1-1-2004

Tracking Pirates in Cyberspace

TRACKING PIRATES IN CYBERSPACE†

*Jennifer Stisa Granick, Moderator**
*Peter Harter, Panelist***
*Mark Ishikawa, Panelist****
*Joe Kraus, Panelist*****
*Fred von Lohmann, Panelist******
*Kent Rowald, Panelist*******

MS. GRANICK: Welcome to the last panel of the day, "Tracking Pirates in Cyberspace." I'm going to introduce our panel today and then my plan is to propose to them a simple hypothetical and ask them to respond to this hypothetical. First on the panel we have, in order here, Kent Rowald. Mr. Rowald has extensive experience in all phases of intellectual property practice, including patent and trademark prosecution, litigation, licensing and general counseling. His practice focuses on litigation related to patents, trademark, copyrights, trade secrets and general intellectual property matters. He has been practicing intellectual property law for over 13 years.

Seated next to Kent, we have Fred von Lohmann. He is a senior staff attorney with the Electronic Frontier Foundation,[1] specializing in intellectual property issues. In that role, he has represented programmers, technology innovators and individuals in litigation against every major record label, movie studio, and television network, as well as several cable TV networks and music publishers in the United States. Before joining EFF, Fred was a visiting researcher with the Berkeley Center for Law and Technology, where his research focused on the impact of peer-to-peer

---

† On March 15, 2003, the Stanford Law and Technology Association (SLATA) presented a symposium on creating and protecting intellectual property in the international arena, or "Ideas Without Boundaries." The following is an edited version of the transcript from the conference panel and discussion. More information about SLATA and its conferences can be found at http://slata.stanford.edu.

* Director, Center for Internet and Society, Stanford Law School
** Managing Principal, The Farrington Group
*** President, BayTSP
**** Co-founder, DigitalConsumer.org
***** Senior Staff Attorney, Electronic Frontier Foundation
****** Partner, Bracewell & Patterson

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

technologies on the future of copyright law. He received both his undergraduate and law degrees from Stanford University.

Next, we have Peter Harter. Peter is a leading Internet law and public policy authority. He consults with a variety of early stage firms in music, security and microfinance. Previously, as Securify's Senior Vice President for Business Development and Public Policy,[2] he managed relationships with senior government officials and industry executives in various business development, legislative, regulatory standards and market development activities.

Next to Peter we have Joe Kraus. Joe is the co-founder of DigitalConsumer.org,[3] a grass roots consumer organization dedicated to protecting consumers' fair use rights to digital media and to safeguarding the ability of technology companies to innovate freely. Upon graduation from Stanford University in 1993, Joe founded the highly successful Internet company, Excite.

Next to Joe, we have Mark Ishikawa, who is the Chief Executive and Technology Officer of BayTSP,[4] a Los Gatos Internet intellectual property tracking and security company. Mr. Ishikawa is an expert in the field of Internet content distribution, spidering, electronic security, networking, database design, and has served in a variety of executive level positions in numerous Silicone Valley technology companies. You can read more about our illustrious panelists in the biographies.

So, here's my question for the panel: I own a small record label and film studio, and I suspect that a Stanford student or students are using the Internet to download and to upload my music and movies, using some very popular peer-to-peer software. Can the law help me with this problem? Is this illegal? Is there a legal solution to this?

MR. ROWALD: Is there a legal solution? Certainly there can be a legal solution and there certainly are legal issues associated with that kind of downloading. First off, I guess we're going to presume that your software, your movies or whatever, are copyrighted. Whether they're registered or not, they are copyrighted as soon as they are created. And although Carl mentioned that, yes, you need to register those copyrights, and I wholeheartedly agree with him, you do have a copyright in those as soon as they're created. You just are giving up rights if you don't have it

2. Securify, Inc. can be found at http://www.securify.com.

3. DigitalConsumer.org works to restore the balance between citizens and copyright holders and protect fair use rights in the digital environment. DigitalConsumer.org can be found at http://www.digitalconsumer.org.

4. BayTSP's customer objective is containment and compliance by "Tracking-Security-Protection" for digital assets. BayTSP can be found at http://www.baytsp.com.

registered. So regardless of whether it is registered or not, you do have some protection there. Now, you're going to have to register it before you file suit, because that's what the statute requires.[5] But nevertheless, there are some legal issues involved there and it is illegal to be copying those.

I think the first thing that you've got to do when you have that kind of a question brought in by a client, is to look at who are your potential defendants? And then, who do you want to sue? And I think those are two very different issues because your potential defendant is a much larger universe than who actually gets sued. And there are a lot of different reasons for that. Like when you look at your potential defendants, the university itself could be a defendant. It's more interesting when you've got a state university rather than a private university because then you've got all sorts of immunity issues involved. If you look at the *Chavez v. Arte Publico Press*[6] case, that kind of tells you a little bit about the copyright immunity issues that universities look at. The private universities may or may not have some of those immunities depending on where they are and . . . the [relevant] state laws . . . . If you've got a separate ISP that you're looking at, you may want to look at that ISP as a defendant. The student who uploaded the file, [is] very likely a defendant, is a very likely candidate. The student who downloaded may be a candidate to get sued. The creator of the peer-to-peer software that was used may be a defendant if he is contributing or inducing that infringement. The distributor of that peer-to-peer software, as we heard on the last panel, may be a defendant. If it is being used through a specific domain, you may look to the domain name owner and skip some of these other people, or go strictly to the domain name owner. [I]f you can shut down the domain, you've put a big kink in the distribution network. Who's the website host? You get to the Digital Millennium Copyright Act stuff with that on going after the host, going after the ISPs both that way. The peer-to-peer search engine host, if that's a separate person than the peer-to-peer network themselves.

MS. GRANICK: Well, that sounds, that sounds great. It sounds like I have a lot of options. But why do I have to put the money out for this? Why doesn't the government help me? Isn't this, you know, if its theft, isn't this kind of, like more of a government problem, Peter?

MR. HARTER: That's a very important question, I think. How long money can be spent, tax payer dollars, can be spent on enforcement of laws, and whether copyright law should be enforced with civil and criminal means. We can talk about that. We see an expansion of that in the past ten

5. 17 U.S.C. § 411(a) (1976).

6. 157 F.3d 282 (5th Cir. 1998).

or fifteen years in the U.S. and other countries. But at the end of the day, do we want local law enforcement officials spending their finite time and resources, based on their little training, going after someone downloading music illegally or going after really bad people? Now, of course, you could argue, as an artist, that someone who downloads thousands upon thousands of copies, burns CDs and sells them, they could be a really bad person, so this is very subjective to some degree.

But I think one topic to think about, especially in the international context is, and it goes to something Mr. Hadley mentioned, his remarks, his two points of enforceability and the damages. How many countries have actually ratified the 1996 WIPO Copyright Treaty? I spent a month in Geneva in December 1996 [when] that great treaty was passed. And the treaty, over the month long negotiation, was a five-year process preceding the treaty conference at the diplomatic level. Things like folklore, which many people in Africa and other cultures outside of the Western legal system and cultural system would think needs international recognition, folklore was dumped out of the treaty because the African block was not economically relevant to the people at the conference. Database was dumped out because the industry people on that issue couldn't come to agreement. Other things were dumped out, and Internet was all the rage in '96. And, I think a lot got lost in the shuffle. We have all of these countries, 150 plus countries for the first time, looking at having copyright law when these countries . . . have far more significant problems for their people than enforcing copyright property rights from Western interests. We're talking about developing countries. Countries that don't have law enforcement, [that] don't have a stable regime, and so on. What is the public good of enforcing copyright in this manner?

And I, as you can see from my bio, I used to work for a music company call EMusic,[7] now owned by Vivendi Universal. It is actually making money, and it sells music in the open MP3 file format. It has the most number of tracks available on the net legally, and the most number of paying subscribers. And their subscriber bank is growing. So I think we see litigation, as law students, and I'm a lawyer as well, we look at the public policy context internationally. [We] look outside the U.S., about how artists in Africa want to get their music online, and look at music from other cultures and . . . priorities in this country. I think you'll see that. Do you want the local FBI enforcing copyright or going after other social issues? And you can argue on both sides, but I think there's just another context here. Do not look at a Stanford student necessarily as someone who is a

7. Emusic can be found at http://www.emusic.com.

priority for our tax dollars to go to work on.

MS. GRANICK: What's the view from—Fred do you want to respond to that?

MR. VON LOHMANN: Yeah.

MS. GRANICK: You look like you do.

MR. VON LOHMANN: I just want to jump in for a moment and suggest that perhaps you, as the small record label owner, should, while there are no shortage of lawyers that will give you very good advice on all the options you have on copyright law, you may want to realize that if the students at Stanford are downloading music from your artists, that suggests you have fans at Stanford. Maybe you should be booking the coffeehouse, and maybe you should be seeing why students at Stanford like your artist's music and whether or not there's an opportunity for you to grow your audience, grow your fan base, deliver additional products to the Stanford community, rather than exploring whether or not you can kill the Stanford.edu domain name.

(LAUGHTER)

MS. GRANICK: So are you saying there's a business downside to my going after Stanford students?

MR. VON LOHMANN: I was suggesting that there's a business upside toward your—that could come from your understanding where that demand comes from. I agree, however, that there is a serious business downside. If word snuck out in the Stanford Daily, for example, that your record label and your artists were behind a campaign to hunt down Stanford students, I might suggest that that may not be in your long-term business interest. However, I agree with Kent, there's no shortage of onerous copyright tools at your disposal. You could take the course that Vivendi Universal took earlier this month and deliver 155 complaints in one day to the University of Wisconsin about file sharing.[8] You could do that. You could deliver a subpoena to the Stanford University demanding that they identify the student behind a particular IP address. You could spend money on services such as those perhaps being sold by companies like BayTSP and others in order to identify more IP addresses at Stanford. You could do all those things, but I'd suggest that after you got done doing all of them, you would have not a single additional sale of any product of yours. You would not have converted one additional fan for any of your

8. Subsequently, the RIAA sent out 261 lawsuits in one day, signaling a strategy to combat file-sharing including going after the individual users. *See* Benny Evangelista, *52 Piracy Suits Settled*, S.F. CHRON., Sept. 30, 2003, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/09/30/BUGSF214IF1.DTL.

artists. And I'd say maybe that wasn't the most productive use of your time.

MS. GRANICK: Kent, is this true?

MR. ROWALD: That is very true. That's why I said when we started out here, you've got all these potential defendants, but they may not want to be actual defendants in a lawsuit. You might not want to sue all these people. It could hurt your business in the long run. I think you've got to look at your client's ultimate goals. What is their real goal here? Are they trying to shut down the university computer? Are they trying to determine what their market is? Are they trying to protect a particular market? Are they trying to punish a student that went out there and downloaded 600 MP3s? Do they really want to go after the guy that downloaded one, or do they want to just identify him, and say—hey, he's a potential customer? So you've got to look at what those goals are before you can determine who is going to get sued, and if anybody is going to get sued.

MS. GRANICK: So Joe, you spend a lot of time in Washington. What's the government thinking about this problem that I'm having? It seems like litigation has its up sides and its downsides for me. Does my friendly government have anything that they can do for me, here?

MR. KRAUS: I think one of the challenges is that the government over the last, certainly, forty years has viewed copyright issues really as not a matter of balance, but rather [as] one of enforcement. I think that, generally speaking, it is particularly the Judiciary Committee and to a lesser degree, but still nonetheless, the Commerce Committee tends to view these issues as, "well, this is really about just giving copyright holders greater and greater authority," as opposed to necessarily viewing the kind of historical balance that seems, at least to me as a non-lawyer, to be at the foundation of the Copyright Act. I would agree also on the previous question with Fred's comments. Is it worth it? I think that the content industries generally are facing an important question these days, which is—beat it or join it? There was a recent study by KPMG,[9] the consulting firm, that found that eighty-one percent of—I think this was specifically focused in the music industry—eighty-one percent of the music industry executives were actually more focused on prosecuting violators and the encryption of content than they were on actually addressing the market. And I would say that the hypothetical example that you give is framed in that exact light. Most people are focused on, instead of addressing the market, or joining the market, they're focused on how do we stop the illegality before we even put that toe in the water? And I commend the music industry actually,

9. KPMG International can be found at http://www.kpmg.com.

over the course of the last year, for really starting to change course and move into the category of joining in.

MS. GRANICK: So I hear what you're saying but I'm still not happy with the idea that the people are trading my things that I would prefer to sell. And so, Mark, I come to your office and I want to know from you, how can I tell what kind of possible loss I'm experiencing here? And how could I find out who these people who are trading my copyrighted material are?

MR. ISHIKAWA: Some of our clients come up to us and want to find statistics as to what their level of damage is right now. We're working with one of the studios now to determine what the effectiveness is of alternate technologies, including tracking. And what we do, we'll go through and spider the Internet, get an idea of what's been made available, and get a rough idea of how many downloads are occurring at a given time. So, that way the client can now figure out what their damages are, what effect—or what enforcement actions they'd like to take. Our system has been designed to issue Digital Millennium Copyright [Act][10] notices. We send them out to universities. In fact, we have a quick report here that I'd like to show you of Stanford violations that we've discovered.

(LAUGHTER)

MR. ISHIKAWA: Since December 10th of last year. Put this up.

MS. GRANICK: Just as I've suspected.

MR. ISHIKAWA: So you can tell from the period ending December 12 to March 14, we've discovered, oh, 20,000 violators of our client's material that has originated from Stanford University.

(INAUDIBLE)

MR. ISHIKAWA: I'm sorry. Which number are you referring to? Oh, the total infringement count which is a summary report—19,635. We can tell you by protocol. We can tell you how it's been distributed. We can tell you geographically where it's coming from, the file types. And actually, Adobe is one of our clients, and we know that we have sent several notices to Stanford where it has been discovered Stanford was making available, publicly for download, Adobe software. So we sent out the notices, Adobe authorized [us] to send out the notices. Stanford immediately took down the users. We find people all over the world that are sharing files. One of my favorite stories is we caught a student at Harvard University downloading huge numbers, or making available, huge numbers of files belonging to our client. We sent the notice off to Harvard. We got a response back that says that the student's punishment was to write

10. 17 U.S.C. § 512(h) (1998).

a paper on copyright law.

(LAUGHTER)

MS. GRANICK: When you find something like that, who do you contact at the university? Do you try to figure out who the individual person is, or is there some other entity that you get in touch with?

MR. ISHIKAWA: We typically go to the copyright office for the DMCA registered agent. If that is an invalid address, then we'll go and contact the people who administer the network, and they'll typically tell us who to go see. We have an extensive database of about 100,000 DMCA contacts. The one problem that we have is that the DMCA database, or the registered agent database is a PDF file, and there is no electronic version, and it's very out of date. Seems like everybody in the world started filing for DMCA protection,[11] including corporations, when they really didn't have an ISP status to fall under.

MS. GRANICK: So that means it's hard to figure out who to write to?

MR. ISHIKAWA: No, actually we have, throughout the years, we've been doing this for four years—we've built our database. We know who to call, or who to contact. One of the things that we like to do is we like to enlist ISP cooperation, versus just sending them a million notices. So what we'll do is we'll work with the ISP as they get what's called a cooperative flag, and then we'll send the take-down notices in a format that they find acceptable.

MS. GRANICK: What if there is no ISP, or what if the ISP is out of the country, located somewhere else? It's not Stanford University but let's say Oxford University?

MR. ISHIKAWA: We've been able to get compliance worldwide. In fact, our record so far is twenty-three minutes from notification to take down in Austria at three-a-clock in the morning their time. A lot of the ISPs—unlike the U.S. where you can just go buy a router and an Internet connection and, suddenly, I'm an ISP—a lot of ISPs are government regulated. So they understand they have obligation under the Foreign Convention of Bilateral Trade.

MS. GRANICK: Well, that sounds pretty easy. What's the downside of my doing that, of my getting a firm like BayTSP to write to Stanford University or wherever these peer-to-peer networks are sharing my information and getting them to shut this stuff down?

MR. ISHIKAWA: For us, it's a matter of, you know, we can send

11. 17 U.S.C. § 512(b)(1).

out all the notices you want. We can get the content taken down. It's a company policy decision or copyright policy decision to determine whether they want to go after large pirates. We have two categories of pirates. We have the casual infringer who really didn't know that it was bad. Typically, once we send out a notice, we get two types of responses. One is, F–you and the other is, I'm sorry, I didn't know any better. Typically our copyright holders that we work with want the content to go away. We work with some organizations in the U.K. in the record industry where they're asking us to target people who have large volumes of content being published. We find upwards of 60 to 100,000 MP3 files, movie files, [and] software packages being made available. And those are what we'll call professional pirates that the copyright holders really want to go take care of.

MS. GRANICK: And so, let's say this is what I want to pursue. I want to try to stop the professional pirates. I also want to minimize the kind of sharing of my stuff that goes on. Can technology, is there technology in the works or stuff I can do now to my content that will help me either prevent infringement or help me find infringers after the fact?

MR. ISHIKAWA: Yeah. Let me talk about a couple of technologies. I don't want to take over the whole panel so I'll give you a little bit of insight on the technologies available. There's watermarking which has been around for a long time. Digimark is the premiere provider of that technology. The problem with that type of imbedding technology is you can't find content that was distributed prior to watermarking. So if you have a picture that has been on the Internet for a couple of years, and you suddenly say, I want to start protecting it, every digital copy that was released previously is untraceable using watermarking technology. There are other technologies, called interdiction, where tech companies will try and poison the files or make the files unavailable on peer-to-peer networks. And the problem is there are millions of users and the interdiction companies may have a couple of hundred machines. So the problem is you really can't poison the network effectively. It just is not possible. Once one copy gets out, there really is no way to stop the viral distribution.

MS. GRANICK: Is there any problem with these kinds of technologies? Maybe I should start watermarking and fingerprinting my stuff and putting DRM on it. What's the downside of that?

MR. VON LOHMANN: I want to jump in here for a moment and offer, while I think there are a number of technologies coming on line that offer rights holders various options, including the ones that Mark discussed, I think it's important to notice a few other trends at issue here. I encourage everyone who's interested in this question to look at a paper that

was published by several senior Microsoft engineers, back in November, called *Dark Net and the Future of Internet Distribution.*[12] You can Google for Dark Net and Microsoft and pretty reliably find it. It was a paper presented at an ACM conference in November in Washington.[13] And in it the four Microsoft engineers, all of whom are actually senior people in Microsoft Security Group, looked at this question of whether or not technological measures could reliably stop peer-to-peer file sharing. And after looking at the question, they concluded that the answer was, "no." That, in fact, you may be able to use technical measures to slow down or stop certain existing file formats, but that new technologies would arise that would be increasingly resistant to the tools you have at your disposal. I'll also mention to everyone here that Freenet is due for a new version, I believe on Monday, that is going to be much more user friendly than prior incarnations of Freenet.[14] For those who aren't up to speed on Freenet, it is an entirely encrypted and anonymous file sharing network that takes advantage of a lot of different features that make tracking much, much more difficult. I won't say impossible. I'm sure Mark and his folks are working on ways to trace that now. But the reality is it's going to make a lot of this much more expensive and difficult to accomplish.

So all the while, the question for our rights holder is: Is this the most plausible and practical course of action for the long term? Is this the right way to explore "protection" of your content assets? For some people it might be. I suggest that for many, perhaps most, it's probably not in the long run a terribly effective measure. I think, what you might want to consider, what we at the Electronic Frontier Foundation have decided it's time to consider, are some alternatives. Compensation is probably your chief concern. You want to be paid. You want your artists to be paid. That seems a fair demand for content owners, and for artists themselves, as a matter of fact. There are other ways to address the compensation problem other than ever-spiraling efforts to interdict, invade your customer's privacy and otherwise break the Internet effectively. Those measures include compulsory licensing, which is something that we've done in this country in many other circumstances, including web casting, cable television, [and] music publishing. It's a tried and true solution in our copyright history for new technologies that prove resistant to our traditional property model.

---

12. Peter Biddle et al., *The Darknet and the Future of Content Distribution, at* http://crypto.stanford.edu/DRM2002/darknet5.doc (last visited Nov. 1, 2003).

13. The Association for Computing Machinery (ACM) can be found at http://www.acm.org.

14. More information about the Free Network Project can be found at http://www.freenetproject.org.

MS. GRANICK: Well, I'm not sure I like the sound of that. And I'm not sure I like the sound of this Freenet either. Mark, is this true that you aren't going to be able to find major pirates who are distributing my stuff over services like Freenet or Bit Torrent?

MR. ISHIKAWA: We have heard every developer of a new protocol say you can't trace us, you can't track us. You know, my background, twenty years ago, I started working for the Lawrence Livermore National Laboratories, and we actually tried to come up with, when we first created BayTSP, we tried to come up with a digital rights management solution. And I'm pretty good at cryptology. I'm fairly decent we'll say. I can get into almost anything. So every technology that I created I would send it back to my friends at the labs and they'd say, "no, this is how you get through it." So, I don't believe that there's ever going to be a technology where the content will be completely hidden. And the way we view it is if it's two or three people sharing files with a private PGP type encryption, the damage to the copyright holders is very limited. When it starts getting into wide mass distribution, then you really can't keep the key secret or you can't keep it locked. Because everybody has to know how to unlock it, and while we're spidering the Internet, we're finding the ways that they lock it.

MR. KRAUS: I would say two things. One, it's interesting to look at, when it comes to DRM technologies, the different approach that the software industry tends to take than the kind of entertainment content industries, because there's a lot of history here. If people remember in the early '80s in the software business, everybody was layering on essentially relatively crude DRM systems back then. And what software companies found is two things. One, it didn't actually stop piracy because motivated people figured out a way. As Mark was saying, everything is essentially circumventible in some way. So, motivated pirates found a way around it. The second thing that they found is that it actually punished their paying customers, because it tended to alter the expected behavior of the software. In the early '80s it was essentially you weren't able to make back-up copies of software and you weren't able to— when you bought a new computer— upgrade it from that lovely XT to an AT machine or something like that. You weren't able to move that software package from one machine to another. And so what the software industry generally found is that the better way to do it is to embrace your customers, and then use enforcement mechanisms, as opposed to protection mechanisms, to go after the people who truly are stealing your content. I think, unfortunately, that lesson has in some ways been lost. And that's why, actually, in Washington, you don't see, generally, the software industry coming and saying what we need is a

Hollings-style bill.[15] We need a bill that puts content protection on every digital device. Because the software industry generally knows, wait a second, it's not going to work. But I think the content industry hasn't actually picked up that lesson—and that's unfortunate.

MR. ISHIKAWA: Let me add one other thing. One of the things that we've discovered with digital rights management, which is one of the key things to our technology, is once somebody finds a way to break the digital right management solution, which happens—if you remember the Charlie Pride CD that came out, that was broken in the first five minutes that it hit the store. Our company is able to—we're like the safety net. We're able to find and identify content even after the digital rights management solution is broken. The problem that you have with the digital rights management solution [is that] you can actually create one that is absolutely bulletproof. but your user, your typical home consumer user, would not be able to use [it]. So it would become ineffective.

MR. KRAUS: And when I listen to this it's funny. And this whole debate about—having been involved in it now for several years—it feels like a full employment program for many new kinds of technology businesses in DRM and a whole host of lawyers, because—

(LAUGHTER)

MR. KRAUS: Because essentially we're fighting an escalating war, right? We're fighting an escalating war between those who wish to suppress piracy and those consumers who essentially are out there demanding digital downloads. And I think the real challenge here is—one, to me it is actually a market failure. We aren't seeing enough people that have content addressing the legitimate market place with terms and conditions that consumers want. And I would tell you that when you have a music download service that allows you to burn ten songs a month and that's it, that is not actually addressing the market effectively. You essentially are creating a full employment program for an escalating battle. So, I would invest in Mark's company because I think there is no shortage of people who want this, and until the market's actually addressed properly, I think the opportunity for more and more jobs in that arena is there.

MR. ISHIKAWA: I'd also like to add one thing. We hear the term digital piracy or pirates. When you think of the word pirate you think of a

15. Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002) (introduced by Senator Fritz Hollings (D-SC)). The bill proposed "[t]o regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes."

guy with a patch. You think of sitting in the Caribbean on a beach in a boat. It's really not digital, it's not digital piracy, its digital theft, okay? They have all, you know, you see it in the paper, and I come across [as] the absolutely draconian guy, of course—but you see in the paper how they claim it's a victimless crime. It really isn't, because our clients, who own the copyrights, need to maintain and control them. Otherwise, who's going to create movies, who's going to create music, if there's no revenue model behind it?

MR. VON LOHMANN: Okay, wait just a minute.

(LAUGHTER)

MR. HARTER: He was baiting you, I think.

MR. VON LOHMANN: I think so.

MR. HARTER: Entrapment?

MR. VON LOHMANN: At a time when, to take one example, the motion picture industry is having the most successful year in world history to say that they are having their economic legs cut out from under them by file sharing is nothing but pure fantasy. And in fact, the record industry, although they are suffering a bit, I know a lot of airline executives that would gladly trade places with them. The notion here that file sharing is the imminent demise of the content companies is belied by the numbers in all sorts of areas of media. In fact, at a recent conference, a major record label executive announced proudly, the sales of our big hits on the Eminem records is actually doing better this year than it has in years past. So it's not actually the case that file sharing is solely to blame, or perhaps even to blame at all. I think that the empirical jury is very much out. And for people to say this is theft, that it is not a victimless crime, every download is a lost sale, I think is frankly, just simply not true.

MS. GRANICK: Well, I'm the owner of this record company and I think I should be able to, you know, not only sell to who I want, but I also want to know who my demographic is and stuff like that. So I kind of want to keep better track of who has my stuff. And it seems like what you're saying is that prevention isn't really so much of a choice. There's all sort of things I can do for enforcement later on, after somebody's already infringed my copyright. What kind of legal tools are there for me to help track some of these people down, whether they be individual infringers or more large scale?

MR. ROWALD: I think there's a couple of things you've got to look at here. First, obviously, Fred is looking towards a market solution. Mark is trying to lock it up. And I think you've got to look at both as a practical matter. And I think what Mark's talking about is kind of like locking the doors in a record store. It keeps honest people honest. People that are going

to want to rip off that record store are going to go through that lock, whether you've got it locked or not. So I think you've got to look at it that way. And I think that, ultimately, we're headed towards a BMI, ASCAP, SESAC type solution to this problem, where you're going to have compulsory licenses, like Fred is suggesting, that we're going to have to have. I think we're also going to be looking at companies going after somebody that's downloading that 600 or 700 or 800 MP3s. And, as a practical matter, you're not going to get any money back out of that. You're going to go after that Stanford student that's really done it bad, and you're going to hammer him for lots and lots of dollars. You know, if he's downloaded 500 MP3s you're going to hit him for 750 bucks per MP3 because that's your statutory right.[16] And then you're going to publicize that like crazy so that you've got a deterrent effect for everybody else that's out there. They'll come to your website and buy that MP3 from you instead.

MS. GRANICK: Is that what you think is going on with the *Verizon v. RIAA*[17] case where the record industry served subpoenas on Verizon?

MR. HARTER: I think that's largely what's going on there. I think the record companies are going through Verizon to find out who the ultimate downloading person is, so they can say look, I've got to make an example of somebody out there that's a real big thief. I've got to hammer them.

MR. ISHIKAWA: There's this misnomer on the Internet that you can be anonymous. And that people—you can do things on the Internet and not be held liable. You can hide on your AOL dial up account. It really goes back to the real root of the problem, which is the mindset of your digital thief. I'll refrain from using that word here. But your digital infringer.

MS. GRANICK: That's the officially sanctioned word of the panel.

MR. ISHIKAWA: Okay; very good. But what you're going to find is, when I was growing up, if I wanted some music, I saved my pennies, and I went to the store and bought a record. And if somebody were to share that piece of music, it's like the Betamax scenario, where you know, you can only make one digital copy at a time. The mindset of today's youth is I need to go home and download this instead of going to the store and buying it. So that's where the real problem is. And going back and identifying, you know, the people and showing the consumers or the Internet users that you

16. *See* 17 U.S.C. § 504(c) (1976).

17. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., (In re Verizon Internet Servs.), 240 F. Supp. 2d 24 (D.D.C. 2003).

can't do this, it's illegal, and this is what happens to you. You make a little example out of them. People understand –

MS. GRANICK: What does that have to do with anonymity?

MR. ISHIKAWA: As far as anonymity, people think that they can do this without being caught. I mean, we're able to identify somebody who's making a file publicly available. We go back to their ISP. We can identify that individual through their ISP. We've successfully done this with the subpoena process prior to the Verizon RIAA case for three years. The first time we went to the place where you file these things—excuse me, I'm not the lawyer—you know, they looked at us and said, what are you—you're out of your mind. There's no judge's stamp on this. So we worked with them, and worked with them, and finally they said, okay, here's the DMCA, here's how you get the subpoena, we're the authorized copyright agent. We get it stamped. We get it served on the ISP, and we get the identity of the infringer. Typically, when that occurs, we'll send a FedEx letter to that person and say, "knock it off or else a lawyer's going to be knocking on your door." And then we get the response that says, "I'm sorry, I didn't realize it was illegal." But the mindset really is instead of going home—instead of going out to the store and buying it, I have to go home and download it, and that's the biggest problem for our customers.

MS. GRANICK: So, isn't that a good solution for me. I can find out the IP addresses of these people who are uploading my stuff?

MR. VON LOHMANN: Well, to start with, if you really wanted to contact the user of a peer-to-peer system and warn them, please stop doing this, what you're doing is infringing. There are a lot of ways to do that. Kazaa, for example, includes an instant messenger function that will allow you to do that without having to actually serve subpoenas and violate somebody's anonymity in that fashion.

MS. GRANICK: Well, what's wrong with violating their anonymity? Why should I be worried about that?

MR. VON LOHMANN: That's where, as a lawyer, I get concerned. The Supreme Court in this country has recognized, on numerous occasions, that there is a constitutionally protected right to anonymous speech. Now, it's not an absolute right by any means. There are plenty of occasions where that right can be abridged on a proper showing. The difficulty here, however, is the DMCA, for the first time in federal law that I am aware of, has authorized a pre-complaint, blanket subpoena power that allows you, essentially by going into court, signing a piece of paper, to abridge someone's right to anonymous speech without any due process at all. Without any possibility of a judge having an opportunity to review that. That, in our minds, is a serious change of the status quo. And, this is

nothing special about the Internet. I would feel exactly the same way if someone were entitled to get my name and address simply by serving a subpoena on the post office, or on my telephone company, or on a magazine I happen to subscribe to.

MS. GRANICK: But this isn't speech. This is copyright infringement.

MR. VON LOHMANN: That's the interesting thing. We don't know, right? At the time the subpoena is issued there is nothing more than a raw allegation. That's exactly what the due process guaranteed in other contexts is intended to address. Is this speech or is this infringement? If it's infringement, then okay.

MS. GRANICK: Mark, is there any way that I can tell whether this is actually infringing? I mean, how do I know that these people are really putting out my stuff as opposed to something else?

MR. ISHIKAWA: Using our proprietary technology, we are able to identify positively or negatively whether it is the infringement area. In the case of a movie, we can tell you what movie it is. We can verify it against the original content that's been supplied to us by the studio. In the case of music, you know, we get CDs. We'll validate the content. So we have positively identified the content prior to the issuance of that subpoena.

MS. GRANICK: But I hear a lot of—Joe?

MR. KRAUS: Mark's statements not withstanding, there are certainly examples, that are pretty well known, of any time automated law enforcement is essentially in place, technology is brittle. It tends to be pretty dumb. But these issues are very complicated. And so, I'll just read something from a brief that was filed against the RIAA on an issue of automated law enforcement. The lists are basically the lists of files that were claimed of being copyrighted, and which were being shared on, I think in this case, it was Verizon's network. The list has not even been culled to eliminate items that should never have been included in the first place. "While most works which were identified appear to be songs featuring George Harrison, the note also demands removal of a file labeled 'John Lennon, Yoko Ono and George Harrison interview.MP3.' The notice further objects to a file, 'Portrait of Ms. Harrison Williams, 1943.jpeg.' It even claims infringement by distribution of a file whose appalling title includes phrases such as 'nude preteens and young teens naked, Brian is 14, and Harrison is 8.'" The point here is, in looking for items of George Harrison, you run into a whole host of things where automated law enforcement, again, is dumb. And any human actually looking at that goes—well, that's dumb. We'll throw that out. But clearly, in many cases automated law enforcement is making mistakes where, in certain cases,

other criminal activity is occurring, and in other cases it was clearly non-infringing uses. So I can't speak directly to what Mark's technology does, but certainly there are examples in the market of mistakes being made.

MR. ISHIKAWA: Just to clarify our technology. It is not automated law enforcement. Our system detects and brings it to the attention of the copyright holder. The copyright holder reviews the material to make sure it is what it is supposed to be and you know, pushes the appropriate button and has the appropriate action taken. The Verizon case was a great example. One of our so-called competitors sent out an infringement for a Harry Potter book report when, in fact, they were claiming it was a Harry Potter movie. And that's why we're in business and they're fading. We don't make those mistakes.

MS. GRANICK: Peter, what do you think about this? What about businesses like Mark's? What about copyright owners wanting to go after pirates, the infringers, either individually or people who are in this more as a business?

MR. HARTER: I would think it would be a very good business to invest in. But without speaking too much out of school, there was a company in London called Copyright Control Services, and for a variety of reasons they decided to merge with another company in Oregon. This was during the height of the Internet boom when the rush to get on NASDAQ and to get the liquidity of stock in America was the goal for any company, especially those in Europe where the market move was not as swift as it was here in the Wild West. And I visited with these people thinking, they came to Emusic when I was with Emusic, saying, well we can help enforce your copyrights. We can track down people who are pirates. I said, well, we just like selling MP3s and people pay us for it, and so we're not going to spend resources on chasing down people who are really pirating them. But we struck up a conversation and visited their offices, and talked to the staff, and talked to the CEO. He got profiled in Wired and all this stuff. He used to be a roady for a rock band doing the soundboard stuff and produced bands. When he hunted down people, they hunted him back. And, in his office on his computer screen he showed me the email of one of his targets, taunting him, the text, and then had a satellite photograph of his home, and this executive got in touch with Scotland Yard and sent in a special unit of Scotland Yard, and found this boy at his mother's house, and bomb making material and all kinds of things. You're going to find very unsavory characters in this business.

Going back to the business side of this industry that Mark's involved with, again, whether because they did a reverse shell merger with this dubious security company in Oregon and they had unsuccessful floatation

on NASDAQ and they imploded, revenues went down. One story my friend at Copyright Control told me early on, they lost a major contract. They were doing work for Adobe, for the National Federation of Phonographic Industries and other rights holders. FP, for example, is very happy with their services. All of a sudden FP's sister organization, the RIAA in Washington, D.C., merry band of lawyers that they are, suing people, told FP we don't like the fact that you're allowing your enforcement activity to be conducted by this private company. We're in the business of doing that. I'm grossly summarizing a conversation from four years ago. But as a lobbyist and a lawyer and a policy person, I can see how that could, hypothetically at least, be construed. What would the RIAA benefit by having policy being made in the market place by market based solutions, whether its Copyright Control Services or Mark's company? So I wish Mark luck, but I think, watch out for unsavory people targeting your home and you better know people with the FBI and NSA and other people who will protect you and your family, because there are some strange people out there that don't like being tracked down by services like yours. It's not a warning from me, it's just an observation. This poor guy. He seemed very calm and collected about it. It was a joke to him. But, I thought, gee, I don't want some bomb making kid chasing down me at my home. And again he was a roady in the '60s for a rock band so I guess he's seen worse fights and he was a pretty tough character.

MR. ISHIKAWA: Just so you know, I'm ex-department of defense. I'm not worried. And we've had the same scenarios with the satellite picture, looking up. Everybody knows I have a racecar. I have training for the aerobatic team. They've done the whole research. If you go to Slash dot,[18] you will see my name and about 1,000 different posters about how bad we are.

MR. HARTER: Is the racecar a Porsche because my friend in London had two racecar Porsches. Strange pattern?

MS. GRANICK: A characteristic.

MR. HARTER: He was a spy for GCHQ.

MR. ISHIKAWA: But the other thing is we are not the enforcement arm for the client. We give the client the tools to become their own enforcement. So originally when we first had the conception of the company, my name was on the bottom of every one of those notices. Now we make the client do that.

(LAUGHTER)

MR. ISHIKAWA: So we're giving the client the tools. We detect the

18. Slashdot can be found at http://slashdot.org.

content, we give them the infringements. We say, okay here's what we detected. You make the determination what you want to do. So we do not pull the triggers per se. We let the client make the determination what actions that are appropriate.

MR. VON LOHMANN: Before anybody rushes out to make an investment decision on anything said on this panel—

(LAUGHTER)

MR. VON LOHMANN: Let me just offer a slightly different perspective. While I certainly have a great deal of respect of Mark's company, they've managed to do a great deal of complicated technical work in this field, I'd suggest that maybe you want to look at a company like Big Champagne,[19] for example, an L.A. based company that's focus is not on tracing and interdiction, but rather on tracing trends in peer-to-peer file traffic. And in fact, Clear Channel has apparently just licensed their results for distribution to their radio station affiliates to basically say to people, listen sixty million people are using Kazaa. What they like to listen to is actually an important piece of market information. Rather than using that information to hunt people down maybe we should be using it to build a business.

Now, I think we're frankly facing a rather stark choice in the next coming couple of years. We can either choose to continue down a path where we characterize the enormous demand for digital media as theft, and as criminal conduct worth violating our privacy rights, worth deploying thousands of people who might otherwise find other lines of work into areas where they essentially hunt down people behind IP addresses. Armies of additional administrative staff and ISPs to address the tens of thousands of notices that come flooding in from companies like Mark's. All of this in an environment where none of this activity gets any single artist paid one red cent. Or, we can think about a world where we address the fundamental problem, which is that of compensating owners and artists while addressing the demand instead of criminalizing the demand. Saying clearly there's a need here and clearly the content companies have failed to address it. I agree with Joe there are some signs of hope but come on people, Napster showed that it was ready to be done years ago, and still we have, with the stark exception of Emusic, almost nothing out there in the music space that offers a terribly compelling value proposition. So that's why I say, let's talk about compulsory licensing. Let's talk about collecting a pool of money from users, in exchange for that making their activity legal, rather than hunting them, encouraging them to share as much as they can. The more

19. Big Champagne can be found at http://www.bigchampagne.com.

they share, the more they'll pay through whatever levy system is put together. And in exchange then, the more the demand grows, the more the artists and the owners actually make.

MS. GRANICK: What do you think about that, Joe?

MR. KRAUS: I completely agree with Fred, and I think that one thing that is driving this entire push in the content business is a misunderstanding that a major consumer shift is occurring. And that is the shift, at least in the American consumer, from what I'll call an analog consumer to a digital consumer. Where the analog consumer generally is a passive recipient of content, they watch, they listen. You don't use those words with the digital consumer. Digital consumers tend to create. They tend to compose. In the analog world you listen to an album in the order in which it was sent to you. In the digital world you rip, mix, and burn, and you alter the compilation in the process. In the analog world, you watch TV at an appointed time. In the digital world, you Tivo it, you time shift it, you edit out inappropriate content for your family. And, more fundamentally, is a shift from centralized, high cost creativity. So, high cost of production, highly centralized production to decentralized creativity, decentralized production and much lower cost of production.

And what I think you see is, because that isn't well understood, the legislative proposals you see in Washington, which are under the rubrick of preventing piracy—such as things like the broadcast flag which are essentially supposed to be anti-piracy—actually when you look under the hood, are really about control. They're about preventing this shift from the analog consumer to the digital consumer by controlling content beyond the point of sale. And I'll give you an example, just a fun anecdote that I had with Jack Valenti who I ended up interacting with on this issue in Washington. I said Jack, you know, I have a friend who took a video of their child playing flag football and then took a great application like iMovie and they edited it down, and then what they did is they took, when their child scored a touchdown, they took ten seconds of a movie they owned—the movie Rudy—and they clipped into the home movie. So, the kid scores a touchdown, the crowd cheers from the movie Rudy, and when the other team scores, the crowd boos, again from Rudy. I said, "Is that legal?" He said, "Absolutely not." I said, "Well, wait a second. He didn't show it to anybody. It's not on a file-trading network". He said, "It's still not legal. He circumvented copy protection on the DVD." I said, "He owned the DVD." "It doesn't matter." I said, "Well what should he have done?" And he says "Well, he should have called up Disney and cleared the rights."

(LAUGHTER)

MR. KRAUS: And I said, "You're serious?" And he said, "Absolutely." So, to me that's a good example of how the content industry generally isn't understanding that there's this major consumer shift going on, and I think that's driving a lot of the decisions. Whether it's decisions to make legislative proposals which would mandate digital rights management in all devices. Whether it's the pursuit of litigation against individuals or larger ISPs. It's really more about the ends and control and a movement trying to stop that shift.

MS. GRANICK: While you guys are talking about the brave future, I'm worried about my bottom line right now. And I would like to know whether the ISP or the University in my hypothetical at Stanford, are they my friend or my enemy? Are they somebody I should be thinking about suing, Kent, or are they somebody that can help me track this guy down?

MR. ROWALD: That's a good question. And you don't know at this point whether they are your friend or your foe. Now, I think you might want to start with the university. I think it's a good business decision to start with the university. You can go to them and say, hey guys, we got this problem. Shut it down. Most universities, I suspect Stanford for example here, will shut it down for you. They're your friend. You don't have to file that lawsuit. You give them notice and it goes away. Because most large entities want to do what's right, and they don't want to risk that liability. I think that's where you get back to that BMI model. They want to make sure that the liability is high enough so that people are going to comply voluntarily when you give them the notice.

MS. GRANICK: Is there a difference in liability between the public and the private university?

MR. ROWALD: There can be, yes. If you've got the public university, you've got state's immunity from copyright infringements. That's what that *Chavez v. Arte Publico Press*[20] case was all about, along with the *College Savings Bank*[21] on the trademark side.

MS. GRANICK: So they might tell me to fly a kite.

MR. ROWALD: The public university in all likelihood is not going to tell you to fly a kite, because they don't want the bad publicity that's going to come out of it when they do tell you that.

MS. GRANICK: Mark, how can a university—let's say, I find out that it's not a Stanford student here in Stanford, California but it's somebody who's using the Stanford network, maybe a student affiliate of

20. 157 F.3d 282.

21. College Sav. Bank v. Florida Prepaid Postsecondary Educ. Expense Bd., 527 U.S. 666 (1999).

Stanford, but somebody who's in another country, let's say Korea. How do you find out who that is?

MR. ISHIKAWA: Again, we go back to look at the DMCA. If you think about the Verizon case, you needed to identify—the DMCA really gave the copyright holder the ability to identify an individual who is sharing or violating their Copyright Act. If you think about the old days when you had the Internet, and you could register a domain, there was no way to find that individual. If you set up a hotmail account, you never could actually go serve that person with a lawsuit or whatever legal preceding you wanted to do. The DMCA made the ISP liable because that was the only person that you could actually find in the food chain that was—that had a presence. You knew where they were. They weren't going to be this anonymous person on the Internet. So what we'll do is we'll go back to the ISP or the person who's responsible for the address space and serve—get the notice sent to them for identification. Because we have no way to identify any end user on AOL, because they're dialing up from their home in Kansas into the AOL network. So for us we go to AOL and say okay who is this person who is doing this, and then we're able to find them.

MS. GRANICK: So Fred if it—

MR. VON LOHMANN: Let me clarify a little bit about the DMCA. Since DMCA, the relevant section of the copyright act, Section 512,[22] was put into place by the DMCA, that is a safe harbor provision for ISPs. Far from making ISPs liable, it actually makes ISPs not liable for infringing activity on the part of their users so long as they comply with certain requirements. The subpoena provision as contained in Section 512(h),[23] it is one of the conditions of that safe harbor. The precise scope of the subpoena power under Section 512(h) is currently being litigated in district court in D.C. and presumably will soon be on its way to an appeal before the D.C. Circuit. A very interesting area of law, again. We think there are interesting constitutional questions involved in that.

MS. GRANICK: Well, let me ask you what those are. If the DMCA puts the responsibility for dealing with the problem on the ISP once they

22. Digital Millenium Copyright Act, 17 U.S.C.S. § 512(c) (1998).

23. *Id.* § 512(h). Section 512(h)(1) allows the issuance of a subpoena to identify an infringer by providing: A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection. *Id.* Section 512(h)(5) provides: Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

get a DMCA notice, what's the problem with that?

MR. VON LOHMANN: Let me clarify further. The DMCA, Section 512, is a complicated statute. But it's important to note, when we're talking about peer-to-peer file sharing, there is no notice and takedown provision in the act that applies to this activity. The appropriate provision of Section 512 that applies to peer-to-peer file sharing is Section 512(a),[24] which is the section that applies to ISPs merely passing bits on behalf of their users. It's the same whether you're a university or Verizon, the same provision applies, it's Section 512(a). There is no notice and takedown provision associated with Section 512(a). That is a provision that applies to Sections 512(c) and (d), which applies to web hosts and search engines.[25]

So, focusing on Section 512(a), the requirements are just two. First, the subpoena issue, once again, being litigated. The constitutional question again is whether or not pre-complaint subpoenas, without any due process recourse, violates the right to anonymity that has been established in defamation cases in other areas. The other requirement of Section 512(a), which I expect to go to litigation at some point this year, is Section 512(i). Section 512(i) requires you to establish and reasonably implement a policy of terminating repeat infringers who are using your network.[26] Now what a

24. *Id.* § 512(a). Section 512(a) of the DMCA limits the liability of ISPs for material that is communicated online, which provides: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if— (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content."

25. *Id.* §512(c)-(d). Section 512(c) provides that "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." Section 512(d) provides, in pertinent part: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link."

26. *Id.* § 512(i)(1)(A). Section 512(i)(1)(A) provides: "The limitations on liability

repeat infringer is, is quite an uncertain thing. The Act says repeat infringer. It does not say you must terminate upon receipt of repeated allegations of infringement. Congress knew how to say that and in fact said exactly that in Section 512(h) in the subpoena area. They explicitly said an allegation is enough to trigger. Section 512(i) doesn't include that language. Nevertheless, tens of thousands of termination notices are being delivered, predominantly by motion picture studios to ISPs today, presumably universities are now receiving them as well. So I fully expect since the bottom line of ISPs is very much at issue when a termination requests arrives—it basically says, this user, almost always a broadband user when peer-to-peer is involved, must be terminated. You may no longer accept their check for fifty dollars a month. I fully expect that issue will end up in litigation soon. ISPs are very concerned about it.

Returning to your original question, are universities your friend or foe? I'll start by saying they're your friend in the sense that the first thing you should do is book an artists showcase at the coffeehouse once you discover that 20,000 people want to listen your artists' work here at Stanford. Whether or not they're your friend or foe as ISPs I think is an issue that is still very much in flux. I think to this point a lot of universities have thought it's better to cooperate with copyright owners. The University of Wyoming in fact has now installed a system whereby they monitor and copy all Internet traffic. Everything, emails, web traffic, you name it. All of it is copied and monitored and cross-checked against a database that checks for supposedly infringing file transfers. I would suggest that if universities are going to be that much your friend, it's time for the university communities to rise up and say—excuse me, you work for us.

MS. GRANICK: Peter, what do you think about that? About universities and workplaces monitoring their traffic for these types of purposes?

MR. HARTER: One thing that came to mind, sex, drugs, rock and roll.

(LAUGHTER)

MS. GRANICK: Because of this conversation?

(LAUGHTER)

MR. HARTER: No. it's late in the afternoon and I want to get the audience to laugh. I was also a rhetoric major undergrad so you got logos,

---

established by this section shall apply to a service provider only if the service provider has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

pathos, ethos, you got to know how to work the audience, have them work with you. Anyway, that's a diversion we can talk about in the courtyard. Sex, drugs, rock and roll.

In Pennsylvania, where I was educated both undergrad and law school in the late 1980s, my private school, Leehigh University, had a very strong Greek fraternity system, and there were a lot of incidences stemming from that. And the Board of Trustees and the management of the university looked the other way because they did not want to offend tradition. And I can tell you when the state law changed because of liability and made members of the Board of Trustees and the management team, the employees, the university, the president, the provost, and all those people with funny titles, personally liable for damages that students would incur upon themselves and their peers after being inebriated on campus, that the policies changed. And so that kind of activity went underground. Students still broke rules. Fraternities lost their charters. Lawsuits still occurred, but the liability shifted and you saw a change. The segue way to music is abusive alcohol or drugs in terms of civil society to be equated with the abuse of intellectual property, I don't know.

I think it's an interesting question to ask in a university setting because sex, drugs and rock and roll kind of go together, at least in a philosophical sense, for some people. So I would—to answer your question about your music and film company, if you have any connections to anyone on the Board of Trustees at Stanford and the management team, ask them how they feel if they are personally liable. Ask the university CFO how they would feel if their insurance companies, say hypothetically it's a big one like AIG,[27] if Maurice Greenberg at AIG decided to shore up his bottom line. The insurance industry is still reeling after September 11th. If they were simply to say that if you have knowledge of any illicit activity on your networks, and information assets are increasingly as viable to any enterprise, be it a university, or a company or a government agency as your physical assets and your financial assets in this era of renewed corporate governance and knowing what your money's doing in your company. And, Stanford being a company as much as a university, in theory, their biggest exposure is not someone getting drunk on campus any longer. In theory, maybe their biggest exposures are intellectual property activities going on in the networks.

So maybe, rather than going after law enforcement or litigation, behind the scenes lobbying of the insurance industry to tweak their clauses so it becomes very expensive to maintain insurance, and personally

27. AIG can be found at http://www.aig.com.

expensive to take a blind eye to this kind of activity. But then again, is stealing music, films, books other kinds of intellectual property equated with the social harm of excessive or abusive conduct with regard to sex and drugs? I don't know.

MR. ROWALD: You just mentioned one other defendant that we hadn't talked about before and that is all the people that are behind—the individuals themselves standing behind these networks. Because when we look at the copyright statute, it's very unusual. You can pierce any of those corporate veils very easily under the copyright statute. Because all you have to do is show they had a right and ability to control the infringing activity and a financial interest. And if you're looking at the Board of Governors or Board of Directors, whatever you've got here at Stanford, they have the right and ability to control what's going on over their own internet sites and over their own internet connections and their own computer system, absolutely, they do. Do they have a financial interest in what's going on there? If it's a student, they sure do. They're getting paid money by the student. And that's enough to breach that veil and go after each of those individuals that are standing behind them. And that's a large part of why your universities are going to try to work with you here. Primarily because you've got not only the university assets at risk, you've got all those individuals behind them at risk. That's why people like Carl, who is running his own little ISP there, have to be pretty worried about it. Does he have a financial interest and a right and ability to control that little ISP and what's going on over it? Sure he does.

MR. VON LOHMANN: Let me just note again, if Section 512 applies none of those claims will have any purchase, which is again why I think the Section 512 DMCA harbor, especially Section 512(a), is going to go to litigation this year. Because threats like that, I submit, the right answer is the ISP industry needs to stand up together and say, if you talk like that, let's see you in court. Let's test the theories and then we'll know. We'll know what the limits to our obligations are and then we'll be able to have a clear discussion. You know, and I also think frankly that the technology is going to keep moving regardless. I personally think if universities are going to start monitoring all traffic, whether in response to a fear of liability or any other reason, the right answer is for university students to set up their own networks. I can buy wireless access points today for less than one hundred dollars. I can mesh network them together. I can get single, high bandwidth activity from an off campus ISP provider. The way I see it, every single wireless node in the network could be eligible for Section 512(a) DMCA safe harbor. I can build a pretty copyright resistant network, completely without the university's resources.

And if that's what it takes to protect our ability to have private conversations without having everything be monitored, then okay, maybe that's what needs to happen.

MS. GRANICK: Peter.

MR. HARTER: I don't know if this is the answer to this question. But just for amusement, when you go into the labyrinth of how the DMCA came into being, you can point your stubby finger at one person, Manis Cooney, who was Chief of Staff to the U.S. Senate Judiciary Committee and also Chief of Staff to Senator Orrin Hatch[28] who has been chairman of that committee, and that Judiciary Committee has not devolved intellectual property to the subcommittee. They have always, for years, had a great tradition in the Senate of looking at copyright issues at the full committee level. And he works pretty closely with Senator Leahy,[29] the Democrat, so when the change of control occurs, it's either Orrin or Patrick or Patrick or Orin. Manis was there a long time and then got the Internet bug and went to be head of Business Development Public Policy at Napster.[30] And it was very interesting when Stanford colleague, John Place, former general counsel of Yahoo and former lawyer at Adobe, on the board of EFF—John, I don't think he's here today. He told me about his frustration with lobbying Manis Cooney when he was still in the Judiciary Committee on the DMCA, and Yahoo was a little too late. Manis said although their interests have come and gone through this office, the Internet industry is late, and too small. Despite how visibly important Yahoo and other Internet companies are, this is the circa '97, '98, and I was working for Netscape at the time. I had lobbied on the DMCA since '95 with some limited successes and some provisions. But the battle had been lost. The MPAA, RIAA, the publishers are much more powerful in Washington, influential with these little letters that Fred keeps mentioning which are very important. So my question to you, Fred, did Manis know at the time that he would be going to work for a Section 512(a) company: Napster?

MR. VON LOHMANN: Well, since Judge Patel ruled very early in the case that Napster could not shelter under Section 512(a), if that was his guess, he was woefully mistaken. Manis, by the way, is now freelancing if any of you need Washington representation.

MR. KRAUS: Actually, Peter's comments bring up something interesting, at least for me, which is examining why Silicone Valley has a huge amount at stake in this debate. Particularly in that trend that I was

28. U.S. Senator Orrin Hatch (R) of Utah.

29. U.S. Senator Patrick Leahy (D) of Vermont.

30. Manis Cooney was Vice President of Corporate and Public Policy for Napster.

mentioning before of enabling this new kind of digital consumer. That digital consumer relies on a huge number of technological products, new video cards, sound cards, bigger hard drives, new PC hardware, new software packages, etc., so Silicone Valley clearly has a huge interest in making sure that that digital consumer future exists. But it's really interesting to hear Peter's story and ask ourselves why does Silicone Valley generally suck in Washington.

(LAUGHTER)

MR. KRAUS: And I think the answer is actually kind of interesting as I try to think a little bit about it. I think it really gets at its heart. Silicone Valley is an engineering driven culture. It employs fact based decision making. As any of us who interact with lots of engineers know, when you're having a discussion, if you don't agree with that engineer's conclusions, usually their response is, "you haven't understood my facts well enough." And that doesn't work in Washington. This is not a fact based decision-making environment. I've never been successful arguing with a senator or a congressman when they disagree with me to say wait, let's start over from the beginning because clearly my presentation of fact has not been swaying enough for you.

The second is an engineering driven culture tends to believe that technology outpaces all policy decisions. And historically, that may have been the case, but I think in this particular instance, policy is having a dramatic effect on the development of technology. Several people that I work with in the venture capital community will tell you that they no longer want to make investments in anything in the digital media space at all. And, increasingly, that's broadening to a wider variety of new technologies or technological categories because of the liability associated with even playing in the space. And I think that's a threat to Silicone Valley, generally. I think pace is another issue. And I think, generally, Silicone Valley acts in Washington like a teenager. It says, leave me alone most of the time, and then it says I'll come to you when I need you, and you should treat me specially. So Silicone Valley tends to not have a constant presence, whereas Hollywood tends to have a very consistent presence, and it comes in way late, as Peter was just describing. It comes in late and it tries to spend a lot of money to get itself out of problems, but in reality it doesn't work very well.

MS. GRANICK: So, I want to move on a little bit and talk about—back to my Stanford student who's in Korea. Let's say that I want to explore my options for pursing this person legally. How do I do that? Do I have any kind of legal recourse against somebody who is in another country or even against a company or an ISP that's located in another

country?

MR. ROWALD: I think you really do. As a prctical matter, obviously, if you can get him here in the U.S., you're better off doing that. But if you don't know where they are or if they're in a foreign country, I think you can still go after these folks if you chose to sue them.

The first thing that I would suggest to you when you want to go after these folks, though, is to avoid any copyright claims in your complaint. Your copyright claims tie you down to Section 1400 of 28 USC, when you start talking about venue. And there you've got to find them and they've got to find them in the U.S. and you've got to find them where you want to sue them. I think you're better off avoiding those copyright claims initially and go after them for unfair competition, making a claim that, because they're making these files available for download, you're losing that musical sale, and that's unfairly competing with you for musical sales. When you make it , when you cast your complaints in those kinds of terms, unfair competition, tortious interference with prospective business relationships, perhaps, trademarks, if they're posting the song titles out there and you've got some trademark rights in those song titles. I think you can cast in those contexts and then you get into 28 USC 1391,[31] where you say the corporation is subject to personal jurisdiction anywhere where you can find the websites. For example, you get into the *Agar v. Multi-Fluid*[32] active-passive websites. *Zippo*[33] came out of the *Agar* case. It was part of the progeny there. You heard about the Kazaa personal jurisdiction battle here a couple of weeks ago.[34] You get into all those types of jurisdictional issues when you avoid the copyright cases. And I think you can get jurisdiction here as long as you avoid those copyright allegations. You then come back and add those copyright allegations back in later under the ancillary jurisdiction of the court. I think you can get around it that way. But that's the first thing I would suggest you do. You avoid those copyright claims initially.

MS. GRANICK: Peter, do you want to respond to that?

MR. HARTER: Could you put a lien on the tuition?

---

31. 28 U.S.C. § 1391 (2000).

32. Agar Corp., v. Multi-Fluid Inc., 1997 U.S. Dist. LEXIS 17121 (S.D. Tex. 1997).

33. Zippo Mfg. Co. v. Zippo Dot Com, 952 F. Supp. 1119 (W.D. Pa. 1997).

34. *See generally* Jon Healey, *From Vanuatu to L.A.: A Court Test for Kazaa*, L.A. TIMES, Nov. 26, 2002, at B1, available at (describing the dispute in the District Court in Los Angeles as to whether Sharman Neworks had established enough of a presence to be held for trial, during which Judge Stephen Wilson called "compelling" the minimum contacts which included over two million Kazaa subscribers in California and over twenty contracts with U.S. advertising agencies, law firms, and other companies).

MR. ROWALD: I'm sorry?

MR. HARTER: Could you put a lean on the tuition? If he's paid cash or has a scholarship, could you force him not to attend class or make him forfeit that right? There's economics involved.

MR. ROWALD: Once he's paid the tuition, it's not his money anymore, it's Stanford's. At least arguably it is. It may depend on where it is, certainly.

MS. GRANICK: What kind of financial compensation could I get? I mean, the person is in another country.

MR. ROWALD: Well, if you've got the copyrights registered, then you can go after statutory damages. Instead of having to prove actual damages, you say, I've got my copyrights registered, I want the minimum seven hundred and fifty dollars per file that he downloaded.

MS. GRANICK: But what I really want, I just want this stuff off the Internet.

MR. ROWALD: Well, you get the injunction on top of that.

MS. GRANICK: How are they going to enforce an injunction against somebody who lives elsewhere?

MR. ROWALD: Well, that's when you have to start going after the people that are making it available here in the U.S. If you've got some contacts here in the U.S., where you really have the most bang for your buck, I think, when you've got this sort of a thing, is you find out what domain name everybody's going to get these things. You sue the people that own the domain name. And even if you've only got a seven hundred and fifty dollar judgment, you go foreclose on that domain name and transfer it to your music site.

MR. VON LOHMANN: There's one additional piece of law you might use. Section 512, in its imminent and unlimited complexity, also granted to copyright owners, with respect to overseas works, the ability to demand that ISPs block IP addresses from overseas, if those IP addresses are being used to distribute infringing works. So, to my knowledge, I don't know how often it's been used, but there's only been one complaint filed and it was filed by, I believe, the RIAA or MPAA, one or the other, and it was filed against all the major backbone providers in the United States. Now if you could actually get that Korean IP number blocked by the five major backbone providers in the United States, you will pretty much have blocked that IP address out for everyone in the United States, probably also a lot of people in Canada and Mexico. But over-breadth is not something Section 512 worried about. So that's one possibility. It's one that I think only the largest content owners have played with thus far. But it's a tool in the box.

MS. GRANICK: So let's try to wrap up a little bit here. Mark, let me ask you, what future technological innovations can we look forward to seeing with regards to figuring out who infringers are and stopping them?

MR. ISHIKAWA: Well, for us it's really the game of cat and mouse. As the infringers come up with new technology, you know, we're staying right behind them. We find what we consider critical mass and then we develop the technology to go continue tracking and tracing. One thing I did want to add is, you know, not speaking on behalf of our copyright holders, our company is really there as the enforcer. I believe that they would much rather find a viable economic model where they can distribute on the Internet and use us for those that are fragrantly violating the copyrights.

MS. GRANICK: Joe, what are we going to see as far as future legal initiatives in this field?

MR. KRAUS: On the docket politically this year is certainly broadcast flag legislation. So, there's going to be, at least in the House Energy Commerce Committee, chairman Billy Tauzin will be introducing a piece of digital television legislation and a piece of that will actually mandate something called the Broadcast Flag,[35] which, if the draft of the legislation that was circulated last year is any indication, will require that all devices capable of demodulating digital television signals from an over-the-air transmission will have to respect and obey something called the broadcast flag, which a copyright holder can insert, and controls the behavior of your downstream devices like your Tivo. Can it record? Can it record once? How long can that recording last, etcetera? I think you'll also probably see something in what's being called the analog hole space which is essentially regulating the analog ports on a lot of your digital devices and potentially mandating watermarking technology for that. I think those are both some scary initiatives from my perspective, but certainly things that I think you'll see moving in Congress this year.

MS. GRANICK: Okay. So last question from me, and we're going to do this kind of McLaughlin group style, where you have to answer in three words or less.

MR. KRAUS: I don't know. How's that one?

(LAUGHTER)

MS. GRANICK: That was a good one. Okay. What is the right way

35. Letter from W.J. "Billy" Tauzin, Chairman, House Committee on Energy and Commerce and John D. Dingell, Ranking Member, House Committee on Energy and Commerce, to the Honorable Michael K. Powell, Chairman, Federal Communications Commission (Jul. 19, 2002), *available at* http://energycommerce.house.gov/107/letters/07192002_684print.htm. A draft of the bill mandating the broadcast flag can be viewed at http://bpdg.blogs.eff.org/archives/tauzin-bf-mandate.pdf.

to deal with the problem of widespread copyright infringement? I'll start with you, Kent.

MR. ROWLAND: Attack the worst offenders.

MS. GRANICK: Close.

MR. VON LOHMANN: Compulsory license.

MR. HARTER: Damn the torpedoes.

MR. KRAUS: I'll also say compulsory license.

MR. ISHIKAWA: I believe its education—educating the users.

MS. GRANICK: Okay, on to questions. You're first.

AUDIENCE: I'm an independent marketing optimization consultant, and I understand you're a small music label.

MS. GRANICK: Yes, I am.

AUDIENCE: So you've got a band that has their music getting distributed on this network. You actually have a distributor in Korea already? I mean, that's pretty awesome. So you're competing with these large labels, right? You want your band to get out there. You want to make as much money as you can for them because that's going to make you more money, right?

MS. GRANICK: Yeah, but the distributor in Korea is not giving me any money.

AUDIENCE: Right. Exactly. Not yet. So why not find a way, rather than seeing him as a foe, to make him a friend, by making him a distributor instead of a pirate and take advantage of this trend. It's something you can do as a small label to take advantage of this climate and get a leg up on these larger companies, that, you know, it's like moving a battleship, right? You can be a lot quicker. So you can take advantage—things like Spiderman, the largest grossing movie ever. Something like a million downloads of that movie the week before it came out. So again, going back to some of these actual facts. Let's look at some of these things and the opportunities that are there for you in the market. Take some of these thieves and maybe make honest thieves out of them. I don't know if you're aware of a new company in the Netherlands called TheHonestThief.com.[36] They can enable you to share the files and yet collect money and distribute it back to you and to your artists. And that way you can take this thing and through electronic bill presentment and payment turn this to your advantage.

MS. GRANICK: Peter, is this a viable business model for me to take this distributed network technology and turn it into something where I'm

36. TheHonestThief.com can be found at http://thehonestthief.com.

going to get paid?

MR. HARTER: Well, without speaking out of school, yes. Some people have "Napsteritis" where they refuse to spend any money on digital media even though they blew tens of millions of dollars personally and through their Angel funds and VC funds on Napster and that group of start-ups. Others from that tribe—I've got money, I've got time, and I've got interest. I want to invest in media companies. And happily, I've been advising a company that's not a file-sharing company. It's a search engine in San Francisco. They've been boot strapped for two and a half years. And, cross my fingers, I think they'll get some Angel funding and they'll be able to hire a few more engineers, and help grow consumption—legal consumption—in the online music space.

Because one thing that we saw from file sharing and continue to see to some degree, people want to find other music they like. That's why you make compilation cassette tapes for your friends. That's why you burn CDs for your friends. That's why you send files, or point out files, or share files over peer-to-peer software. I think the record industry and—it's a shame we only focus on the record industry, because we have to look at books, games, and film and convergents of those media—but looking at music, we are all trapped as consumers. This is a personal comment. We're trapped spending eighteen bucks on a CD, buying twelve to fifteen songs when we only want one or two songs. And the price point, I think, is wrong. I've seen Clive Davis of Jay Records—a former BMG executive—argue that it's a bargain to pay eighteen bucks for a CD. I think the Federal Trade Commission and its five-year price fixing investigation at directed labels will disagree with that to some extent. Yes, you can listen to songs over and over again, and so over time the cost actually may be a bargain, but it's not a bargain to waste money and bit space on songs that are crap. And I think you can listen to Billy Joel's song from Turnstiles, going back a long time, they maybe cut it down to three minutes, five seconds. The vinyl 45 only could contain so much data. And as we go from one file format to another file format, we're now in what Professor Goldstein, in his book from many years ago—if you haven't read it, I suggest you read it—the Celestial Jukebox.[37] Where you're only limited by bandwidth and disk space and that's getting cheaper and bigger "every breath we take"—the Police. So it just seems to me that there's so much opportunity here in the market that if you can go track by track and not be forced into buying a packaged collection of music—which you may not like or want to spend

37. PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX (1995).

the money or time on—and as long as there's so much time on this planet, we could have a celestial jukebox to search and find the songs we like and find songs like it from other cultures. They'd be much more enriching and digital artists could really be in the business of distributing music to their fans and the labels [can] get back to the business of being in A&R. How many people in this room know what those initials mean, A&R? Artists and Repertoire. I think the business models of the major record labels are doomed as we see them presently constructed today. And I think EMI, with its new CEO, that's the company to watch. They're a pure music company getting back into A&R. You see they did a big deal for a hundred million with Robby Williams—the male version of Brittany Spears in the U.K. I guess you call him—where they're taking a chunk of his revenue from concerts and marketing and he's getting an advance on that. David Bowie was mentioned before by Carl. I think it was him that had that quote but he did that junk bond debt offering where he sold the future royalty rights. Artists are getting very clever about how they're making money. And I think we have to see this and get away from making profits to support their huge overhead costs of their fancy pants management people and to get to the start up [a] more lean and mean way of thinking and running a business [as] we're used to doing here in Silicone Valley, that you can make a lot of profit from a artist who sells only 1,000 or 10,000 songs. You need not have ten million albums. This whole platinum thing, I think, it's really a sickness that has perverted the ability to make money in the music business. And this obsession about litigation and piracy—it's legitimate to go beat up really bad actors and pirates. And there are, but you should not also go and attack your consumers because they want to spend money on music. And fundamentally, is this country going to spend more than $150 a year on buying music? There's only so much a consumer will spend. You can look at all the marketing data. People buy ten to fifteen CDs a year, and they spend "X" amount of money cash, out of their income, a year on music. But strangely enough, games and DVDs are taking more of that finite consumer dollar and time. Music is at risk of losing out to other things that will compete for time and money. I think there's a crisis in the music industry. So, invest in a start-up.

MS. GRANICK: Other questions?

AUDIENCE: (INAUDIBLE)

MR. VON LOHMANN: I think the main event in these issues is not legislation. I think you're right. I think we would all be much better off if we took a more modest approach toward having law take command of this space, especially when, to take the motion picture industry for one, that industry appears to be having remarkable success and in no immediate

danger. And even the recording business, I think tales of its demise are somewhat exaggerated. People will still be buying CDs for some years to come. Certainly my parents, they're not in a Kazaa universe there. Getting Dad to turn the computer on reliably is still —

MR. KRAUS: You haven't set that up for him yet?

(LAUGHTER)

MR. VON LOHMANN: I'm a few hundred miles away and if I'm not there, well. So I think things are not yet settled and the technology is moving quickly. But the danger here—and I want to echo Joe's point—the danger here is not legislation, although that is dangerous and much of what is being considered is both premature and unwise. The major danger that I think most people are overlooking is the onslaught in litigation and the effort to change the balance of secondary copyright liability in the United States. That's really threatening innovation today on the ground in an immediate fashion. If you want to see a remarkable extension of secondary liability principles, take a look at the complaint filed by the music publishers against Bertelsmann. The theory being that because Bertelsmann invested fifty million dollars, and I'll note it was not an equity investment but a debt transaction, that that investment should make Bertelsmann liable for every infringement committed by a Napster user during the year and a half or so that Napster existed as a result of that investment. That's a terrifying precedent to set for investors in digital media technologies. If I loan money to a company whose technology may be used by third parties who I never meet to commit copyright infringement, all those liabilities may land on my head. Well, I submit that that's a very terrifying legal precedent. The precedents that are being pressed also in the cases themselves, cases like the Morpheus and Kazaa case,[38] the *Aimster* case,[39] and others represent a real incursion of copyright law into the area of building tools, of building innovative technology. So that I think is a danger today already, and I think too few people are paying attention to it.

MR. KRAUS: Let me add on just another scenario. Silicone Valley generally plays defensive politics. They don't play offensive politics very well, so it's much easier in Washington to stop something than it is to get something passed. So let me make the assumption that for the next couple of years, Silicone Valley actually stops some of the more egregious legislation that's out there. But I can certainly envision the following scenario. In two years, one of the big six record labels goes under. Okay. That happens. That is a cataclysmic event in Washington where all of the

38. *See* Jon Healey, *File-Sharing Firms Feud Over Users*, L.A. TIMES, Mar. 2, 2002, at B1.

39. In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

defense that Silicone Valley has been playing to stop things like the Hollings bill[40] or the Berman bill[41] or some other things that would be very detrimental – it doesn't matter anymore. Whether or not that record label went out of business because of peer–to–peer file sharing, I guarantee you it will be the political motivation to get some really bad legislation passed. So while I would like this to be a go slow event, or a go slow scenario, I can certainly envision the motivation of going fast being provided by just one of these labels going under and then all of the work that Silicone Valley has done on defense won't matter for naught.

MR. VON LOHMANN: Go out and buy CDs, you hear? Prop those companies up, for God Sakes.

MS. GRANICK: And now our last question.

AUDIENCE: We've talked a lot about consumers, as just consumers per se of digital media. We talked about consumers as creators. We talked about a market failure. It seems to me that there's also a sort of political process failure. And I guess I'm less cynical about legislation per se, but I wonder if any of you can speak to the issue of consumers as citizens, and whether they will—whether there will eventually be a point where they will organize around this issue. And if consumers fail to organize this issue, if maybe they are not—I'm saying this a little bit sarcastically—but maybe not entitled to what they get if they are not willing to be more proactive in looking out for their interests however they may ultimately define them.

MR. KRAUS: Well, DigitalConsumer started about a year ago. And I was unbelievably surprised that within six months about 50,000 people had signed up and basically said, hey, we want to be kept informed. We want to contact our members of Congress. So I would say that I've been pleasantly surprised actually at the level of citizen engagement on this issue. I think the challenge, it's really interesting in D.C., the challenge seems to be that consumer activism definitely puts an issue on the radar screen. And it doesn't have to be that many people. I mean, ten to fifteen people who fax their member of Congress does move the needle and takes an issue from nowhere to somewhere very high on at least the congressional radar screen. The challenge is, consumers are necessary but not sufficient as part of this equation. So they have to be in there, but generally speaking, unless there is an alignment, and I think there is a growing alignment between the technology business and consumer citizens because their interests tend to

40. *See* Consumer Broadband and Digital Television Promotion Act, *supra* note 15.

41. Teresa Wiltz, *Music Debate Heads to the Hill*, WASH. POST, Aug. 21, 2002, at A08; *see also* H.R. 5211, 107th Cong. (2002), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h5211ih.txt.pdf (July 25, 2002). The bill proposed by Howard Berman (D-CA) was also known as the Peer to Peer Privacy Prevention Act.

more aligned. Without that kind of corporate blessing, it gets very difficult to actually move a piece of legislation. So I am optimistic. I think the more Hollywood overreaches, whether it's restricting the rights of what consumers can do with media, the more I think you're going to activate consumers. And so far, Hollywood hasn't shown restraint in overreaching which I think means more and more people will be getting engaged in this debate.

MR. ROWALD: I think the other thing you're going to run into here, you're going to see companies that are starting up that embrace the technology. I've got a client that has formed his own little record company. He puts his, the first song on any given, what would be a CD out there on the net and says, "copy it and share it with all your friends and tell them where you got it." And if they like it, they can come and buy the other ones that are on that CD. And it's a buck a piece for the songs. And what he's finding is that people are willing to come in and listen to it and say, "okay I'll pay a buck for that." I'll pay two or three bucks and get the two or three songs on that selection that I want. And he's got almost no costs. He doesn't have to burn the CDs. He doesn't have to have any shipping. He doesn't have to have any advertising, at all. And I think you're going to see a lot more of those kinds of models with people embracing the technology and using that technology to get basically honest people to do what's right, and pay them for what they want. And I think that when you see that big record company that's going to go under, you're going to see a ton of legislation and you're going to see a proliferation of these other technologically savvy companies coming out there to try to fix that very problem.

MR. VON LOHMANN: Keep an eye on Natalie Merchant. Natalie Merchant just severed all of her connections with the mainstream record business, formed her own label and said she is issuing her next record from her own website. It will be very interesting to see what position she takes with respect to offering tracks in MP3 or other formats. I think there will be an increasing number of artists who say, you know, this industry isn't working for us, anyway. So, you know, it's time for us to experiment because, as Janice Ian points out, she records twenty-six albums, wins nine Grammy's and has never seen a check for a single penny of royalties from any record label.

MS. GRANICK: With that I want you to join me in thanking our panel.