drahos from Australia has written a lot about this.

MICHAEL W. CARROLL: The question refers to the history of "international piracy." If we define piracy as conduct that is illegal rather than something that's considered objectionable. The behavior Dickens was concerned about in the nineteenth century was not illegal at the time he was writing. In the United States, as we've heard, it was all about the political autonomy, and we were a net importer of intellectual property from England and he was an artist not protected under U.S. copyright law. It was not illegal to print a Dickens novel and not pay him a dime.

There was a "Gentleman's Agreement" among the publishers in order to get first dibs on a manuscript to pay some English authors, but Dickens, and then later, Gilbert and Sullivan, protested. In the 19th Century, the United States saw a series of repeated visits by high profile British artists saying to Congress, we want protection, we want international protection. And the U.S. resisted it until the end of the 19th Century.

So if complying with domestic law is piracy, then the United States was a pirate nation until the end of the 19th Century, but eventually we became a net exporter and the United States government has been pushing for stronger and stronger protection. The account that's worth reading is Information Feudalism by Peter Drahos and John Braithwaite, a wonderful telling of the story of how TRIPs—how the conceptual framework behind TRIPs was fashioned, and then the political moves for pushing that out.

AUDIENCE MEMBER: I have a two-part question for Professor Carroll, primarily. I just find the Creative Commons to be fascinating,

and one of the areas that you focused on in your talk is about music. And the specific question that I have pertains to these multiplayer online games. So for those of you who haven't seen this, it's just really interesting if you go to the game Second Life. There's this digital characterization of Lawrence Lessing who's involved, obviously, with the Creative Commons, and it's a remarkable likeness of him, and the likeness is basically him entering this online world and providing a lecture about copyright and the licenses to the users within the game, which I just thought that was really cool.

So my two-part question is number one: is Second Life a true exception? Are there game developers coming to you being interested in tapping into user generated content or social media, whichever way you choose to phrase it? And the second one is: to what extent does this also put you in a quasi-regulatory role in that your colleague, Mia Garlick, has written about gamers feeling entitled to content even when they actually don't have the legal rights to the derivative works based on the individual licenses? So to what extent do you actually serve a monitoring role about what gets offered for license through a Creative Commons site?

MICHAEL W. CARROLL: So let me take the second question first. We don't take any enforcement role, and we're not parties to the license. We've created the standardized license, but the licensor adopts that and says, "This is my license. These are the terms that I'm offering my copyrighted work under," and it's up to the licensor to enforce that license.

Our role is to provide the words and three ways to represent those words that we call the legal code, which is the formal license, the human-readable deed, which is sort of a description of the key terms, and then a machine-readable layer that identifies which license is attached to a digital object. We've just sort of created a standardized tool that they can use.

In terms of the online gaming industry, the issue is that copyright is so easy to attach. The minimal level of creativity required by copyright law is quite low, and in these interactive online environments where you're allowed to manipulate the media and create new derivative works, a copyright automatically attaches to those and then it becomes a legal issue of what is the legal status of that and how can it be shared. Second Life, I think, has been a leader in recognizing and making those resources open to other users who create greater value in the game and so those are offered under Creative Commons license. So that if you're in the game, what you create is part of the environment.

We have not been approached as far as I know. Mia would be better it seems to answer that. But for game companies, it's a business model choice whether the user-generated aspects of the game create enhanced value which should be open resources within that environment or whether you're going to have some form of control over the game resources, tight control.

RICHARD OWENS: While the next question is brewing, let me ask a quick one of Professor Oswald if I may. You suggested that there's room for a lot of empirical research. I'm wondering in which questions you might be most interested in terms of looking to see if IP regimes exist and also whether or not the uniformity and globalization kind of IP regimes might benefit the multi-jurisdictional laboratory effect that Michael Geist referred to.

LYNDA OSWALD: I'm sorry. What was the last part of your question there?

RICHARD OWENS: Sorry. The last part of the question is just whether, in the efficiencies of uniformity across nations we may not be foregoing, when different nations take different approaches, the benefits of additional opportunities for empirical observations arising from the disparity of conditions.

LYNDA OSWALD: In answer to the first part, I personally would undertake no empirical studies. I'm a lawyer and the fact of the matter is I'm not good at empirical studies. My business school colleagues trained in quantitative disciplines are good at empirical studies; they have the background necessary to do that. And I myself, while I can see issues I think are interesting, could never conduct that study. I wouldn't attempt to do so because it wouldn't be legitimate at the end of the day.

Which is not to say I don't think those empirical studies are important to do because I think we tend to look at these issues in IP from our own narrow perspectives. That's the perspective we have in the west, and we can't assume that other countries, people with other perspectives, will react the same way to changes in the law that we might expect we would react, and I think it's worth exploring what the effects of some of those changes might be.

But with respect to your second question, I do think Michael's idea of a laboratory of entitlements is a good idea because I don't think we can assume up front we know what the best international standard is. I don't even think we can assume that ultimately there'll be a single international standard. It might well be that we do need different standards around the world to accommodate different types of perspectives.

What I think that we will see, though, is that businesses, rights holders, and rights users are going to push for more standardization. My

business students don't talk anymore in terms of American business. They don't know what that means because they're looking at a company which might be incorporated here in the United States, but might be well getting its supplies from Canada, it might have its assembly done in Mexico, might have its call-center and its back offices in India. They recognize that indeed it is a worldwide web of business as well as a worldwide web of the internet itself. And that's true of hard assets as well as digital assets.

When I talk to business executives, they're not so concerned really about what the standards are as they are about whether the standards are predictable and clear. They don't expect complete certainty in the system but they want predictability.

I think Fred raised this earlier. Managers know if they send all of their tech information, for example, to a call-center in India, there's a risk associated with that. They're giving up valuable information. How is that information protected? Will it be protected? If it gets out, how can they enforce their rights against those who might have misappropriated it in some way? Those issues are very real to them, and I think what we will see are people pushing for a clearer playing field. Whether the standard is the same internationally is a different question. Whether it *should* be the same is a different question as well.

I don't think we'll ever get true harmonization. I just never see that happening, but I think we're moving in that direction, and I think that can be a very positive thing in terms of certainty and predictability in business relationships.

RICHARD OWENS: Any other questions?

MICHAEL GEIST: I actually thought we did have international standards called Berne and TRIPs. There are an assortment of international agreements that have been around for a very long time that do create minimum standards. Richard says you need this kind of legislation for Creative Commons. I took a look at all the flags that Michael displayed, and there were lots of countries there that allegedly don't have certain copyright rules, and certainly don't have anti-circumvention legislation.

So I don't think Creative Commons relies on it and frankly, I don't think that there's a great deal of business relying on it either. We have certainty. What we're talking about when we talk about the push at a bilateral level for WIPO-like standards and the WIPO Broadcasting Treaty Initiative or a whole range of other issues, they're not harmonization. What they are is a continual ratcheting up at the behest of a fairly small number of groups. It isn't about harmonization. We all know it's not about that. It's just about certain groups, Disney in particular, trying to

extend the life of a copyright for as long as possible, not about any kind of business certainty, whatsoever.

RICHARD OWENS: Any other questions?

SHARON ARMSTRONG: Thank you. Can we just have a round of applause for the panelists?

[Applause]

On behalf of our entire *Journal*, it's been our pleasure to have each of you in attendance for today's Symposium. I think you'll all agree with me that it's been an exciting day to hear this incredible group of panelists come debate and discuss the unprecedented changes that are coming about in copyright law that's succumbing the internet revolution.

It's been our privilege to have the speakers come and to have each of you come and hear what they had to say. We look forward to seeing you at the banquet at Campus Inn at 6:30 where we will have dinner and hear some closing remarks from our keynote speaker, Professor Pamela Samuelson. Thank you.

[Applause]