S. HRG. 108–987

CONSUMER PRIVACY AND GOVERNMENT TECHNOLOGY MANDATES IN THE DIGITAL MEDIA MARKETPLACE

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 17, 2003

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

91–289 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina, *Ranking*
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN D. ROCKEFELLER IV, West Virginia
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	BYRON L. DORGAN, North Dakota
GORDON H. SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	BARBARA BOXER, California
JOHN ENSIGN, Nevada	BILL NELSON, Florida
GEORGE ALLEN, Virginia	MARIA CANTWELL, Washington
JOHN E. SUNUNU, New Hampshire	FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

CONTENTS

WITNESSES

APPENDIX

CONSUMER PRIVACY AND GOVERNMENT TECHNOLOGY MANDATES IN THE DIGITAL MEDIA MARKETPLACE

WEDNESDAY, SEPTEMBER 17, 2003

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m. in room SR–253, Russell Senate Office Building, Hon. Sam Brownback presiding.

OPENING STATEMENT OF HON. SAM BROWNBACK, U.S. SENATOR FROM KANSAS

Senator BROWNBACK. I call the hearing to order. Thank you all for joining us today. We have got an important hearing. I would like to begin this morning by thanking the Chairman, Chairman McCain, for permitting me to hold this important full Committee hearing.

Today's hearing focuses on two timely issues for consumers in the information age, new challenges to their privacy and an ongoing Federal Communications Commission proceeding that raises the specter of depriving them of their customary and legal uses of broadcast television content.

Our first panel will discuss the merits of the Digital Millennium Copyright Act information subpoena, included in section 512(h) of the Act. Recently, a Federal court has held that copyright owners may use a subpoena to compel Internet service providers to disclose to them the names, addresses, and phone numbers of their subscribers suspected of piracy. This occurs when an ISP service acts as a conduit or the transport over which the subscriber sends and receives data. This subpoena process includes no due process for the accused ISP subscribers, none.

This past July a hard-core pornographer, Titan Media, filed a subpoena against SBC Communications seeking the identifying information of 59 SBC Internet subscribers. Since that time, Titan has offered a most generous amnesty program: those ISP subscribers it suspects of piracy can go to their website and buy porn and in exchange Titan will not identify them. Gracious indeed.

I strongly support protections of intellectual property and I will stand on my record in support of property rights against any challenge. But I cannot in good conscience support any tool, such as the DMCA information subpoena, which can be used by pornographers

and potentially even more distasteful actors to collect the identifying information of Americans, especially our children.

Yesterday I introduced the Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, in part to eliminate the results of the RIAA case against Verizon to ensure the DMCA information subpoena cannot be used in this manner. The Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003 also addresses other issues vitally important for consumers in the digital environment. This legislation seeks to preserve consumer and educational community customary and legal use of content and to create minimal protections for them as digital rights management technologies are increasingly introduced into the marketplace.

Digital rights management, otherwise known simply as DRM, refers to the growing body of technology, software and hardware that controls access to and use of information, including the ability of individuals to distribute that information over the Internet.

Today's hearing seeks to answer the questions of whether government should mandate DRM solutions to combat piracy and whether such an action can be achieved without limiting the public's customary and legal uses of content.

I do want to note the 2 days ago AT&T Labs issued a report estimating that 77 percent of the pirated movie content available through peer-to-peer file-sharing software has been made available by movie industry employees, not unaffiliated consumers. This report raises strong questions about whether digital video piracy occurring today is primarily a governmental or intra-industry issue to be dealt with at this point.

Currently the Federal Communications Commission is considering how to implement Hollywood's proposal for the broadcast flag, a DRM proposal designed to protect digital television programming. This proposal would require that a flag be attached to DTV programming which would in turn inform consumer electronics devices that the DTV content cannot be redistributed over the Internet.

The flag as envisioned by Hollywood is clearly problematic. Today consumers in the educational community are empowered to use content in a host of ways, none of which require the permission of the copyright owner. By including a complete ban on Internet redistribution of DTV programming, Hollywood's broadcast flag proposal will artificially limit the way consumers may take advantage of the Internet to make these customary and legal uses.

In fairness to Hollywood, I am not aware of an existing DRM technology that both prohibits piracy yet also allows consumers to redistribute content over the Internet in legal ways.

To the degree that digital piracy of video content is a real issue, I have proposed a different way to address the protection of DTV content from piracy in the Consumers, Schools, and Libraries Digital Rights Management Awareness Act. Instead of mandating specific technologies and giving one set of stakeholders a veto over others, my bill would create a self-certifying self-certificate environment where hardware manufacturers may use whatever technologies they determine meet the requirements of the flag.

In addition, the flag itself imposes a rule that DTV content cannot be illegally redistributed to the public over the Internet, which is a more flexible anti-piracy policy than the one Hollywood proposes. In my bill it is the FCC that will resolve any disputes that arise in determining if a self-certified technology does not comply with this anti-piracy safeguard.

These are important issues for our Nation's transition to digital television, as the content community has threatened to withhold digital content unless the issue of digital piracy is addressed. I certainly look forward to hearing from our witnesses on these important issues and as this issue develops for us to be able to resolve this so that we can move forward on digital television and protect the privacy and rights of the individual along with the property rights of those developing this content.

With that, because of time constraints I would like to ask my colleagues if Senator Burns could go next. He has to go to chair a hearing, if that would be OK. Senator Burns.

STATEMENT OF HON. CONRAD BURNS,
U.S. SENATOR FROM MONTANA

Senator BURNS. Thank you very much. We have got Interior Appropriations going on on the floor this morning and I manage that bill and I thank the Chairman. I thank my colleagues for allowing me to do this.

Mr. Chairman, today's hearing addresses an issue of critical importance to our Nation's continuing technological development, the protection of intellectual property in the Internet era. The 1998 Digital Millennium Copyright Act, DMCA, represented the most comprehensive reform of copyright laws in a generation, updating the U.S. copyright law for the digital age. The act included clear provisions prohibiting the circumvention of technological safeguards on copyrighted digital material.

I have always been a strong proponent of laws protecting intellectual property rights. Such protection is fundamental to nurturing what is a consistently strong sector of our economy. At stake in this debate is not only the livelihood of artists and musicians, but that a significant number of citizens are involved in the commercialization and distribution of creative content.

Such protection has taken on a new meaning in the digital era, though. Today's technology can not only be directed at defeating protective mechanisms, but also in sharing pirated content in volumes and at rates that are resulting in massive levels of financial loss to owners of copyrighted material. While digital technology enables the production of high-quality audio and visual entertainment content, it also makes such content highly vulnerable to piracy and distribution over the Internet.

The move to a digital medium of dissemination is well under way and at mind there is little that can reverse this process. Lack of adequate safeguards for content will only prevent our citizens from enjoying the benefits of this digital entertainment revolution. Furthermore, inaction in this regard will put a brake on commercial activity that usually surrounds adoption of new technologies.

While I am confident that the marketplace will eventually evolve a technologically and financially balanced solution that is agreed

upon by a broad cross-section of stakeholders, I am concerned over the prolonged debate surrounding the issue. I see the role of government as one that encourages the principal stakeholders to arrive at an agreement expeditiously. This is a dynamic technology arena. Government technology mandates, even if a broadly acceptable set could be devised, would have to be flexible so as not to thwart or choke technological evolution.

I am heartened by last Wednesday's FCC decision with regard to the cable CE or plug-and-play agreement. This decision helps to establish the technical standards by which digital TV will receive and display digital television signals available on cable systems nationwide. While the issues surrounding the copyright protection in the digital area are difficult and complex, it is my hope that the parties involved can reach an agreement on a way to protect content that works technologically.

If that is not possible, Congress may indeed have to step in and take a more active role, a prospect that I do not look forward to, but which may be necessary as events evolve.

Mr. Chairman, thanks for holding this hearing today. I am sorry I am not going to get to participate as much as I would like. But nonetheless, it is important, and it is just spam days all over again. It is the industry must make the decisions and it will be through the industry stakeholders working on this that we will finally get some sort of settlement. I thank you for holding the hearing and I thank you for your courtesy in allowing me to go to the floor now.

Thank you.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Mr. Chairman, today's hearing addresses an issue of critical importance to our Nation's continuing technological development—the protection of intellectual property in the Internet era. The 1998 Digital Millennium Copyright Act (DMCA) represented the most comprehensive reform of copyright laws in a generation updating the U.S. copyright law for the digital age. The Act included clear provisions prohibiting the circumvention of technological safeguards on copyrighted digital material.

I have always been a strong proponent of laws protecting intellectual property rights. Such protection is fundamental to nurturing what is a consistently strong sector of our economy. At stake in this debate is not only the livelihood of artists and musicians but that of a significant number of citizens involved in the commercialization and distribution of creative content. Such protection has taken on new meaning in a digital era. Today, technology can not only be directed at defeating protective mechanisms but also in sharing pirated content in volumes and at rates that are resulting in massive levels of financial loss to owners of copyrighted material.

While digital technology enables the production of high quality audio and visual entertainment content, it also makes such content highly vulnerable to piracy and distribution over the Internet. The move to a digital medium of dissemination is well underway, and in mind, there is little that can reverse this process. Lack of adequate safeguards for content will only prevent our citizens from enjoying the benefits of this digital entertainment revolution. Furthermore, inaction in this regard will put a brake on commercial activity that usually surrounds adoption of new technology.

While I am confident that the marketplace will eventually evolve a technologically and financially balanced solution that is agreed upon by a broad cross-section of the stakeholders, I am concerned over the prolonged debate surrounding this issue. I see the role of government as one that encourages the principal stakeholders to arrive at an agreement expeditiously. This is a dynamic technology arena—government technology mandates, even if a broadly acceptable set could be devised, would have to be flexible so as not to thwart or choke technological innovation.

I am heartened by last Wednesday's FCC decision with regard to the Cable-CE "Plug and Play" agreement. This decision helps to establish the technical standards by which digital TVs will receive and display digital TV signals available on cable systems nationwide.

While the issues surrounding copyright protection in the digital era are difficult and complex, it is my hope that the parties involved can reach agreement on a way to protect content that works technologically. If that isn't possible, Congress may indeed have to step in to take a more active role, a prospect that I don't look forward to but may be necessary as events evolve. Thank you, Mr. Chairman.

Senator BROWNBACK. We will go in the order of attendance unless there are needs, that people have time needs here. So we will go next with Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Mr. Chairman, thank you, and I will just make a couple of brief comments.

The entertainment industry, which is of course big in my state as well as particularly the Senator seated next to me, her state, it accounts for nearly 5 percent of the Nation's economic output. So if damage is done to that marketplace, it is clearly bad for everybody, but it is especially tough on the creative artists who depend on the royalties to support their families.

I have a daughter who is a songwriter and a singer. Now, we are not to the point that she is supporting her family. It is exactly the reverse. But seeing this through her eyes clearly has been an education for me.

I think it is unfortunate that the recording industry has had to resort to the filing of individual lawsuits, but this is an industry that is facing a very serious and a growing threat. So it is going to be up to us to strike a careful balance between protecting the rights of copyright holders and the right of the Internet users to remain anonymous and to get them to obey the law. That is a delicate balance for us to find.

I do not want us to see people hiding behind the veil of privacy to conduct illegal actions. That is part of our law, is the law of privacy, but we do not want that to be an excuse for illegal actions. I believe the burden is on the ISPs to show that the customer information that they are required to share is sensitive enough to outweigh the copyright holder's interest in protecting their property, and if they can demonstrate that a valid privacy concern exists I am all for changing the law. If not, we need to move forward with all available speed to help curb the piracy before it deals a devastating blow to the entertainment industry.

With your permission, Mr. Chairman, I am going to go and introduce a judicial nominee in the Judiciary Committee and then I will come back.

Senator BROWNBACK. That would be just fine.

Senator NELSON. Thank you, Mr. Chairman.

Senator BROWNBACK. Thank you.

Senator Sununu.

STATEMENT OF HON. JOHN SUNUNU,
U.S. SENATOR FROM NEW HAMPSHIRE

Senator SUNUNU. Thank you, Mr. Chairman. I very much appreciate your having the hearing and, while I most certainly will not be here for the entire hearing, I want to note the large number of witnesses that we have scheduled and thank them for their time.

This is an important issue, as are many of the ones we deal with. It is a very difficult issue, difficult because it matches two very important issues, two very important concepts, one being property rights and intellectual property, which is just critical to our country. A friend of mine is fond of saying that intellectual property nourishes the American economy, and that is absolutely true. But intellectual property is an element of property rights and in this case we are dealing not just with the property rights, but also with privacy rights. So we have a very difficult balancing act to strike.

It is also an issue that is not going away. Senator Burns indicated the pace of evolution that we see, the process of digitization of so much of the content that we enjoy as consumers, and the content around which very important segments of our economy are based. That process of digitization, the reduction in the cost of transmitting content, is only going to continue.

So I have a sense that we are going to be dealing with and talking about this issue 2 years from now and 4 years from now and 10 years from now and 15 years from now. So it is important that we get all the information and the points of view on the table and that we act in a very, very deliberate way.

I have, as do many on this committee, significant concerns about government-mandated standards for technology and that extends far beyond just the issue of broadcast or the issue of entertainment or the issues of telecommunications. We need to be very careful about having the Federal Government try to forecast what kinds of innovations, breakthroughs, or new technologies are going to come to the forefront 4, 8, 10 years from now. So I think it is important that we approach this in a very steadfast way.

It is important, it is an importance that has been recognized by industry, that industry work as collaboratively as is possible to try to deal with some of these issues. Senator Burns mentioned the plug-and-play issue that is moving toward resolution, and I think we should give credit to the many industry players that have worked to already resolve some of the concerns that we will be talking about today. But we have a lot more work to do and I look forward to the testimony.

Thank you, Mr. Chairman.

Senator BROWNBACK. Senator Boxer.

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Senator, thank you very much.

This is a very important issue for the well-being, economic well-being, of my state. That means jobs, that means prosperity; and of course for the entire country.

Senator Brownback, I did not hear your opening statement. I did hear the others. I think there is a lot of wisdom in those statements that I would agree with.

There are four issues surrounding illegal file-sharing and these are the issues that I think there are. You may have more. First, we must clearly define downloading copyrighted work as theft, because that is what it is. You steal a bike, you steal a bike. You steal someone's work, it is copyrighted, it is stealing.

Second, we must recognize the economic harm that this theft causes, as well as of course—I know we will look at some of the victims of these lawsuits—there are victims of theft.

Three, we must recognize the threat the privacy inherent in open file-sharing networks, which is really interesting to me.

Fourth, we must recognize that these networks misleadingly expose children to pornography. That is an issue that I know, Mr. Chairman, you care about, as do I.

First the issue of theft. Using Internet peer-to-peer networks to acquire copyrighted work for free is theft and it violates copyright laws. There is such a thing as right and wrong in our society. There it is: it is theft. It undermines society's interest in compensating authors for their works and discourages creative production. If the message coming out of this hearing is anything other than the fact that stealing a copyrighted work is theft, then I think we are doing a great disservice.

It is perfectly legal to share non-copyrighted work, but it is not legal to share copyrighted work. There is a difference. File-sharing, for example, between scientists as they work to solve a problem, they share their files, that is one thing. Copyrighted work is something else. Unless you pay for it you cannot have it.

Again, I think this is really important and it is a lesson that we have to teach our children. It is part of family values.

Congress addressed this issue in 1998 in a carefully considered provision of the Digital Millennium Copyright Act. The provision granted copyright holders the right to access the names from Internet service providers of those that were stealing their work. In exchange—and this was a compromise—service providers were granted broad protection from liability for theft that was conducted over their networks.

I strongly believe that was the right thing to do. So the question is whether this committee will stand behind copyright laws or whether we will choose to change those laws and, perhaps inadvertently, doing that encourage theft, because the only way to enforce the copyright on the net is to find out who is doing the stealing. It is virtually impossible to find out those names—if it is, if it is made virtually impossible, then theft is encouraged. I am very willing to look at ways that we could work around that, very willing to. But that is the basic bottom line.

If you have a lineup if somebody has stolen a car and there are witnesses looking at the people, if they are all covered up in a white sheet, each one of them, you cannot find who did it. So if you want to find the person who committed the theft and you have got another way to do it, I am willing to listen.

But we have to emphasize that stealing copyrighted work is not a victimless crime. The music industry has lost 25 percent in sales over the last 3 years. It has gone from a worldwide $40 billion industry in 2000 down to a $26 billion industry in 2002. Fewer art-

ists are being signed and people who work in distributing and promoting these artists are losing jobs.

Jobs are being lost, folks, and we have lost in the last couple of years almost 3 million of them and we cannot afford to keep losing jobs. Our Nation's creative people—songwriters from Austin to Memphis, filmmakers from New York to Hollywood, software developers from northern California to New England, and authors everywhere—cannot afford to give away their art for free. It is the way they make a living. Now, maybe some people can work for free, and if they can it is wonderful. But in our society most people have to work.

My third point is that using file-sharing itself poses a threat to privacy. There are those who will argue today that the provision in our act that we are discussing is an assault on privacy because it can be used to unmask anonymous Internet users. But remember, these are the people who are stealing, so we have to find out who they are somehow.

But beyond that, I argue that use of peer-to-peer file-sharing for piracy actually places your privacy at risk. Most users have no idea that they are frequently sharing their private documents with everyone on the network. So let me show you, Mr. Chairman, a page from Kazaa where you agree in fact that you will share your files and that your files are in your shared folder, and it allows you to add any other folder you wish.

Users often do not know that a document or an automatic backup of the document is being saved in their shared folder and unwittingly they are making those files available to everyone on the network. A House report from the Committee on Government Reform found in a search of one peer-to-peer network at least 2,500 Microsoft Money backup files. Each of these files store a user's personal financial records and all are readily available for download.

That means if your son or daughter downloads music through Kazaa during the afternoon, the information you work on at night—private tax returns, medical records, financial portfolios, and private communications—may also accidentally become available to everyone else on the network. This is just something that is happening, that has been proven.

I am almost done, Mr. Chairman. The fourth and final issue we must address is how these networks expose children to pornography, and I am going to show you how that happens. According to the GAO, juvenile users of peer-to-peer networks are at significant risk of inadvertent exposure to pornography, including child pornography.

Again, let me show you this screen. The user has put in a search for "The Beatles." That search then generates a series of files available for download, and it lists them and here they are listed. Most of these files are copyrighted works and it is illegal to download them. But look at the file highlighted on the chart. It is titled "Drunk Teen Sex 2," which is a teen porn file. Plus there is no guarantee that any of these other files are actually not pornography. Your child could think she is downloading a Beatles song and actually be downloading pornography.

Ultimately, we have to look at what we did in our Copyright Act. I believe that if we change the law and we make it harder to en-

force the theft of copyright works, we will be inadvertently expanding the use of pornography to unsuspecting kids and we will not be enforcing a law that has made our country great, which is that the owner owns the property and if you want it you need to pay for it.

Thank you very much.

Senator BROWNBACK. Thank you, Senator Boxer.

We are joined by Senator Coleman, who heads a subcommittee in the Government Affairs that is looking at this topic, as well as has a number of personal interests, a great deal of personal interest in this topic. We welcome your attendance and your testimony, Senator Coleman.

STATEMENT OF HON. NORM COLEMAN,
U.S. SENATOR FROM MINNESOTA

Senator COLEMAN. Thank you, Mr. Chairman, and I do want to thank you for your leadership on this issue, for holding this hearing, and for giving me the opportunity to come before you.

On September 8 the recording industry, RIAA, fired its first volley of copyright infringement lawsuits. The industry had promised to, quote, "approach these suits in a fair and equitable manner," it is initially focusing on egregious offenders who are engaging in substantial amounts of illegal activity.

As Chairman of the Permanent Subcommittee on Investigations, I requested documents from the recording industry to assess the scope and nature of the procedures used to identify and sue consumers who engage in potentially illegal file-sharing. For the purpose of being equally gracious with the time you have shared with me, I just want to briefly outline the problems as I see them and where the PSI intends to go with our investigation.

I would note, technology and the Internet offer such great hope for a bright future, but with it clearly there are concerns about how it is used and who uses it and how do you deal with those who use it in an illegal manner.

On the matter of subpoenas, I am concerned about the scope and impact of the broad powers extended to the RIAA to issue subpoenas. To that extent, I believe we need to understand whether or not it is possible for innocent people to get caught up in the legal web that the RIAA is trying to create to stop illegal piracy.

I understand that there are 60 to 90 million people who use P2P networks to illegally trade copyrighted material. Many of these users are teenagers or younger. This generation of kids needs to be made aware that they are engaging in illegal behavior.

But I do not believe, however, that aggressively suing offenders will be sufficient to deter the conduct of an entire generation. We will review penalties, both civil and criminal, that may be future tools to ward off stealing of copyrighted materials.

As it relates to the use of technology in general, I am troubled by the growing use of systems and devices to reach into our online lives and pluck out information about us, with or without our knowledge. This is particularly relevant here since technology is being used not only to steal the works of artists, but to prove that someone has indeed stolen it.

In addition, part of our continuing inquiry will address why P2P networks do not proactively prevent this illegal activity from initially occurring and how P2P networks like Kazaa envision moving from a business model predicated upon illegally trading songs to a legitimate business model that derives revenues from licensed copyrighted intellectual property.

There is more at issue here than just subpoenas and the impact of the use of a power of subpoena and the threat of legal action to compel consumers to cease and desist. I believe the very future of the American music and motion picture industries is at stake here and with it a major contributor to our Nation's economic stability. I believe Senator Nelson noted that the movie industry alone contributes 5 percent to the Nation's economic output.

The growth of current and future technologies bode well for improving the quality of lives and productivity, but it could also spell economic doom for the entertainment industry. In a short time, just a short time, it will be possible to download a full-length movie picture in just minutes. It will be possible to have this then distributed across the world before it makes its cinematic preview.

I believe we have the capacity to preserve the integrity of the arts and entertainment industry in America, but it will take a concerned, cooperative effort among all involved to make it work. It will require a way of thinking, I believe, that allows the industry to protect its rights, but to do it in a way that creates new consumers by intellectually and financially investing in new and creative means.

The goal of the entertainment industry should be to create loyal long-time customers, not engage in short-term strategies that scoop up and make example of folks who may or may not have knowingly engaged in improper behavior, and which then alienates current and potential customers.

It is a reality that the state of ethics, law, and technology are woefully out of step with one another today. Hopefully the dialogue that we engage in here today in this hearing and the hearing I will hold on September 30 will be the factual and intellectual foundation upon which we can engineer some thoughtful and practical solutions for the future. As Senator Sununu noted, we are going to be at this discussion for a while.

There are challenging issues that are involved here. But they touch so many, many people and are so important they deserve this focus. Again, Mr. Chairman, I applaud you and thank you for your leadership on this issue.

Senator BROWNBACK. Thank you, Senator Coleman.

I thought those were all excellent opening statements on a big issue, the narrow ones that we have cast here and the overarching ones that are here as well. Thank you very much, Senator Coleman.

I call up our first panel. That consists of: Mr. William Barr, Executive Vice President and General Counsel for Verizon Communications; Mr. James D. Ellis, Senior Executive Vice President and General Counsel for SBC; Mr. John Rose, Executive Vice President of the EMI Group; Mr. Cary Sherman, President of the Recording Industry Association of America; and Mr. Alan Davidson, Associate

Director, Center for Democracy and Technology in Washington, D.C.

Gentlemen, thank you very much for joining the Committee today on what promises to be an opening salvo of a big discussion, a big discussion that we need. We will go, proceed from left to right if that would be OK, and so, Mr. Ellis, let us start with you, Executive Vice President and General Counsel of SBC. Thank you for joining us.

STATEMENT OF JAMES D. ELLIS, SENIOR EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, SBC COMMUNICATIONS INC.

Mr. ELLIS. Good morning, Mr. Chairman and members of the Committee. Thank you for the opportunity for SBC to share its views on the important issue of individual right to privacy, due process, versus the recording industry's efforts to enforce its copyrights. It is an important issue and one that we believe certainly deserves the exposure that these hearings will provide.

It is a timely topic. As has been mentioned, the explosion in subpoenas from the recording industry took place this summer. I believe the Internet community and the public are only just now beginning to be aware of the full implications of the position taken by the recording industry. I believe that the community as it begins to understand the full scope of the position advanced by the recording industry is going to become very vocal and insistent that their right to individual privacy and due process not be compromised by efforts to enforce copyrights.

Having said that, I want to be very clear. SBC's position is unquestionably that owners of copyrights have every right to enforce them vigorously. And to that extent, we certainly agree with most of the comments that have been made here today. We think it is important to the industry, to the economy, that copyright protections be served and accomplished.

Having said that, I would also add that SBC has a lot of intellectual property and we take every reasonable and responsible step to enforce those copyrights and protect that intellectual property. We do so by going to court, filing a lawsuit, availing ourselves of the rights under the Federal Rules of Civil Procedure. We obtain subpoenas subject to judicial oversight and review.

That happens every day in the courts across this land. That is how it is done, has been for generations. That is how the system has worked. In contrast, the recording industry has taken the position that merely by going into a clerk, making an assertion that their copyright is being infringed, and without notice to the Internet user and without any judicial oversight, they are entitled to obtain the names, address, and telephone number of that user.

Now, I do not believe that any civil litigant or law enforcement agency in this country has that capability. The essence of their position is that once they make that filing with the court clerk and pay their $25, due process and individual right of privacy goes out the window. That cannot be the law in this country.

The implications to that go well beyond the recording industry. If the recording industry can go in to a clerk, pay their $25, make an allegation, and obtain the name, address and telephone number,

then anyone else in this country, regardless of their motive, can do the same thing.

The implications go beyond privacy. They unfortunately go to personal security. The fact is the Internet is not the personal safe haven we wish it was. To the degree there is security, it is usually associated with the fact that e-mails are anonymous. They do not include, your e-mail address does not include, the name, address, and telephone number of the user. So people go into chat rooms, they access web pages, they use the Internet, counting on that anonymity.

Now, if the position of the recording industry prevails that anonymity is stripped away very simply. File your $25 and submit your statement that somebody is infringing on the property. That cannot be the test. If it is, I believe it will be inevitable, inevitable, that the Internet stalker, the child molester, the abusive spouse, or some other whacko who uses the Internet is going to use that same approach to find their victims.

It is for this reason that we support the legislation that was introduced by the chairman. It puts the recording industry in the same position as every other litigant. That is, you go file your lawsuit, you get your subpoena, and you pursue it subject to the Rules of Civil Procedure. If the recording industry has the evidence that people have violated it to the degree that they are entitled to this subpoena, then file the lawsuit. They served 2,000 subpoenas and to my knowledge they filed 200 lawsuits. I assume that means there are 1,800 people that have had their privacy violated without justification.

Bottom line for us is very simple: We do not believe that your constituents, our consumers, and Americans in general lose the right to privacy and due process simply because somebody makes an allegation that there has been wrongdoing and pays $25 to a clerk. That cannot be the law.

I would be happy to have any questions, sir.

[The prepared statement of Mr. Ellis follows:]

PREPARED STATEMENT OF JAMES D. ELLIS, SENIOR EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, SBC COMMUNICATIONS INC.

I would first like to thank Chairman McCain and Senator Brownback and Members of the Committee for inviting me here today to discuss the important issues surrounding the Digital Millennium Copyright Act, the privacy and security of Internet users, and the protection of copyright content.

SBC has a considerable body of intellectual property and we take all reasonable and responsible steps to protect those property rights. We recognize and respect the legitimate interests of other copyright owners as well.

However, when SBC acts to protect or assert its intellectual property rights, it has to follow fundamental and time-tested rules and procedures that are applied every day in our courts. Others, however, advocate what we believe to be a misapplication of the DMCA in order to create a private and limitless right of subpoena—devoid of all rules and procedures. The recording industry has legitimates rights and concerns—but the answer is not to create a private right of subpoena that completely ignores the safety and privacy of America's 100 million Internet users.

Peer-to-peer file swapping technology, like that utilized by music file swappers, did not exist in 1998 when the DMCA was passed. Yet, the recording industry would have you believe that Congress and the ISPs foresaw the future and agreed to strip all Internet users of their rights of privacy, anonymity and due process just because they are accused of infringing copyright over a peer-to-peer network.

Under this distorted interpretation of the DMCA, we have already seen that SBC and all ISPs are being besieged by thousands of subpoenas, all without any court

supervision. Given the fact that these subpoenas are merely rubber-stamped by a court clerk without judicial oversight, we are concerned about the protection of our customers' safety, rights of privacy, anonymity and due process. However, we remain committed to working with the recording industry and all copyright owners to find solutions that properly balance the rights of all interested parties.

I. Accepted Safeguards and Rules of Civil Procedure

SBC and thousands of other litigants adhere to the following fundamental and time-tested rules of procedure when protecting their intellectual property rights:

i. We have to investigate our claim and the elements of the claim.
ii. We have to expose our allegations to the light of day in a court of law;
iii. When we file a suit, SBC must abide by the requirements of Rule 11 of the Federal Rules of Procedure which insures that the attorney who signs the pleadings has undertaken a good faith investigation of the facts alleged,
iv. If necessary, we would petition the court for expedited discovery to learn the name and location of unknown defendants;
v. We could obtain a subpoena for the records of third parties in order to identify such unknown defendants;
vi. We would observe the provisions of Rule 45 of the Federal Rules of Civil Procedure and insure that the subpoena is issued by a Court within 100 miles of the party served which affords that party an opportunity to resist the subpoena in a forum convenient to them; and
vii. Interested parties would be afforded an opportunity to challenge us in court under the supervision of a judge or magistrate.

These same procedures are followed by litigants thousands of times a day in courts all across the country.

II. A System Without Safeguards or Rules

In contrast to the well-settled rules that everyone else follows, the Recording Industry Association of America ("RIAA" or "Recording Industry") and others would propose the following special treatment to avoid the annoyance of rules and procedures:

i. Without regard to Fed. R. of Civ. P. 45, a person claiming to be a copyright owner or its agent can pick any Federal District Court, from Guam to Maine, and can use that court as its private subpoena factory [1] to generate hundreds or thousands of subpoenas on the mere assertion of a "good faith" belief that their copyright has been infringed;
ii. The "good faith" belief is not subject to the obligations or sanctions of Fed. R. Civ. P. 11 because no lawsuit need be filed;
iii. After paying a small fee, and without any substantive review, the alleged copyright owner can require the clerk of the court to issue a subpoena whereby, under force of law, an ISP must within 7 calendar days, provide the name, address, telephone number and e-mail address of the person or persons informally accused of wrong-doing;
iv. The alleged copyright owner never needs to file a formal claim, and never needs to appear before a judge or magistrate. In fact, the party never has to explain what it did with the personal information it obtained.
v. By the time any Internet subscriber would be allowed to protect his/her private information or interests, it would be too late.

Again, Congress did not intend this application of the DMCA to peer-to-peer activity because peer-to-peer technology did not exist at the time the DMCA was passed in 1998.

---

[1] RIAA's disregard for Rule 45 by using the District Court in Washington, D.C. to obtain subpoenas issued to entities located across the country has resulted in at least four court challenges. In addition to SBC, Boston College, MIT and Columbia University have all challenged this disregard for Rule 45. In all but the SBC case, RIAA has either been defeated in court, withdrawn its subpoenas or abandoned efforts to enforce them. While indicating its intent to voluntarily have subpoenas issued from the proper court on a *going forward* basis, RIAA still maintains that it can disregard Rule 45 in that "[t]he DMCA does not require formal service of subpoenas" and that "[t]he DMCA authorizes nationwide service of process." *See: RIAA Reply Brief in RIAA* v. *SBC Internet Communications Inc.,* U.S. District Court for the District of Columbia, Misc. Act. No. 03–MC–1220–IDB, pages 15–16.

III. The Safety and Privacy Risks of No Court Oversight

While SBC appreciates the need to protect legitimate copyright interests, this unsupervised private right of subpoena poses safety, security and privacy risks to all Internet users. There is great risk that others who under the guise of a copyright owner would obtain a subpoena for illicit or illegitimate purposes. A person's name, home address and telephone number might be released without that person ever knowing that the information is no longer private. Based on nothing more than an unverified allegation, personal information can be tied to activities, subject matter or affiliation of a person on the Internet and that information can be used for illegitimate reasons that go beyond copyright enforcement.

In this system, by the time any abuse is discovered, the name, home address and telephone number of the Internet subscriber has already been released. In addition, this private right of subpoena is available to anyone and everyone, not just the Recording Industry. That thought is especially disturbing considering this private right of subpoena is available to a pedophile lurking in an Internet chat room; an abusive spouse, or a stalker. Someone who is intent on doing bodily harm is not going to be dissuaded simply because the law states that they may be liable for "damages or attorneys fees" for misrepresentations. By then, the harm is done.

This past August alone, SBC's affiliated Internet Service Providers received almost 200,000 e-mails complaining of abuses of the Internet. While most of these e-mails complain about spam, and other Internet abuses, a significant number pertain to harassment and threats.

A female subscriber recently complained "This man has been Internet stalking me. He was first asking me to call him and when I refused, he started saying that he loved me. Then I received this in my mail . . . look at the title. I feel he is a threat to me." The title of the e-mail contains clear threats of bodily harm and is too offensive to repeat in this forum. I have submitted a redacted copy of the e-mail for the record.

If this private right of subpoena is ratified, the person making these threats can go to the *clerk* of any district court, submit a short form letter, pay a small fee and force an ISP to tell him this person's name, where she lives, and what her telephone number is. This is but one very real example of how the public policy implication of this issue extends far beyond mere music piracy.

SBC Internet Services, through its Pacific Bell subsidiary, recently filed suit in California against a company called Titan Media, along with the Recording Industry and one other company, over misuse of the DMCA. Titan Media is a purveyor of gay pornography and, by obtaining the issuance of one single DMCA subpoena in California, Titan demanded that Pacific Bell Internet Services turn over the names, addresses, telephone numbers, and e-mail addresses of 59 individuals who were alleged to have illegally obtained its pornography through peer-to-peer file swapping. SBC has no reason to believe that Titan's intentions and tactics are based upon any motivation other than simply protecting its copyrights. However, imagine the potential for abuse if such information is provided to a party with less than honorable intentions. Even associating a person's name with such material might have far reaching affects on the individual's personal and professional life beyond any copyright issues that may exist. The privacy implications of this unsupervised, private right of subpoena are frightening.

IV. Private Subpoena Power—Constitutional Issues

The private right of subpoena sought by the Recording Industry and its allies present difficult Constitutional problems as well. Article III of the Constitution limits the power of the courts to pending cases or controversies. Courts may not be private enforcers. Under this proposed system, there is no requirement that a lawsuit is ever filed. The party obtaining the subpoena never has to expose his claims to a judge or magistrate and never even has to explain what he did with the personal information he obtained.

The evidence at hand indicates that the Recording Industry alone has obtained close to 2,000 subpoenas—all out of the court in Washington, D.C.—but it has only filed approximately 250 lawsuits. This is a clear example of our courts acting as private enforcers with no pending claim or controversy, and this is directly contrary to the Constitution.

This unsupervised private right of subpoena also strips Internet users of their First Amendment rights to communicate and publish anonymously-without due process of law. The Recording Industry and its allies have taken the position that they need only make an allegation of infringement and Internet users have no rights. But that "guilty until proven innocent" proposal goes against our entire judicial system-whether civil or criminal. That so-called logic is analogous to saying that citizens who are merely accused of one particular type of crime have no constitu-

tional rights. Thankfully, our judicial system requires the often bothersome task of actually proving your allegations before the rights of the accused are forfeited.

V. Resource Burdens and Substantial Costs

The interpretation of the DMCA advocated by the Recording Industry and others would result in a limitless, private right of subpoena. As the Recording Industry has shown us, this process can be mechanized like an assembly line. Further, the Recording Industry demands compliance to its limitless subpoenas, all within 7 calendar days. This misuse of the DMCA would require ISPs to allocate significant resources at substantial costs which, according to the RIAA, cannot be recouped from the party seeking the records. In our experience, each subpoena requires approximately one hour to fully process, and that assumes that all information is correct and easily available. That estimate does not include the time to notify the subscriber that a stranger is asking for his/her personal information. That estimate also does not include the cost of assets and tools necessary to do the job.

The Recording Industry has taken the position that ISPs must respond within 7 calendar days, and that they must do so free of charge. This goes against the well-established provisions of Fed. R. Civ. P. 45, and the DMCA and the Federal District Court in the Verizon decision both clearly demand that the protections of Rule 45 apply.

However, this assembly line of subpoenas results in other very real and practical problems as well. ISPs do not operate with unlimited resources. Therefore, if any person can submit a limitless number of private subpoenas and demand an "expeditious response" at no cost, then ISPs will have no choice but to divert resources away from assisting with law enforcement subpoenas and warrants so that they can act as unpaid private investigators for the Recording Industry and others exploiting this abuse of the law.

This issue is NOT just about music piracy, and it is not just about the Recording Industry. Before we create an unsupervised private right of subpoena, sweeping away important procedural and Constitutional protections, all of these public policy issues should be addressed by Congress.

VI. Legislative Resolution

Legislation like that proposed by Senator Brownback addresses all of these issues because it relies on the same time-tested rules and procedures that the rest of us must follow. Requiring the filing of a lawsuit would bring this subpoena power within Constitutional and procedural safeguards. It would require that the alleged copyright owner reasonably investigate his claims, and expose his claims to the light of day, pursuant to the protections of the Federal Rules of Procedure. In so doing, it would provide Internet users basic notice and an opportunity to be heard—all the protections denied to them by the current abuse of the DMCA—and it would require more than a mere allegation based upon not even the slightest amount of due diligence.

Finally, a judge or magistrate would be able to examine the copyright owners' claims, address any glaring deficiencies in the claims, address any applicable defenses, and ensure that no mistakes were made by copyright owners or their computerized search robots. It would recognize the right of third-parties to recover costs associated with these burdens. And, it would provide basic due process before privacy and First Amendment rights are forever lost.

We don't seek to deny them the ability to assert their rights. We seek an opportunity to work together to protect legitimate copyright interests, while safeguarding the security and privacy of Internet users, and respecting the legitimate interests of ISPs. We propose to do this by applying the same rules to one and all. Thank you for your time and attention to this important matter.

Senator BROWNBACK. Thank you very much, Mr. Ellis. We appreciate it.

Mr. Rose, Executive Vice President of the EMI Group. Welcome and the floor is yours.

STATEMENT OF JOHN ROSE, EXECUTIVE VICE PRESIDENT, EMI GROUP AND EMI MUSIC

Mr. ROSE. Thank you, Mr. Chairman, and thank you, members of the Committee, for inviting EMI and me in particular to testify

today. Given the short nature of my remarks, I would ask that my complete statement be entered into the record.

Senator BROWNBACK. They will. And for all of the witnesses today, your complete statement will be put in the record, and so you are free to summarize if you choose.

Mr. ROSE. Thank you.

Unlike many on this panel, I am not a lawyer. My responsibilities include strategy, corporate development, digital distribution, and anti-piracy. I am here today to talk about the impact of the deliberations today on our business.

EMI is a music-only company. Music is the only thing we do, so what is decided and discussed here today is critical to us and critical to our employees. In the United States we employ approximately 2,500 people and, contrary to common belief, the largest concentration of those people are in Jacksonville, Illinois, and they do things like drive forklift trucks and work in warehouses.

I would like to make four points or at least talk about four topics: first, the degree of change that we are facing in the industry and how it is transforming our industry and our relationship to the telecom, computer, and software industries; second, the economics of piracy, the economics to us and the economics more broadly to the telecom and computer industries; third, why this subpoena process is so critical to us; and fourth, while critical, why it is only one small element in a much larger set of initiatives that we are addressing and pursuing to address the changes facing us.

Turning first to the degree of changes, we are facing the functional equivalent of a perfect storm, *i.e.,* change on multiple fronts that are dramatically transforming our business, changes in technology, changes in consumer behavior, in the digital world, in the physical world, changes in retail, and a new set of competitors from other industries, for whom now the content industries are a critical part of their businesses.

Piracy underlies all of these changes and I just want to point to one of the types of changes we are facing. If you go back to this chart, back in 1995 the music industry was pretty simple. You created a disk—vinyl, LP, cassette, CD—you sold it to a consumer, who put it in a purpose-specific device that played it. If you look at the world today, however, just a scant 7 years later, the number of devices have proliferated dramatically and at this point almost any device—number of formats have proliferated—and almost any device can play the content from any format. So we are really facing a world in which the music itself has been disconnected from the format—CD, cassette, digital download—on which it rode in.

One of the things that is doing is changing the underlying nature between the record industry, the telecom industry, the computer industry, and the software industry, creating a degree of interdependency in our economics that heretofore we had never seen.

Let me move to the economics of piracy. Piracy hurts us dramatically in four ways as a record company. First, it affects our ability to invest in artists. We have had over the last couple of years to cut our artist roster by 25 percent because of our inability to continue to invest in generating new artists.

Second, it affects our ability to invest in new technologies and new products and services. Just at the time when we need to be investing in innovation, we are actually counting every penny.

Third, it affects our shareholders. Despite increasing our profits by 33 percent over our last fiscal year, the market's view of the future of the record industry has led to a 76 percent drop in our market cap.

Finally, it affects our employees. Unfortunately, over the last 2 years we have had to lay off approximately 20 percent of our workforce in order to provide returns to our shareholders.

Ironically, in the midst of what has been truly a vitiating set of economics for the record business, if you look at the economics of piracy it is kind of interesting to see that there are actually significant benefits to the telecom, computer, and software industries and consumer electronics industries from file-sharing in a peer-to-peer environment. And while a lot of this debate is about privacy, it is also about economics.

In a good year, the music business, record and publishing, earns between $1 billion to $1.5 billion. The last couple years have not been good. If you decompose the traffic charges, the network service charges, the incremental profits from the sale of purpose-specific content equipment, there is approximately $7 billion of incremental profit that accrued to the telecom, computer, and software and consumer electronics industries.

This is preliminary work, it was done by a third party, and even if it is half right it is pretty important. But those economics threaten to kill the goose that lays the golden egg.

These subpoenas are critical to our future because expeditious identification of infringers are important. One brief example. One of our leading artists recorded a record. Before we actually got our hands on it to start developing marketing plans and manufacturing disks, it was leaked onto the web. 36 hours later in Asia, in the night markets, there were physical copies of his new album for sale with bonus tracks from his previous album, something that dramatically hurt our sales.

The DMCA recognizes the balance between the safe harbor for the ISPs and the need to identify individuals.

Finally, this is just one of several elements we are proceeding. We are pursuing a number of initiatives on enforcement, a lot on awareness, and we are working very hard to make all of our content available in the digital world. We have agreements with over 75 different digital providers currently and we are negotiating more than 100 as we speak now.

Thank you, Senator.

[The prepared statement of Mr. Rose follows:]

PREPARED STATEMENT OF JOHN ROSE, EXECUTIVE VICE PRESIDENT, EMI GROUP AND EMI MUSIC

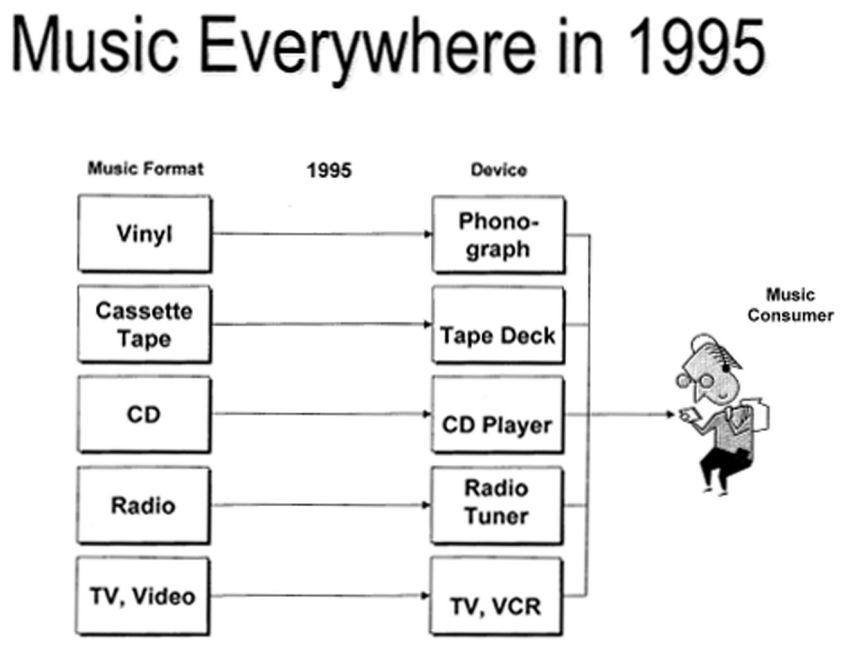
Mr. Chairman, members of the Committee, thank you for inviting EMI Music to testify at this hearing. I am the Executive Vice President of the EMI Group and EMI Music. My main areas of responsibility include business strategy, digital distribution and anti-piracy. I have been with EMI for the last two years. Prior to joining EMI, I had a 20-year career as a consultant at McKinsey and Company serving media, telecommunications, and high tech companies. I am not a lawyer and so am here today to testify about the impact of piracy on the record industry and the var-

ious ways that we are combating piracy, adapting to the emergence of new technologies, and creating new products and services.

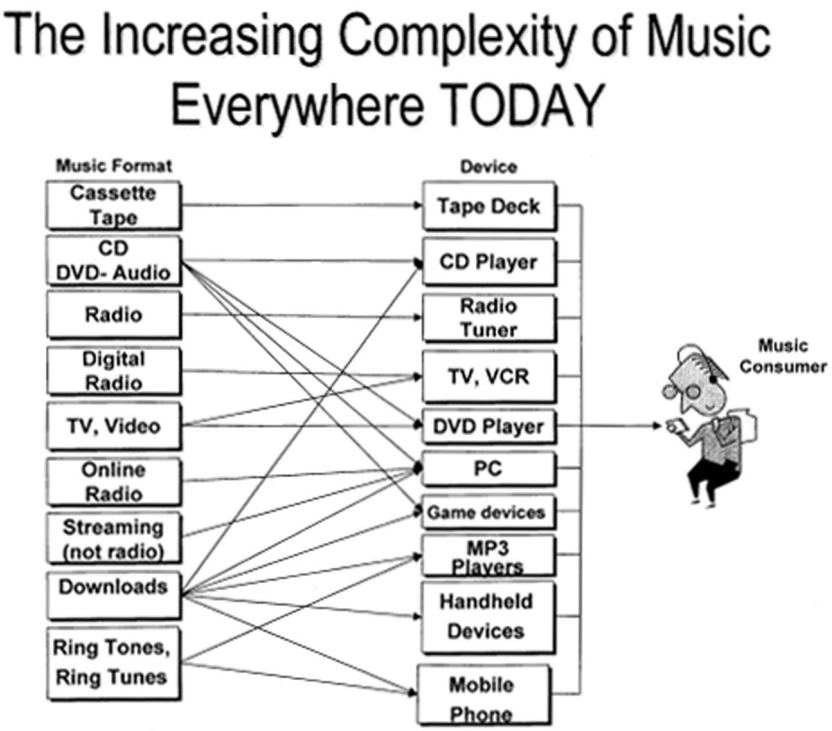
Mr. Chairman, we have to win the battle against digital piracy, and we need your help. We have to win not only because hundreds of thousands of American jobs are at stake, not only because a vital sector of the economy—one of the few that runs a positive trade surplus—is at stake, and not only because our product helps drive expansion of the telecommunications, consumer electronics and personal computer industries. We have to win the battle because the future of a unique American heritage—music—is at stake. EMI Music is the home to the recordings of Frank Sinatra and John Coltrane. Where is the next American music icon? If piracy continues unabated, we may never find him or her.

EMI is unique among the music companies—our only business is music. As a result, we have a big stake in online music. EMI has acted aggressively to make its music available to consumers through legitimate online services to meet consumer demand and thereby combat piracy. The lawsuits brought by the RIAA are only one part of an overall strategy whose goal is to reduce the amount of egregious digital piracy that is eroding our business. The other parts of that strategy are educating consumers and aggressively and eagerly providing our music to consumers the way they want it—by licensing our music to any number of legitimate digital distributors. I plan to discuss these other elements of our strategy later in my testimony.

The last few years have been dramatic ones for the record industry, including EMI. Few industries have faced the intensity of discontinuity felt by the record industry as a result of dramatic changes in technology, new competition from non-music entertainment products, consumer behavior through piracy, and a changing retail environment. Let me give you just one example of the transformative events experienced by the music business. In 1995, music formats and the devices for playing them were simple and the relationship between the two was straightforward. A vinyl record played on a record player. A cassette tape in a tape deck, a CD in a CD player and so on.



A mere seven years later, and not only have the number of music formats and music devices multiplied, but the relationship between the two has grown remarkably complex:



Few industries have coped as well with such extensive changes in their business environment. Still, the future of music has the potential to be dynamic and exciting. As we digitally deliver music to consumers and embrace the potential of new forms of distribution, the music industry has the potential to drive dramatic innovations among the music, telecommunications, consumer electronics and computer industries. But if we do not work across industry lines to solve the music piracy problems we face, the future of the industry also has the potential to be bleak.

I am not going to repeat all of the piracy facts that Cary Sherman of the RIAA has already presented to you in his written testimony. But I do want to highlight three recent statistics. First, according to the NPD Group, 7.5 billion music files on Americans' computers were obtained through peer-to-peer (P2P) file swapping. That's almost two-thirds of the total number of music files on computers. Second, in June of this year, even after extensive publicity that music piracy is illegal, long after the RIAA had initially sought its first subpoena, and long after the RIAA had won its lawsuit against Napster, only 37 percent of people surveyed in a poll knew that downloading files on P2P systems is illegal. Third, the growth in these P2P services has directly and unequivocally harmed our business. Every serious and credible study of these services—conducted by the industry and by third parties—concludes that a significant portion of the decline in record industry sales over the last three years is attributable to these P2P services.

At EMI those numbers have had a real and painful effect on us in several major respects:

- Piracy affects our ability to reinvest in new and developing artists thereby imperiling the livelihood of new artists and the future of music itself. Last year, at least in part due to digital piracy, EMI had to cut its artist roster by roughly one-fourth. Moreover, there is simply no question that digital piracy affects our decisions about signing new artists, how much we are willing to pay artists when we sign them, how long we are willing to maintain an unprofitable relationship with them hoping it will become profitable, and how many artistic risks we are willing to take.
- Piracy affects our ability to invest in new technologies and in new or creative ways to distribute our product.

- Piracy affects each of our shareholders. EMI is the most profitable large music company. Last fiscal year, our operating profits increased 33 percent. But in the same period, our market capitalization declined by 76 percent.
- And finally piracy affects our employees. Last year, digital piracy contributed to our decision to publicly and painfully cut our workforce by about 20 percent. Every other record company is facing the same situation.

In order for us to successfully adapt to these changes and to combat piracy, the legal environment has to remain stable and our ability to enforce and protect our property rights has to be guaranteed. The current legal strategy being pursued by the RIAA using the subpoena authority granted under the Digital Millennium Copyright Act (DMCA) is the result of long and careful thought.

Mr. Chairman, there has been a great deal of debate about the privacy implications of the DMCA subpoena process. As I say, I am not a lawyer, but I am confident of three things:

First, the DMCA subpoena process is structured the right way. It facilitates rapid and efficient resolution of copyright infringement claims, which is vital if we are to have a legal and business climate where technology can develop while at the same time content producers can thrive—protecting their substantial capital investments and making the reinvestments necessary to produce new content.

Let me elaborate on why an expeditious process is so important. Digital piracy of a new CD produced by an EMI artist—or any record company's artist—spreads in a flash. A digital pirate file on P2P systems multiplies like a virus. The pirate file is a perfect replica of the genuine file and enables P2P users to essentially set themselves up as miniature digital factories that can churn out our CDs faster than we can. In order to fight the virus, we have to move very quickly. A delay means that the perfect pirate file can have replicated thousands or hundreds of thousands of times before we can get to it. The DMCA subpoena gives us the speed that is so vital for us to survive.

You may be under the impression that digital piracy is only conducted by unsuspecting teenagers who just want to listen to the music they love. But that's not the case. Digital piracy also encompasses the organized and malicious piracy of hacking groups—rings of thieves whose goal is to obtain advance copies of music, videogames, business software and movies and to leak them onto the web. It also includes the piracy of egregious uploaders who make thousands of copyrighted songs available to anyone with an Internet connection. In fact, according to NPD data, eight percent of the total population of people who save digital files on their computers have more than 1,000 files. Those eight percent account for nearly 60 percent of the music available for download on P2P systems. To be sure, some digital piracy is what you may think of as casual—a 14-year-old coming home after school and listening to a few favorite songs. And, yet, more than 40 percent of all music files downloaded today are by people over the age of 30 according to NPD studies. All these types of digital piracy have direct connections to global physical piracy by organized crime rings.

In one instance late last year, the new album of one of EMI's biggest artists was leaked onto peer-to-peer sites several months before the CD was due to arrive in stores. In fact, it was leaked before EMI itself even had the master recording or could begin to execute its own marketing and sales plan. But because of P2P systems, within a matter of hours, a perfect digital copy of the music was available worldwide. Organized crime rings in parts of Asia were able to download the music, burn thousands of physical CDs, and have them on sale on the streets of Singapore and Hong Kong within a few days—complete with bonus material.

Second, the recent public debate spurred by the DMCA lawsuits has been enormously useful in raising public consciousness. I recently met in my office with a father of two children who told me that he would never allow his children to copy software. But he actually had been proud of his son's ability to download music using P2P systems. The RIAA's public education and legal strategy helped him realize that no principled distinction was guiding his thinking. A three-minute piece of intellectual property that you can listen to on radio may seem like a very different thing than a computer program. But the legal underpinnings of all these copyrighted works is the same. If you undermine the legal support structure for one, you undermine it for all of them.

Third, the current argument raised by Verizon and SBC about privacy is not so much about their customers' privacy as it is about economics. Ironically,

Verizon and SBC's bottom lines are directly tied to the record industry's fortunes as a result of the increasing interdependence and interrelated economics of our industries. The real question is whether the relationship between their profits and ours has to be inversely related. EMI believes that it does not.

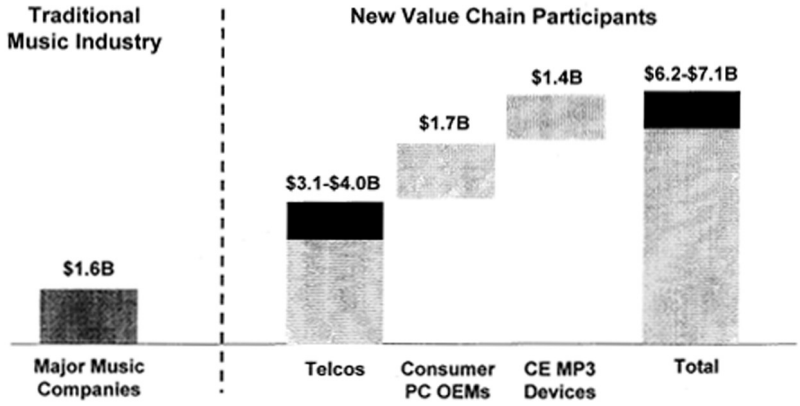
Thus far, the RIAA has asked for approximately 1,500 subpoenas. The regional Bell operating companies, two of which have representatives sitting before you today, have more than 200 million customers. They provide those customers with detailed bills on a monthly basis. They daily respond to many hundreds of thousands of consumer and government inquiries that dwarf the number of subpoenas that the RIAA has issued. Relatively, responding to a few hundred, or even a few thousand, DMCA subpoenas from the RIAA can hardly be a significant administrative burden.

This debate is not about privacy. It is about two phone companies attempting to protect the anonymity of customers who are breaking the law. The telecommunications companies, and the PC and consumer electronics industries, have become increasingly dependent on the content industries, music, movies and video games, to drive their businesses. These are the new economics of piracy.

In a good year, the largest record companies and the largest music publishers generated combined worldwide profits of approximately $1 to 1.5 billion, and this is likely an overestimate. As you know, the last few years have not been so good for the record companies, and those profits have been shrinking.

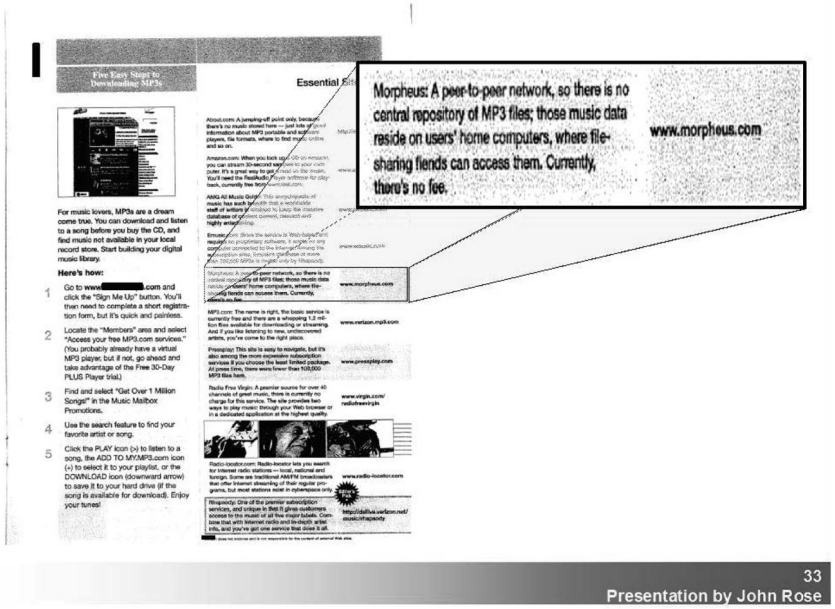
EMI recently commissioned a study that demonstrates that the 2.5 billion to 5 billion files traded per month on P2P systems generate calculable, incremental profits worldwide of almost $7 billion per year for the telecommunications, PC and consumer electronic industries. Moreover, these same companies also derive a completely different set of soft benefits from P2P systems—consumer pick up of their products, accelerated broadband penetration, consumer loyalty to the phone service/decreased churn—that are not included in these calculations. Our findings show that the telecommunications industries alone derive approximately $3–4 billion in worldwide incremental profits from P2P activity. The U.S. share of those profits is approximately $1 billion. The analysis in this study requires further refinement, but it is clear that these three industries are reaping enormous profits as a direct result of consumer digital copyright piracy. Even assuming that these numbers are off by 50 percent, these industries made more profit off digital piracy than the worldwide profits in 2002 of all the largest music companies combined.

Profits Created From Music and Copyrighted Material (2002)



No one in the music industry begrudges the right of the telecommunications, consumer electronics or PC industries to run businesses that profit from consumer behavior. But they certainly should not encourage or protect illegal behavior. A

Verizon brochure from last year illustrates this point. The cover of the brochure on "broadband living" highlights three main benefits to buying a broadband connection: sharing photos, working from home and downloading music. That brochure then lists among music sites, a P2P site whose only application for copyrighted music is illegitimate.



It has never been clearer that what happens in one industry—telecommunications—affects what happens in the other, the copyright industries. The DMCA understood and even tried to pave the way for a mutually beneficial interdependence. ISPs were relieved of liability in most circumstances—thereby removing a legal burden that could have hampered their development. But the copyright industries were provided with a simple, effective and speedy technique for protecting their property—thereby ensuring that rampant digital piracy would not undermine the copyright industries' business model. The DMCA anticipated a collaborative process between all of the stakeholders in the digital copyright world.

At EMI we are trying to deliver on that collaborative process. As I said at the beginning of my testimony, our strategy for combating piracy has three prongs: enforcement, awareness and availability. We will enforce our legal rights vigorously. We will strive to make our music widely available. Finally, we will undertake significant public awareness campaigns. You are already aware of the enforcement efforts that the RIAA has undertaken and the public awareness campaigns.

EMI has been at the forefront of efforts to legally distribute music online. No other company has been as aggressive and assertive about these opportunities. EMI was the first of the global record labels to license its repertoire to Pressplay and MusicNet, the first two legitimate digital music distributors. To date, EMI has licensed its music for digital distribution to almost 75 companies, and approximately another 75 deals are currently in the pipeline. Almost 34,000 EMI tracks are available for download in the United States. 140,000 are available worldwide. Our online music is available at Apple's iTunes store, at *Buymusic.com,* at MusicMatch and on nearly every major portal and site that sells legitimate digital music.

Important Players are Starting To Promote Legitimate Services

In the face of massive industry change, EMI is actively finding ways to rethink its product and its distribution approaches. The music industry is learning to sell its music in an ever-expanding number of formats in only a few years. EMI has created standard deal terms, legal licenses, product definitions and deal policies that it uses worldwide. The music industry has been criticized for being slow to join the party. But given the dramatic paradigm shift the industry has undergone, I would say it's actually been faster than other industries in comparable positions. Our ability as an industry to respond is at least comparable to that of the computer industry's response to the evolution from the mainframe to the mini-computer to the personal computer.

Mr. Chairman, EMI Music is one of the world's oldest recorded music companies. It began in 1897 with the formation of two companies, The Gramophone Company Ltd and the Columbia Graphophone Company Limited. Those two companies merged in 1931 to create Electric and Music Industries.

Today, EMI is the third largest record company in the world and the fifth largest in the United States. Its labels in the United States are Capitol, Virgin, Blue Note, Angel, Manhattan, Narada, EMI Christian Music Group, Capitol Nashville, Astralwerks, Higher Octave and S-Curve. EMI's employees are not just in New York and Los Angeles. In fact the majority of our employees are based elsewhere in the United States. We have employees in Milwaukee, Wisconsin, Jacksonville and Chicago, Illinois, Atlanta, Georgia, and Miami, Florida among other cities. We are actually the largest employer in the Nashville music community as well.

EMI releases the works of some of the world's best known and loved artists: the Beatles, the Rolling Stones, Garth Brooks, Frank Sinatra, the Beach Boys, Norah Jones, Radiohead, Kylie Minogue and Coldplay to name a few.

But we also work with a number of artists you may not have heard of—yet. These are the hundreds of new and developing artists that we hope to be able to bring to the world. Keri Noble is a new artist with Angel whose 5 song EP was just recently released. Joss Stone is a remarkable new soul singer whose first album on S-Curve Records was released yesterday. Jennifer Hansen and Dierks Bentley are two of country music's most exciting new acts. Tribalistas are superstars in Brazil who are beginning to be discovered by American audiences. Maksim is a classical pianist whose first album has just been released in Europe. Online piracy threatens EMI's ability to work with and invest in these new artists and others.

Digital piracy and its follow-on effects have a serious impact on the way we do business. The first recordings made for EMI were made using the old-fashioned horn gramophone. We've been through 78 rpm records, LPs, eight track, cassette tapes and now CDs. More advanced audio platforms such as DVD Audio and SACD could be the next technology leap. But today we have to deal with changes that are

among the most disruptive we've ever faced. Records are still as expensive to produce and market. Those costs do not go down and in fact they continue to go up. But because of piracy, it is harder and harder to run a profitable, long-term business.

EMI is the only major record company whose sole business is music. We want to work collaboratively with the telecommunications, consumer electronics and personal computer industries rather than sitting in conflict with them. We are dedicated to making the music business work and thrive. And we have a workable model to accomplish that goal. We are aggressively distributing our product digitally and physically. We have implemented significant measures to curb rampant physical piracy, and we remain committed to intensifying those efforts in the future.

Thank you for this opportunity to testify.

Senator BROWNBACK. Thank you, Mr. Rose. We look forward to the question and answer session.

Next will be Mr. Cary Sherman. He is President of the Recording Industry Association of America. Mr. Sherman, thank you for joining us today.

STATEMENT OF CARY SHERMAN, PRESIDENT, RECORDING INDUSTRY ASSOCIATION OF AMERICA

Mr. SHERMAN. Thank you for inviting me to testify.

Senator BROWNBACK. You have to get those microphones up pretty close.

Mr. SHERMAN. OK. Is that better?

Senator BROWNBACK. Much better.

Mr. SHERMAN. Thank you.

I am the President of the Recording Industry Association of America, the trade association representing the U.S. recording industry, and our members create, manufacture, and/or distribute 90 percent of all legitimate sound recordings in the United States.

At the outset I would just like to share some of the startling statistics about the impact of piracy on the music industry. Over the past 3 years, shipments of recorded new music in the U.S. have fallen by an astounding 31 percent. Hit records have been impacted most dramatically. In 2000 the ten top-selling albums in the U.S. sold a total of 60 million units. In 2001 that number dropped to 40 million; last year, 34 million.

The root cause for this drastic decline in record sales is the astronomical rate of music piracy on the Internet. Although this Committee has long stood on the front line in the battle to protect consumer privacy online and offline, it is important to make one thing crystal-clear: no one has a privacy or First Amendment right to engage in online copyright infringement. The issues presented by today's hearing have a lot more to do with piracy and a false sense of anonymity than privacy.

Millions of Americans have downloaded P2P software onto their computers in the last 3 years. By doing so, these individuals have opened their hard drives to the world, illegally sharing copyrighted material, and often unwittingly exposing their most sensitive personal information, including tax returns, medical and financial records, resumes, and family photos. At any moment you can log on to Kazaa, the world's most popular P2P system, and find any of these documents at the click of a mouse. It is hard to imagine more fertile ground for identity theft.

It is no wonder why Judge Bates, who presided over our lawsuit with Verizon, concluded: "If an individual subscriber opens his com-

puter to permit others through peer-to-peer file-sharing to download material from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."

Despite the inherent privacy risks of using peer-to-peer software, Verizon and SBC have done absolutely nothing to educate or warn subscribers about the privacy risks of using these services. The record is no better when it comes to warning about the legal consequences of using free sites to get music. Nowhere in their brochures, websites, or advertising are there any warnings or information about the grave privacy and real legal risks associated with using this software.

By contrast, they have used a combination of overt and subtle marketing strategies to encourage people to sign up for DSL so that they can get all the music they want for free and not have to go to the record store any more.

The motivation for this strategy is clear when you look at the broadband landscape. According to a USA Today article a few days ago, 70 percent of Americans with broadband capabilities use cable modems instead of DSL. The same article quotes an Internet analyst saying "It is going to be more streaming video and music downloading that is really going to dictate the switch." A recent report on broadband found that the growth in peer-to-peer is really driving the market and P2P traffic now consumes 50 to 70 percent of the capacity, up from perhaps 20 to 30 percent a year ago.

With a long way to go before catching up with cable, it is no wonder Verizon and SBC, the Nation's two largest DSL providers, are reluctant participants in the fight against online piracy. Fortunately for the copyright community, the vast majority of other ISPs around the Nation have been responsible and constructive partners in this important fight.

It is difficult to discount the commercial interests of Verizon and SBC when weighing the merits of their privacy arguments. After all, rather than focusing on the most pressing privacy problem facing their customers, they champion protecting the anonymity of subscribers who are engaged in clearly illegal activity. So while millions of their users are exposing their most sensitive personal information to the world, Verizon and SBC want this community to believe that the true threat to their customers' privacy is the DMCA information subpoena process.

What is even more remarkable is that their alternative to the DMCA process, John Doe lawsuits, would force copyright owners to sue ISP customers first and ask questions later. That strikes me as one of the least consumer-friendly options imaginable, not to mention the significant and unnecessary burden it would place on our Nation's already overburdened Federal courts.

The reality is that Verizon and SBC, under the self-serving guise of protecting their customers' privacy, simply do not want to live up to their end of the DMCA deal struck back in 1998, providing copyright owners with the limited information necessary to protect their rights in the digital world. In the end, we believe that Congress struck a fair balance in 1998 when it passed the DMCA and gave copyright owners the limited ability to access minimal infor-

mation solely for the purpose of identifying infringers and enforcing our rights.

As these issues continue to wind their way through the courts, we remain ready and willing to talk with ISPs about ways to ensure that the DMCA process operates smoothly and fairly, and I hope we can achieve that.

I look forward to answering the Committee's questions. Thank you.

Senator BROWNBACK. Thank you, Mr. Sherman, for your testimony. I look forward to questions afterwards.

Mr. William Barr, Executive Vice President and General Counsel for Verizon. Welcome to the Committee.

STATEMENT OF WILLIAM BARR, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, VERIZON COMMUNICATIONS

Mr. BARR. Thank you, Mr. Chairman.

The Internet is evolving into the central communications system for our society and promises vast benefits. It perfects markets by bringing buyers and sellers together. It is in fact providing essentially the archetypical public library for our society and it creates public forums for the exchange and debate of ideas.

But, as with any communications system, the vitality of the Internet ultimately depends on people's confidence in the security and privacy of their communications. People would not be using the telephone as much as they do if they felt it was easy for others to listen in. The Internet's development would be severely curtailed in our view if people felt that whenever they went out onto the Internet there were few safeguards against finding out who they are, what their communications—what communications they were having, and what websites they were visiting.

So apart from any philosophical commitment to privacy interests, there is a compelling business reason why community communications companies like Verizon are concerned about the privacy of their customers. Now, as with any communications system, they are capable of facilitating a lot of good, but at the same time they can also be used to do bad things. Telephones can be used for wire fraud. The Internet is used for a lot of bad things—dissemination of pornography, for fraudulent practices, and, yes, for the infringement of property rights, copyrighted material.

Now, up until now Congress has recognized that investigative and enforcement tools that are supposed to police against these kinds of abuses, these kinds of evils, have to be carefully crafted and controlled to ensure that they do not sacrifice legitimate privacy interests. That is why even when the government itself is pursuing the dire interests of the public, such as terrorism investigations or investigations into pedophiliacs stalking kids on the Internet, the government itself is subject to controls and supervision.

We agree that the recording industry has compelling property interests that deserve to be protected. We ourselves hold intellectual property rights and we try to enforce them. But that does not justify sweeping, invasive, and unsupervised access to sensitive information about individuals.

Now, when people use the Internet they rely on some protection of their identity, when they are visiting websites, exchanging e-

mails, because they are only identified by a number, the IP address. What this does is allow someone to come in, get the IP address, and thus identify them with their expressive activity.

Now, as the RIAA is interpreting the statute any individual can come in, file a one-page form that is based solely on an assertion and a statement that they believe that a copyright interest is being infringed, and based on that and on that alone we are compelled to turn over the identity of our customer.

Now, it is important, this is not just a right given the recording industry. Anybody can use this in our society. And it does not just relate to recording; it relates to anything that someone suggests is covered by copyright, including things that are unregistered and therefore could not serve as a basis for a suit.

Now, this is done without any judicial supervision. There is no one determining the bona fides of the person seeking this information. There is no protection against someone coming in and using a false name, getting access to this information. There is not even an inquiry into whether or not there is in fact copyrighted material, much less registered material that could actually serve as the basis for a lawsuit. And there is no scrutiny as to whether there is any reasonable basis to believe that the individual has impinged on that property right.

The Federal Government does not have this power in any arena. Congress has not given this power to the Federal Government investigating terrorism. Why should the record industry, private citizens, have this unfettered subpoena authority to reach the most sensitive information that people have?

There are no safeguards on its use. There is no requirement that it is used only for litigation. There are no express provisions dealing with penalties for the improper disclosure of this information. The government itself is subject to all these requirements.

Now, as you pointed out, Mr. Chairman, this is not just a tool that would be used by legitimate interests. Pornographers, stalkers, identity thieves would have the ability to do this and do it anonymously, so it could never be traced back to them. Even where the interests are legitimate, as with RIAA, a blunderbuss approach inevitably leads to abuses and mistakes. The use of bounty hunters has now arisen because they do not have to—the holder of the copyright does not have to identify themselves. They can go through intermediaries and use bounty hunters.

We now have the use of robots to track down people on the Internet, and we have already many examples of mistakes, like kids getting jerked around because they did a book report on Harry Potter or a university's system being shut down because a professor was named "Usher" and it was confused with the name of an artist.

Now, any response to this really requires three things in my view. One is a technological approach, and that is clearly what Congress envisioned in Title I of the Act. What Congress said in Title I of the Act was, if you protect this information with encryption or other kinds of protective devices, access codes, it will be a Federal crime to try to defeat it. So Congress set the table for the industry to work together to come up with these technological solutions. That has not happened because they preferred this jihad against 12-year-old girls.

Now, the other thing is an appropriately tailored discovery device, appropriately tailored like all available—with all the standard accountability in it, where it deals with registered material, there has to be specificity in the allegations, and strict limits on its use, and ultimately judicial supervision over it.

Finally, I think there has to be attention to the incentives, and this is where I think—I do not view the average American teenager as a thief or intentional thief. I think that the industry itself has to look in the mirror to see what created the incentives for this illegal and illicit activity. It has largely been the untenable business model in my view of the recording industry.

What young people want, as we wanted when we were kids: Buy the 45 rpm, buy the hit, and do your own mix. That is what people have always wanted. What is the model today? Can you go out and buy a hit? No. You have to buy a lot of schlock on a CD and pay 16 bucks for it in order to get the one or two songs you want. That is called bundling, and that is the business model necessary to feed the distribution chain that has come up in this industry.

Now, I am not justifying the piracy, but in my view it is not the freeness that drives the kids to download; it is the desire to be selective in what they want, identify the one song, and put it on their mixes. The industry itself has now slowly come to recognize that it left the vacuum. It did not go out and set up the iTunes or the MP3s that are paid sites. In fact, it fought them and it fought them up until recently.

But if the industry itself would move into this area then, just like the film industry when they tried to—when they said that the VCR was the Boston Strangler of their industry, they would end up making more money ultimately.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Barr follows:]

PREPARED STATEMENT OF WILLIAM BARR, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, VERIZON COMMUNICATIONS

Mr. Chairman and members of the Committee, thank you for inviting me here today to discuss this important issue.

We at Verizon recognize the legitimate interests of copyright owners and the threats to those interests that are posed by the misuse of new technologies, including peer-to-peer software. Verizon remains committed to working with the copyright community to find solutions to these issues that result in effective protection for intellectual property, without placing substantial burdens on Internet service providers or violating the privacy and First Amendment interests of their subscribers. Back in 1998, Verizon and other service providers agreed in the Digital Millennium Copyright Act ("DMCA") to conduct voluntary industry negotiations aimed at developing "standard technical measures" (also known as digital rights management tools), to protect copyright works from online infringement. The copyright community has never accepted our offer to begin negotiations on digital rights management standards and to work cooperatively toward a technical solution to this problem.

Indeed, Congress recognized in its report on the DMCA in 1998 that technological rather than legal solutions constituted the best method of ensuring the lawful dissemination of copyrighted works in our new networked, digital environment. *See* S. Rep. No 105–190, at 52 (1998) ("The Committee believes that technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age."). Congress, in Title 1 of the DMCA created criminal penalties for those who circumvent such technical measures.

In the end, as in the area of VHS recordings and cable television access to broadcast programming, Verizon believes that appropriate technical and legal solutions will be found. As discussed in detail below, a new, unbounded subpoena power is not that solution.

As an Internet service provider, Verizon promptly takes down infringing material that resides on our system or network in response to requests from copyright owners and we have strict policies against infringement of copyrights. Verizon also promotes legitimate pay music sites such as MP3.com and Rhapsody as part of its ISP service. We will continue to work with copyright owners to marry the power of the Internet with the creative genius of content providers through new business relationships and licensed websites that offer music, video, and other proprietary content to the over 100 million Internet users in this country. Verizon believes that lawful and licensed access to quality content is essential to the continuing development of the Internet in general and broadband in particular, and we are committed to exploring technological and other solutions so that copyright owners may enjoy the fruits of their labors and Internet users will have access to a rich array of digital content.

However, the answer to the copyright community's present business problems is not a radical new subpoena process, previously unknown in law, that un-tethers binding judicial process from constitutional and statutory protections that normally apply to the discovery of private data regarding electronic communications. Verizon believes that the district court was wrong in concluding that Congress authorized such a broad and promiscuous subpoena procedure—but whatever the courts ultimately conclude on this issue—the subpoena power endorsed by the district court is not an effective remedy for copyright holders and has great costs in terms of personal privacy, constitutional rights of free expression and association, and the continued growth of the Internet.

As interpreted by the district court, this subpoena provision grants copyright holders or their agents the right to discover the name, address, and telephone number of any Internet user in this country without filing a lawsuit or making any substantive showing at all to a Federal judge. This accords truly breathtaking powers to anyone who can claim to be or represent a copyright owner; powers that Congress has not even bestowed on law enforcement and national security personnel. It stands in marked contrast to the statutory protections that Congress has enacted in the context of video rentals, cable television viewing habits, and even the requirements for law enforcement officers to gain access confidential data associated with electronic communications.

All one need do is fill out a one-page form asserting a "good faith" belief that a copyright has been infringed and one can obtain identifying information about anyone using the Internet There is no review by a judge or a magistrate; the clerk's office simply issues the subpoena in ministerial fashion. This identifying information can then be linked to particular material sent or received over the Internet, including e-mails, web browsing activity, chat room postings, and file-sharing activity. This subpoena power applies not just to music recordings, it applies to the expression contained in an e-mail or posting in a newsgroup, digital photographs, and even pornographic materials. It has and will be used and abused by parties far less responsible than the recording or movie industries. In essence, anyone willing to assert that they have a good faith belief that someone has used their words, pictures or other expression without permission becomes their own roving grand jury, without any of the normal checks and protections that apply to governmental investigations.

This subpoena process lacks the most basic protections that are applied to the discovery of confidential and personal data connected with expressive activity. As noted above, the filing that need be made is truly minimal, and is below the standard for the filing of a civil complaint in Federal court. The normal duties to investigate and substantiate a civil claim that apply to the filing of a lawsuit under the Federal Rules of Civil Procedure do not apply. The clerk's office simply rubberstamps these subpoenas in ministerial fashion—with no inquiry into the bona fides of the party filing the request or the self-interested "belief' that a copyright has been violated.

The individual subscriber, whose identity is at issue, is not even entitled to receive notice of the subpoena before his or her personal information is turned over to a third party. Thus, the subscriber, who may in fact be doing nothing illegal, will have his or her identity revealed without ever having an opportunity to be heard. Nor is there any provision for damages or other punishment for wrongfully obtaining or misusing the identity of a subscriber subject to such a subpoena. It is truly ironic that Congress has placed more substantial requirements and protections on law enforcement access to confidential information regarding electronic communica-

tions than apply to a private party under this statute.[1] This combination of unlimited scope, minimal substantive requirements, and lack of judicial supervision makes both mistakes and intentional abuses of this new power inevitable. Every time you send an e-mail, browse a website, or join a discussion in a chatroom or newsgroup, others gain access the numerical IP address that you are using. Armed with this IP address, anyone to whom you have sent an e-mail, from whom you have received an e-mail, with whom you or your children have spoken in a chat room, or who operates a website you have visited, no matter how sensitive the subject matter, can unlock the door to your identity.

This list is not limited to those with legitimate interests in enforcing copyrights. As safety and privacy groups like the National Coalition Against Domestic Violence and WiredSafety stated in our litigation, it opens the door to your identity to people with inappropriate or even dangerous motives, such as spammers, blackmailers, pornographers, pedophiles, stalkers, harassers, and identity thieves. In fact, over 92 diverse organizations, representing consumer and Internet interests, submitted letters to this Committee expressing serious concerns about the privacy, safety, and security of Internet users arising from the potential misuse of this subpoena process. These include the ACLU, the American Library Association, the Consumer Federation of America, and the National Coalition Against Domestic Violence. These groups do not condone copyright infringement. Rather, like Verizon, they are concerned that this subpoena power will cause great harm to privacy, free expression, and even personal security of Internet users with little gain in copyright enforcement.

As Ms. Aftab, from WiredSafety states, "With one broad sweep, the DMCA subpoena power will frustrate the work of the entire online safety community to arm our children and their parents with cyber-street-smarts. It won't matter what they voluntarily or mistakenly give away. All the information predators need can be obtained far more easily with the assistance of the local Federal District Court Clerk." The potential for abuse of this new subpoena power is limited only by the deviousness of the criminal mind.

Indeed, just since the district court's ruling went into effect in June, the evidence of mistakes, potential abuses, and troubling uses of this subpoena power has continued to mount. As you will hear from SBC directly, their company recently filed a suit in California against the Recording Industry, a copyright bounty hunter called "MediaForce" and an entity called Titan Media Group. Titan Media, a purveyor of pornographic videos over the Internet, sent one subpoena to SBC seeking the names, addresses and phone numbers of 59 individual subscribers who Titan asserted were infringing its copyrights in gay pornographic videos by exchanging them over the Internet. Titan eventually withdrew the subpoena when SBC threatened a court challenge, but the episode highlights the fact that this new subpoena power applies to *anyone* who can claim an interest in *any* form of expression. Titan Media, imitating the RIAA, has recently announced its own "amnesty program." Internet users must reveal their identity to Titan and agree to purchase a copy of their pornographic material or Titan threatens to use the subpoena process to expose their identity. In a similar vein, ALS Scan, a purveyor of graphic Internet pornography, has also been a beneficiary of this process and submitted a declaration in favor of RIAA's broad interpretation of the subpoena power in the litigation with Verizon. The potential for abuse, for invasion of personal privacy, for reputational harm, and even for blackmail is highlighted by these examples.

There is also no requirement that the copyright owner itself obtain the subpoena; it may be obtained by an agent of the copyright holder. A whole industry of copyright "bounty hunters" has sprung up, enterprises that search the Internet for possible instances of copyright infringement spurred on by economic incentives. The use of automated robots, known as "bots" or "spiders" has also led to a significant number of mistaken claims of copyright infringement. These bats operate much like the spiders that crawled through buildings in the movie Minority Report, scouring the Internet in search of file names that look like they match the names of copyrighted works or artists. Bots are far from perfect. Typing words such as "Madonna" or "the police" in an e-mail may earn you a DMCA subpoena, because the "bots" cannot distinguish the legitimate comment or discourse from copyright infringement. In 2001, Warner Bros. sent a letter to UUNet demanding that they terminate the Internet account of someone allegedly sharing a Harry Potter movie online. The small text file was entitled "Harry Potter Book Report.rtf," with a file size of 1k. The file was not an unauthorized copy of the movie, it was a child's book report, but the bot could

[1] *See, e.g.,* 18 U.S.C. § 3121, *et seq.* (pen registers and trap and trace devices limited to govermnental personnel upon court order for valid criminal investigation); 18 U.S.C. § 2703 (limits on disclosure of records pertaining to electronic communications services).

not tell the difference and such an "investigation" can quickly form the basis for a DMCA subpoena.

In the past few months, RIAA has already admitted numerous cases of "mistaken identity." In one case, RIAA demanded the take down of Penn State University's astronomy department's servers during finals week, based on a claim that it contained infringing songs by the artist Usher. In fact, "Usher" is a professor's last name and the file at issue was his own creation. RIAA later admitted sending at least two dozen other mistaken notices to Internet users as part of its campaign to warn peer-to-peer file-sharers. And this was before RIAA began its new campaign sending hundreds of subpoenas for subscriber identity to ISPs across the country. These chilling examples all sound like excerpts from the book "1984," except in this case, "Big Brother" isn't the Government, it is interested parties armed with their own private search warrants.

RIAA's most recent campaign began in July of this year after the district court's ruling went into effect. Despite the pending appeal on this issue, the Recording Industry has chosen to unleash numerous subpoenas on Internet service providers. Verizon has already received over 200 subpoenas, with which we have been required to comply. The Recording Industry alone has sent well over 1600 subpoenas to service providers across the country, placing a significant strain on the resources of the clerk's off1ce of the district court in D.C. and on the subpoena compliance units at many Internet service providers, including Verizon.[2]

As another example of the overreaching uses of the subpoena process,, RIAA now claims that it is entitled to discover subscribers' e-mail addresses and that it may issue these subpoenas from the district court in Washington, D.C., regardless of the location of the service provider or the customer. Obviously, obtaining the subpoena in a distant forum makes it a practical impossibility for many service providers and most customers to ever raise any objection to the subpoena. Indeed, Boston College and MIT successfully fought to quash subpoenas issued out of Washington, D.C. that were aimed at their students in Massachusetts. SBC's lawsuit includes jurisdictional challenges. Columbia University is seeking to quash subpoenas that RIAA has attempted to serve on it issued by the District of Columbia courts.[3]

In Verizon's view, Congress never intended to unleash a massive wave of subpoenas on public and private Internet service providers and their customers. This is not an effective solution to the very real problems faced by copyright owners; it only creates an additional level of problems for Internet service providers and chills the free exchange of protected content over the Internet. The use of the subpoena power in an attempt to create an *in terrorem* effect over the entire Internet is both improper and disserves the long-term interests of both copyright owners and Internet service providers. The district court has truly created a Frankenstein monster that Congress never contemplated and that has the potential to cause irreparable damage to public confidence in the privacy of Internet communications. Like the telephone itself, the growth of the Internet as a medium of political, social and economic change depends upon the confidence of users in the privacy of their communications and communications habits. Every person in this room believes that his or her private e-mail or web browsing habits can and should remain private—yet the district court's erroneous decision is a direct threat to that privacy. It has also burdened Internet service providers with responding to thousands of subpoenas. From our own experience, we can tell you that RIAA's barrage of subpoenas has diverted and strained our internal resources. This new burden on service providers—responding to thousands of subpoenas issued in the conduit context—was never part of the statutory compromise. It also threatens the limited resources of subpoena compliance units to satisfy legitimate law enforcement requests—as RIAA bombards

---

[2] Indeed, press accounts indicate that the clerk's office of the district court in D.C. has been overwhelmed with subpoena requests and has been forced to reassign staff from other judicial duties. *See Ted Bridis,* Music Industry Wins Approval of 871 Subpoenas Against Internet Users, Associated Press (July 19, 2003) at 2 ("The RIAA's subpoenas are so prolific that the U.S. District Court in Washington, already suffering staff shortages, has been forced to reassign employees from elsewhere in the clerk's office to help process the paperwork, said Angela Caesar-Mobley, the clerk's operations manager.").

[3] The Federal Rules of Civil Procedure generally provide for the issuance and service of subpoenas in the district where the party in possession of the material resides to protect the rights of third parties to contest the subpoena. *See* Fed. R. Civ. P. 45(a)(2) & 45(b)(2) (placing jurisdictional and service limitations on district court subpoenas for the protection of those from whom production is sought). Despite the fact that Congress expressly provided that the protections of Rule 45 should apply to Section 512(h) subpoenas, *see* 17 U.S.C. §512(h)(6), RIAA has taken the position that it may obtain and serve a Section 512(h) subpoena from any district court in the country. Thus, in its view, it could seek a subpoena from the district court in Guam targeting a small service provider in New England.

service providers with dozens of subpoenas and purports to require responses on seven days or less notice. The protection of copyright, however legitimate a cause, should never be raised above law enforcement and national security efforts—efforts that Verizon has always been in the forefront of supporting.

Both the district court in our case and the copyright owners have eschewed a more measured remedy that has always existed in the law and is used by numerous businesses for many purposes, the so-called "John Doe" lawsuit. Under this procedure, a judge or magistrate reviews the merits of a case before a subpoena is issued, and the defendant is given notice and an opportunity to contest disclosure. The law demands a reasonable investigation of the relevant facts, ownership of a valid copyright registration, and a complaint filed in compliance with Rule 11. Verizon has successfully used this process to sue unknown spammers who abuse our network. Despite the Recording Industry's assertions to the contrary, the filing of a John Doe lawsuit is much more protective of all parties' interests than the DMCA subpoena process.

Since RIAA launched its subpoena campaign, the DC Clerk's Office publicly complained that its internal resources were being burdened and the clerk's office had to re-assign new employees to the fulltime task of processing subpoenas on an ongoing basis. If the district court's decision in our case is not overturned quickly, it threatens to turn the Federal courts into free-floating subpoena mills, unhinged from any pending case or controversy, capable of destroying anonymous Internet communication, and threatening privacy and due process rights as well as public safety.

While Verizon firmly believes that this subpoena process and the tactic of targeting college students, universities, libraries and other individual Internet users is inappropriate and will lead to serious harms with little gain in copyright protection, Verizon recognizes that a more comprehensive and long-term solution is necessary. Verizon commends Senator Brownback for taking a first step by introducing the Digital Consumer Internet Privacy Protection Act. This bill builds in necessary protections that addresses the fundamental due process and privacy rights of all Internet users, and ensures that subpoenas cannot be issued without sufficient judicial safeguards in place. The bill also appropriately gives the FTC enforcement authority to monitor the use of subpoenas involving digital media products and provides remedies for abuses of the process. An appropriate next step would be for affected parties to develop effective approaches that combine technical and legal solutions to balance the legitimate needs of all stakeholders. We urge Congress to act now before irreparable damage is done to public confidence in the Internet as a medium of free expression and association.

I thank the Chair and the members of this Committee for your attention. We look forward to working with you to resolve this critical issue.

Senator BROWNBACK. Thank you, Mr. Barr. I look forward to questions.

Finally will be Mr. Alan Davidson. He is Associate Director, Center for Democracy and Technology here in Washington. Mr. Davidson.

STATEMENT OF ALAN DAVIDSON, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DAVIDSON. Thank you, Mr. Chairman, and Members of the Committee. The Center for Democracy and Technology thanks you for holding this important hearing and we are pleased to be included, both because of CDT's long history of involvement on online privacy issues and also our current efforts to craft a balanced consumer perspective on digital copyright.

Our bottom line today is this: the 512(h) subpoena process is an important tool for copyright holders who are legitimately seeking to enforce their rights online, but it also raises real and serious privacy concerns for Internet users. The good news in our testimony today is that we believe that a package of minor additions to the law could address many of the most serious privacy concerns while also preserving and maybe even enhancing legitimate enforcement.

I will summarize. Our testimony makes four main points. The first is this: it is unhealthy for our country and unfair to copyright holders for large numbers of people to routinely violate the law of the land. Enforcement actions like those that have been undertaken by RIAA are, unfortunately, today a necessary part, though only a part, only a part, of protecting creators and authors in the digital age.

We actually agree with the approach that was taken by RIAA in its statement with the IT industry last winter that emphasizes new delivery mechanisms, education, and enforcement rather than seeking controversial new government technology mandates or network architecture changes.

Our second point is this: if you believe in enforcement, as we do, then you must give copyright holders the tools that they need to do enforcement, and our belief is that a subpoena process like that under 512(h) has an important role in assisting enforcement. With appropriate safeguards for individuals, it could actually be preferable to filing a large number of Federal lawsuits.

Our third point, and I think one that we need to say a little bit more about, is that there really are privacy concerns raised by the unique subpoena power currently granted under 512(h). As has been said here, online identity can be a very sensitive piece of information for people. People online reasonably expect that they will be largely anonymous when they visit health websites, when they make political statements, when they visit chat rooms or become online whistleblowers. For that reason, our law has traditionally strongly protected subscriber identity.

In contrast, section 512(h) contains very few of the safeguards that are demanded by either fair information privacy principles or that are typically found in existing subpoena or court order provisions. We have heard it from several of the panelists already today: 512(h) is available to any copyright holder, not just mainstream companies, record companies, or movie studios; and it can be used based on a mere allegation of infringement. No judge ever looks at a 512(h) application, no weighing of the assertions in the application is ever done, no user ever gets to challenge those assertions. The law places no real limits on how the information is going to be used, beyond the very open-ended requirement that it is going to be used for, "protecting rights."

512(h) gives no notice to end users, who typically have no idea that their information is being revealed. And notice, I should say, has long been a bedrock of our privacy law because it gives the party that is actually harmed the chance to combat potential misuse.

Because of all of this, 512(h) we believe is ripe for misuse: to reveal sensitive activities online, to blacklist alleged infringers, to embarrass people, to market to them, or even for criminal purposes. People ask why privacy advocates seem to be so obsessed or care so much about what might be a relatively minor provision, and I think it is in part because 512(h) is a very unusual authority and a dangerous precedent. Many provisions exist for government access to information, but always in the context of executive powers and almost in all cases with additional and constitutionally mandated privacy protections.

Private use of the courts exists, but it is always tethered closely to pending litigation and comes with the supervision of a judge able to assess facts and to balance interests. 512(h) stands alone.

Our final point, and I think what we are trying to say today, is that we think that—we propose in our testimony a package of suggested safeguards that will address many of the privacy concerns raised by 512(h) while supporting enforcement. Chief among those is that we support a notice requirement before subscriber identity is disclosed. Notice can give people a meaningful opportunity to quash a subpoena they think is wrongful. It can also have a major deterrent effect because subpoena applicants would know that their targets are actually going to hear of the requests that they make.

A notice requirement also, I should note, actually could help legitimate enforcement. An official notice to targets of investigations that their information was being subpoenaed we believe would be enough to stop a great deal of infringing behavior. We also list a whole set of other approaches—penalties for abuse that could give users redress if a subpoena is misused, clear limits on how information that is collected is going to be used. The least controversial of these is a simple report to Congress on the number of subpoenas requested, which would provide us with some sense of how often this process is being used and in what way. We have no idea right now how many of these subpoenas are being filed and in what way.

In summary, we think that there are relatively minor additional safeguards that do not fundamentally rework the provisions of the DMCA, but that could protect privacy while actually preserving legitimate enforcement. We note and agree that there are a lot of other privacy issues that are raised in the context of peer-to-peer file trading—the issue of privacy of sensitive files, as Senator Boxer has said; the issue of spyware in many applications. And while this hearing is focused on 512(h), which we think is also important, we stand ready to work with you on those issues.

Mr. Chairman, we commend you and members of the Committee for raising awareness of the very real privacy issues that are raised by 512(h) subpoenas. We look forward to working with you and this Committee and others in the community to craft a more balanced approach to this issue.

Thank you very much.

Senator BROWNBACK. Thank you, Mr. Davidson. Thank you for the constructive thoughts.

We will run the time clock at 5 minutes if you do not mind, because we have so many members here that are present and we do have another panel that is up. I think this has been an excellent discussion and an opening panel of thought.

Mr. Sherman, let me ask you just at the outset here. It seems as if everybody supports the intellectual property right that your industry has and that there is just not a question of that. People may vary on the degree of intensity that you think people really agree with this, but everybody supports that this is an intellectual property right, it must be protected.

The narrow focus that we have got on this hearing is on this particular subpoena issue and that is the thing that has really driven me the most on it. I wonder, if you went looking at this, if you just compare even really the PATRIOT Act, the USA PATRIOT Act,

and the ability of the Attorney General to get a subpoena versus your industry, the industry standards or the standards subjected to the industry are much lower than they are to the Attorney General.

The Attorney General, you must have an application made by a senior level FBI official. Under 512(h) it is available to anyone who claims an interest in the copyright. The Attorney General has to go through the courts. You can file this and a clerk does it.

Is there a way that your group could see fit to move those standards up slightly so that you could still get the subpoena, but it has an officer of the court that reviews it? And what would be so harmful to you doing that?

Mr. SHERMAN. You have to look at the information that is actually being sought when the Attorney General is asking for this information from a court versus the information to which we are entitled. We are entitled to merely the identity of the alleged infringer: name, address, telephone number, and e-mail, nothing else, nothing about what communications they have had, nothing about who they have been communicating with, nothing about their credit card information, their usage records, or any of that.

That information is available right now under Federal law under the Electronic Communications Privacy Act without any judicial supervision, just by someone in the government filing a form. It is also the same information that SBC and Yahoo routinely give to marketing partners under their privacy policy.

So all we get, the very limited information we get, is who it is who is engaged in the infringement.

Senator BROWNBACK. Mr. Barr, Mr. Ellis, is that correct?

Mr. BARR. That is totally disingenuous. They just do not get a name. They get the name associated with content, because that is where the IP address comes from. So it is the correlation of the name with activity on the Internet that is the privacy concern. That is what any individual can get under this process.

Someone appears on a website with the IP address, they can find out who that was, and that is the concern. That is the privacy concern.

Senator BROWNBACK. Mr. Sherman, a quick response. I have one more question.

Mr. SHERMAN. The reason that the information is available to be correlated is because it is on a publicly available network for anybody to see whatsoever. We are getting no more information than any other user of the Kazaa system could get. It is as if a street vendor who is selling counterfeit CDs was complaining that we knew he was selling counterfeit CDs because he was doing it on the street when we ask what his identity is.

Senator BROWNBACK. Mr. Davidson, very briefly.

Mr. DAVIDSON. Yes. I would just like to say, it is not just about what the recording industry is doing, unfortunately. It is what other people correlate with other kinds of content. I mean, the Titan Media example that was raised earlier in testimony is a great—maybe by you, Mr. Chairman—is a great example of how correlating identity with access to sensitive or very private information or private behavior online can be very troubling.

Senator BROWNBACK. That was going to be my next question. It is about the Titan Media example, which I presume we are going to see more of these. Either Mr. Rose or Mr. Sherman. Here is a group, hard-core pornographers, asking SBC for 59 Internet subscribers, and then Titan offers an amnesty: you can either buy our pornography and in exchange we will not identify you.

That seems to border, if not be, blackmail. I am concerned that we are going to see more examples of situations like that coming up with this type of process. Do you share that concern?

Mr. SHERMAN. This problem is not attributable to the procedures that we are talking about here. The fact is that under the John Doe process that Verizon and SBC are suggesting Titan Media would be able to get exactly the same kind of information, in fact a whole lot more, because under the DMCA information subpoena process you are limited to just name, address, and so on, whereas in a lawsuit you can get all those other records that we were talking about earlier. Even under the legislation you have introduced, Senator, Titan Media would be entitled to all of that information in the ordinary course of a lawsuit, and that request for information would not even be reviewed by a judge.

Senator BROWNBACK. Mr. Ellis, real quickly, is that accurate?

Mr. ELLIS. No, I do not agree at all. The real heart of the dispute as I understand it between the industry and at least our company goes to the way Mr. Sherman characterized the situation, "the alleged infringer." If we are dealing with somebody who has violated their copyright and they have the reason, the 59 for example in the case of the Titan, and they have reason to believe, then go file the lawsuit. And when you file the lawsuit, it is subject to all the standard protections that judicial review, substantive showings, and all of those protections.

What is at stake here is alleged infringers, the 59 people. If they had the evidence that they are all guilty, then go sue them. The issue is they are trying to use this as a fishing expedition. In this country there is a presumption of innocence until you have the evidence. That is the difference in the two views. We oppose simply fishing expeditions where you pay 25 bucks, make an assertion. They take the position they need that to go get the evidence. That is contrary to basic constitutional law: Get your evidence, go file your lawsuit; do not use the subpoena process to go get the evidence.

Mr. SHERMAN. May I please have the courtesy of a response?

Senator BROWNBACK. Fifteen seconds. My time is up, but please.

Mr. SHERMAN. We have the evidence. We go into court with the evidence. We do not issue a subpoena to get evidence. We just issue a subpoena to find out who the evidence is identifying. We have the evidence. In fact, the DMCA process requires the virtual prima facie case of copyright infringement in order for an information subpoena to issue.

Senator BROWNBACK. Mr. Sherman, it would seem to me then, why not go ahead and have a little higher level of review by an officer of the court? I would hope really, as we look down the road of this process, this is something that reasonable minds really could work out.

Senator Boxer.

Senator BOXER. Thank you.

I wanted to just put in the record an article by Lee Gomes, who does a column for the *Wall Street Journal,* and just read a little bit of it. It ran on Monday. So can I place that in the record in its entirety?

Senator BROWNBACK. Yes, without objection.

[The information referred to follows:]

5 of 5 DOCUMENTS

WALL STREET JOURNAL ABSTRACTS
WALL STREET JOURNAL

February 10, 2003, Monday

SECTION: Section B; Page 1, Column 1

LENGTH: 61 words

HEADLINE: HOLLYWOOD NEEDS A FAST-PACED SCRIPT FOR COPYRIGHT ISSUES

BYLINE: BY LEE GOMES

ABSTRACT:
Portala column reports that the entertainment industry's copyright worries are blocking hardware design innovation in the consumer electronics world; for example, Digital Video Interface technology, arguably the best way to connect a DVD player to a TV set, is being stifled because movie studios worry that DVI connections could make movies easier to copy (M)

LANGUAGE: ENGLISH

Senator BOXER. I will just read the important part that I think weighs on what we are doing today. He said that: "With these suits, the industry is inviting a backlash among users and in Congress." He says: "Maybe I am"—he says: "Maybe, but I am hugely sympathetic to the record industry in this fight, largely because of the way I answer one of the central questions in the online music debate." He says: "It is this: Are music downloaders basically honest people who are simply yearning to breathe free of the inconvenience and high prices forced on them by the tyrannical music industry, or are they just trying to get something for nothing? Are they freedom-fighters or thieves? Maybe I am projecting from my own circles, but I have always assumed the latter."

He says: "I certainly understand why someone would want to buy only a single hit song off a CD"—which is what Mr. Barr said—"but should that be elevated to a Jeffersonian right? I like only the middle part of an Oreo. Does that mean I can just steal them?"

"Many people argue the record industry needs to make music easier to buy, but what could be easier to buy than a CD? And while I may not like the price, that is also true for Sub-Zero refrigerators. And yes, by having to drive to the music store or wait for a FedEx delivery from Amazon you do not get your music right this very second. But society needs to be careful about making a social virtue of impatience or about insisting that an industry provide a product in a manner conducive to its theft."

The point here—and he goes on with some very interesting things that he says. I think every industry can be criticized. Look, that is a fact of life. So can yours, Mr. Barr. Do you not share private information with your affiliates?

Mr. BARR. Yes, we do. And that is customer information within our corporation. We do not give it to third parties. My point—my point was——

Senator BOXER. How many affiliates do you have, Mr. Barr? How many affiliates do you have?

Mr. BARR. Hundreds.

Senator BOXER. Exactly my point. That is why in California we have a law that would prohibit you from sharing private financial information.

So here is the deal here. I see just a little bit of hypocrisy.

Mr. BARR. This has nothing to do with hypocrisy.

Senator BOXER. Excuse me, sir. It is my time to speak.

Mr. BARR. I thought that was a question.

Senator BOXER. Mr. Ellis—no, I made an observation. You do not have to agree with it. That is fine. I have no problem with your not agreeing with me. We agree on a lot of things, but not on this issue.

I find this kind of holier-than-thou discussion from SBC and Verizon amazing, because they share so much information with their hundreds of affiliates and do not think two wits about it. And they admit that they go to court to protect their property rights. But yet they are coming up with this John Doe idea, which they know very well is going to make it exceedingly burdensome for copyright holders to make sure there is as little theft as possible.

These are real lives you are talking about. As I understand the law, and I just had my staff give it to me, you control the information, Mr. Barr, that you give to Mr. Sherman when he files these suits. It says "only sufficient to identify the alleged infringer." So you are the one that controls the information.

As far as the answer that you gave, it is what Mr. Sherman has to do and the industry has to do is figure out exactly how many, how many cases of theft there are. So yes, they are going to look at the theft. It seems to me you are trying to protect privacy of theft. That is what you are really about, and I think it is a problem.

Now, on your own site this is what you say: "Free sites: Likely to have pretty much everything"—I want to make sure this is—this is Verizon, OK. Quoting from your brochure, "Your Guide to Broadband Living," quote: "Subscription sites do offer MP3s, the format for music files, to download. However, the official sites typically do not offer all music that is selling exceedingly well in stores. By contrast, the free sites are likely to have pretty much everything, but you may be pelted with some unwanted ads."

Now, how is that getting the information to people that what they are doing is illegal? I mean, it seems to me you are promoting this illegal downloading.

Mr. BARR. Well, actually that is one edition ago, but if you go to the very first paragraph of that guide you will see that we tell people that it is illegal to infringe on people's copyrights and that, with

all the available sites now that are authorized to provide music, people should be able to get music with a free conscience.

Moreover, that sentence that you take out——

Senator BOXER. Is that what you say, you can "get music with a free conscience?" Or do you say "the free sites are likely to have pretty much everything, but you may be pelted with some unwanted ads?"

Mr. BARR. And that sentence, of course, you are taking—that is a paragraph that comes after the warning about infringement.

Senator BOXER. I would ask unanimous consent to put this all into the record because, frankly, the message I get is not the message you are saying.

Mr. BARR. There is nothing illegal about a free site. There are authorized free sites and unauthorized free sites. You are trying to put a gloss on that.

Senator BROWNBACK. That will be put into the record, and the Senator's time has expired.

Senator BOXER. I think this will answer our argument.

Senator BROWNBACK. Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you very much, Mr. Chairman.

As I think the witnesses know, I have spent a lot of time over the last couple of years trying to find some common ground in this area. I have introduced the Digital Right to Know legislation that essentially empowers the consumers to make choices here, because I think, A, piracy is wrong; and B, I do not want to freeze innovation.

I am going to spend my time just over the next few minutes again looking for ways in which I think we can get to the bigger picture. I mean, you are not going to hold back demand here. Consumers want music in this way. They find it convenient, they find it attractive, and my sense is they are willing to pay for it and will be supportive of legal strategies if efforts are made to make that possible.

So I begin if I might with you, Mr. Sherman. You all seem to almost be on the cusp of a litigation forever strategy, which I think is unfortunate. We have got 261 suits. I gather grandmothers are getting sued, 12-year-olds are getting sued. You all want to send a message against piracy, and I support the efforts to go after piracy.

But give us a sense of how long this is going to go on? I mean, are you going to file 5,000 suits or 10,000 suits? At what point is that going to give way to something that people like me, who think your industry has got a point and the technology side has got a point, are going to take over? I mean, Apple iTunes has got an idea. It may not be the way to go. I have got a proposal in terms of digital right to know. I mean, there are proposals, it seems to me, that could help to find the common ground.

But tell us, if you would, how long do you see this litigation derby going on? Is there something that you can offer in terms of what you really hope to get out of this?

Mr. SHERMAN. I will be happy to respond, but I am also going to ask Mr. Rose to respond——

Senator WYDEN. All right, good.

Mr. SHERMAN.—because you have to understand that the litigation is just one piece of a much larger series of concurrent strategies to force a paradigm shift in the way people get music. Right now people—up until recently, people did not even think twice about downloading music and did not even think about, let alone worry about, whether it was right or wrong, legal or illegal.

The result of these lawsuits, something we did not want to do and something we did not take lightly, has been to inform more people in the space of a week that this conduct is illegal than anything we have done, notwithstanding a multi-year education program featuring artists, songwriters, and the entire music community. So it is having an effect.

Orientation programs at colleges have changed as a result. Parents are discussing with their kids what they are doing on the Internet, which has the added value of not just talking about the illegal activities such as downloading music, but also what they are doing with respect to the security of the computer at home, the privacy of their hard drive, viruses being spread, as well as pornography and kiddy porn.

So this national debate that has been ignited I think has been beneficial to everybody with respect to the ethics and the legality of online behavior. But all this would be irrelevant if we were not offering legitimate alternatives that consumers prefer, and that is why I wanted Mr. Rose to refer to some of the things that we are doing.

Senator WYDEN. Because my time is short, all right, let us say it has been relevant up to this point. At what point—I really am curious, how many suits will be enough? I mean, how many kids and grandmothers and the like are going to be chased down before we get down to what I think are the kinds of approaches, both legislatively and technologically, that are going to bring people together? Will 5,000 suits send the message you want?

Mr. SHERMAN. I really cannot answer the question because this is an evolving target, in which we are trying to change people's mind set and encourage consumers to migrate to legitimate services where they can get exactly what they want, but legally.

How many suits has DirecTV had to file in order to discourage satellite theft? They are over 10,000 now. You do not read anything about it. Why is this somehow—why is music property less respected than signal theft?

If I can just pass this off.

Mr. ROSE. Thank you, Mr. Sherman.

We are working extraordinarily hard, by the way collaboratively, with most of the telecommunications, computer companies, software companies, and consumer electronics companies, to launch a number of legitimate services. And the notion that file-sharing is occurring among teenagers because the only product they can buy is a CD is absolutely no longer true. First, more than 40 percent of the downloading is done by people over 30. Second, for almost a year now every single radio release, meaning every single hit that EMI sells, has been available for purchase through the legiti-

mate download services the day it went to radio, on an unbundled basis, before it goes to retail.

Third, almost every CD that we have for sale is available on a legitimate basis on a track by track basis, and we are focusing now on legitimate downloads.

That is just one of probably 50 different products that we are working with the telecom companies and computer companies to provide.

Senator WYDEN. Mr. Chairman, if I could just get one other question, because I am not going to stay.

In my legislation, and I think it goes right to the heart again of my concern that the only thing that is getting attention is lawsuits rather than efforts to bring people together. I introduced the Digital Consumer Right to Know Act, and it grows out of the fact that not too long ago some CDs were released with a copy protection system that made it impossible to play the CD on a computer, and somebody went out and bought the CD with the specific intention of playing it on their personal computer, they sued.

I said, would it not make a lot more sense and an approach that would be fairer to all sides to just let people know up front what their rights are. I mean, something like that, while certainly not dealing comprehensively with the piracy issue, could be one significant step in solving this problem, empower consumers, be fair to your industry, be fair to technology as well.

I just wanted to wrap up, with the graciousness of the chairman, about whether or not you all would support as part of the solution a digital right to know that would empower the consumer when they walk into stores to actually know what their rights are as part of this effort to be fair to the responsible parties.

Mr. SHERMAN. Actually, I think your legislation has helped stimulate an inter-industry dialogue on voluntary labeling standards that all the digital media industries can embrace, that will give consumers the information that they need to know how their products will work. Everybody shares the view that consumers need to know what they are buying, what they can do with it, and it is a question of how to communicate that information in the best possible way. So we certainly agree with the objective.

Senator BROWNBACK. Thank you very much. I think that is a very constructive thought. I have put similar labeling provisions in the bill that I have put forward as well, and hopefully we can get to some agreements on a few items.

Senator Inouye.

STATEMENT OF HON. DANIEL K. INOUYE,
U.S. SENATOR FROM HAWAII

Senator INOUYE. I have been listening, Mr. Chairman, to the questions. Very interesting.

Two months ago I read an article in the *New Yorker* magazine, and it was such a profound statement I thought I would take it down: "Maybe it is because I am in college, that I have an 18-year-old sister and a 10-year-old brother, but let me tell you, nobody I know buys CDs any more. My sister, she just gets on her computer and knows only two things: file-sharing and instant messaging. She and her friends go online and one instant messages the other and

says, oh, there is this cool song I found, and they go and download it, play it, and instant message back about it. My brother has never seen a CD except for the ones my sister burns."

And this is a quote from a University of Virginia student.

Is this piracy that widespread, Mr. Sherman?

Mr. SHERMAN. Absolutely. In fact, it has really been the combination of downloading and burning that has had the most tremendous impact on sales. When you see those lines converging about the uptick in downloading and CD burner penetration and the number of blank CD disks sold and you start looking at the sales figures, they correlate rather precisely.

The impact is bad, it is worldwide, it is getting worse, and if something is not done about it the creative industries will not be able to sustain a future. This is not just music. This is movies next, and then software. The BSA just came out with a study yesterday showing student attitudes toward software copying and it became quite clear that, because of music downloading, they feel very little compunction about copying software programs as well.

So it holds a terrible future for what is now the copyright industry's contribution to the GNP, 5 percent of our GNP and our number one export, and it is all at risk.

Senator INOUYE. So it involves much more than just a few computer hacks?

Mr. SHERMAN. Absolutely.

Senator INOUYE. What you are trying to tell me is that it is part of our culture now?

Mr. SHERMAN. It has become a part of our culture. We need to begin to change that culture. This is not going to change overnight. This requires a multipronged effort. That is why we have embarked on education campaigns, technical measures, but most important of all, offering legitimate alternatives that will attract consumers back into the paying marketplace.

Senator INOUYE. I have no other questions.

Senator BROWNBACK. Thank you, Senator Inouye.

Senator Lautenberg.

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thanks, Mr. Chairman.

I have not devoted as much time as I would have liked to to a full comprehension, but the one thing—to start with first of all, I would like to put my opening statement in the record as if read.

Senator BROWNBACK. Without objection.

Senator LAUTENBERG. The one thing that I do start with is that we have to protect the process and the value of copyrights. If we understand that, there is an obligation in some way to pay for that creativity and the production of the material that people are so eager to get their hands on. That seems to be only, Mr. Chairman, in your remarks counterbalanced by the subpoena opportunity to find out who is doing what. I would imagine that there are ways to deal with this.

But just in getting some knowledge here, does a company, Mr. Barr, like Verizon advertise—I know that Senator Boxer talked about that briefly—advertise the fact that this is available? What

do you say in terms of offering your broadband services? Do you include music and video and so forth?

Mr. BARR. Yes, I think we do provide a guide, both a printed guide and an online guide. I think two or three editions ago Morpheus was listed as a site in one of the guides, and then we deleted it.

Senator BOXER. I have it here, 2002.

Mr. BARR. Well, it was produced in 2001. And it was deleted from the subsequent guides. Our guides indicate that infringing is wrong, that you do not have to do it. We have a financial interest in promoting MP3 in Rhapsody, which are authorized sites, and we are promoting them, advertising them. On the bottom of every page on our website, we state that unauthorized downloading of songs is illegal and we discourage it.

Senator LAUTENBERG. I wondered, each of you, is there a responsibility—and, Mr. Davidson, you can respond—to launch an educational campaign to inform their DSL customers about the illegality of trading or downloading copyrighted content over the Internet? After I hear Senator Inouye's report on the letter from the child that does not buy CD's any more, but the people who produce them still have the expense and still have the artists who create this hard at work trying to make the product. Go ahead, Mr. Davidson.

Mr. DAVIDSON. Maybe I can jump in by just saying first of all, yes, I think there actually, there should be more done along educational efforts, and I think that the enforcement efforts that are going on will be wasted unless we can figure out how to educate a new generation and also provide them with real alternatives, because there is clearly a giant demand for digital music and we have not yet figured out how to meet that demand.

I would just like to say, both to your question and to Senator Boxer's about the motive, underlying motivations here, I do not think it is fair to the consumer interests that are here also. We do not make any money from selling broadband. I do not think many of the privacy groups that signed onto briefs and have written in support of Verizon or SBC do, either. We think that, independent of that debate, which you can all have, there is also a real privacy concern here and one that we think can be addressed. I just did not want that to get overlooked.

Senator LAUTENBERG. Mr. Rose.

Mr. ROSE. Thank you, Senator. There is really an underlying economic issue here and it is important. We have gone from a world where the economics of the telecom industry and the economics of the content industries were relatively unlinked to a world where they have become increasingly linked.

The primary applications that people who sign up for broadband services are interested in, among others, are entertainment-driven services, and the free and easy accessibility of the peer-to-peer networks have been to a certain extent a driver of the adoption of those services, as well as the underlying traffic on the networks that they create drives real economics.

We are actively seeking collaborative ways to develop new and legitimate products and services with the telecom industries and with the computer industries. But it is absolutely true that our eco-

nomic interests in the short term are not aligned. In the long term, they have to be aligned. The telecom and computer industries desperately need a vital and robust set of content businesses to create the very content that people want to move over their networks and use their access devices for. But in the short term, we have been to a reasonable degree at loggerheads, and it is interesting to note that it is only these kinds of processes that have made the public statements and consumer information around the illegality of digital downloads move to the forefront of the Verizon and other telecom companies' communications.

Senator LAUTENBERG. The question I asked, is it realistic to educate, to try to educate people? The demand is so great, the volume of transactions so enormous, to think that this, all of the education in the world, can make a difference? I mean, is this young woman that Senator Inouye referred to, is she going to feel guilty about burning this music into a disk that she has at home now, the process is so available and so commonplace?

Mr. Rose?

Mr. ROSE. If all of the grocery stores in the world had no cashiers, no one would be interested in buying groceries. They would just go and take them.

We have to really do three things. One is make legitimate music no more than one click away, any music that you want, in whatever form that you want it, so that consumers have the ability to find the music that they love and buy it in convenient ways. We are working with the computer and telecom industries very hard to do that.

That alone will not be enough. Without enforcement and awareness, those three planks—*i.e.,* ongoing awareness campaigns in colleges and elsewhere, so that people understand that file-sharing and moving content around without payment is illegal, and the enforcement tools to identify people who infringe—without those three things, the world will not change. With all three of them, it will change dramatically.

Mr. SHERMAN. If I could just add one point, as somebody who was actively involved in changing the mindset about tobacco, I think you know that a battle can be won; it just may take some time.

Senator LAUTENBERG. There is more physical evidence, though, on tobacco than there are of the dangers of pirating a song that young people love.

Yes, Mr. Davidson.

Mr. DAVIDSON. May I just add?

Senator LAUTENBERG. May I ask for a minute more?

Senator BROWNBACK. Yes.

Mr. DAVIDSON. I just wanted to add a quick point, which was—thank you very much—which was that the old conventional wisdom was that you cannot compete with free downloading. I think that the new conventional wisdom—I think anybody who has used some of these fabulous new downloading products like the Apple iStore—and I am a music addict and I have become an iStore addict. Unfortunately, my wife has been lecturing me about this.

These are fabulous services. I think that they can compete with free. I think that they are fast, they are virus free, and they are

legal. There is a lot of experimentation going on. It is going a little bit slower than some of us would like, but it is happening. And I do believe that real alternatives, coupled with education and enforcement activity, can make a very big difference.

But if we do not have the legal alternatives, this becomes like Prohibition. You know, we are just suing lots of people and not giving them an outlet for what they really want to do.

Senator LAUTENBERG. It is a very simple route, obviously, Mr. Chairman. I leave it in your hands.

[Laughter.]

[The prepared statement of Senator Lautenberg follows:]

PREPARED STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Mr. Chairman:

This is a pretty timely hearing.

The media have characterized the ongoing dispute and litigation between the music recording industry and Internet Service Providers (ISPs) as "piracy versus privacy."

I think it's important to understand that *both sides,* in a sense, need to prevail. We need to stop digital piracy, but not at the expense of privacy. Conversely, we can't protect privacy at the expense of copyrighted material.

We all recognize that musicians and the recording industry are losing millions of dollars from copyrighted materials being downloaded and shared illegally.

If you want proof, just look at the fact that music CD sales have dropped 26 percent since 1999. Meanwhile, the number of blank, *recordable* CDs sold at retail increased by 40 percent last year alone.

Piracy is not only affecting the music industry. Two weeks before the big screen release of the summer blockbuster "The Hulk," bootleg copies of the film started showing up on file-sharing networks around the world.

It cost Universal Studios 150 million dollars to make "The Hulk," yet anyone with a high-speed Internet connection and a big enough hard drive could see it for free.

This problem for the movie industry will only get worse when technology freely allows consumers to trade or swap movies similar to the way they now trade music files.

The recording and movie industries have the right to protect their copyrights.

But I do have concerns about the subpoena process used to obtain the names of those who allegedly engage in significant copyright infringement.

Due process is important. And I believe a consumer's due process rights exist even before a lawsuit is actually filed in court.

The bottom line here is that the music and movie industries *and* Internet Services Providers will have to get creative and invest in encryption technology, consumer education, and new products that are priced appropriately. That kind of collaboration may be preferable to a "legislative fix" since technology is always faster than Congress!

I look forward to hearing from the witnesses on this important subject.

Thank you, Mr. Chairman.

Senator BROWNBACK. Well, we would get it done that way.

I cannot help but think, as Mr. Rose put it, that we have got industries represented here that are absolutely critical to the future of this country and global in their span, and that cannot people of good minds be able to resolve this, because both of you need each other and will into the future. So I am hopeful that we can.

We will continue this debate and this discussion, but I am hopeful we are going to be able to work it out and move forward in the interest of all as we protect the intellectual property rights and we also protect the privacy of the individual. It has been an excellent panel.

Senator BOXER. Mr. Chairman, I wonder if I could just have a chance at another round, because this is so critical to my state. I could make it 5 minutes if you allow.

Senator BROWNBACK. We are really tight. We have got the next panel, too, that is going to be up.

Senator BOXER. I will make it 4 minutes.

Senator BROWNBACK. How about two questions and we will do that. Can we do that?

Senator BOXER. Well, I will do it as fast as I can.

Senator BROWNBACK. Run it at 4 minutes here.

Senator BOXER. I will just make a closing statement on the panel and I will try to do it in a couple of minutes.

Some unanswered points here. I think the fact is that the Digital Millennium Copyright Act did try to do exactly what we are talking about today, find a balance. And guess what, it was not easy. Why we would want to open it up is beyond me.

My Chairman feels he needs the courts more involved. The courts are involved. You have got to prove before you can go forward that you have got a case to make that there was good reason to believe there was copyright infringement.

I know that the Internet service providers were involved in this compromise. You wanted to be off the hook. You did not want to be liable for stealing. You did not want to be liable for the porn that is coming up on these sites. You did not want to be liable. You wanted to wash your hands of it and you got your wish, and now you are not cooperating with the industry. And that was written into the law, that your safe harbor was based upon the fact that you would cooperate with the industry.

So I am rather sad that we have come to this circumstance, because I think we listened to you, we gave you the safe harbor. And I do agree with Mr. Sherman. You know, all of us who have raised kids, we know something about how you change behavior. It is not easy and maybe sometimes we never do. But if we keep saying, if you do this you are going to be grounded; oh, you did it, okay; the next time you do this, you do it, you are going to be grounded, and you keep threatening, it never changes the behavior.

You have got to carry out. You have to have the enforcement. And if you start going this John Doe route, it is going to be a legal nightmare.

I honestly do think, with the combination of the new technologies like the iTunes and making that more available, and with the cooperation of the ISPs on this, not saying, oh, you can go to a free provider but you may get annoyed by popups. Wrong. You may get annoyed by a lawsuit.

We have to all work together. I am really sad that you are just not working together. So my message to you is, as Senator Brownback has said, both of these industries are crucial to the future of our country. Our country has got so many problems. Do we really need this one? Can you please figure it out?

You are all business people. You all know that you need to protect your intellectual property. So why do you not get together, shake hands, and work together, and then we will not need to open up this whole law, because I am not for that. I just think that is a nightmare.

So thank you very much, Mr. Chairman, for giving me the chance to speak about something that is so crucial to the jobs in my state and to the economy of my state. Thank you.

Senator BROWNBACK. Thank you, Senator Boxer.

I want to thank the panel very much. It has been quite illuminating and hopefully we can move forward on this.

Our second panel is: Mr. Lawrence Blanford, President and Chief Executive Officer of the Philips Consumer Electronics Company; Mr. Jack Valenti, Chairman and Chief Executive Officer of the Motion Picture Association of America; Mr. Christopher Murray, Legislative Counsel for the Consumers Union; and Dr. Edward W. Felten, Professor of Computer Science at Princeton University.

We will get that panel in place as soon as possible. Let us get seated as quickly as we can with the panelists in the room in order so we can move forward. The hour is late. We have gone a long period of time.

We start this second portion with—I want to enter into the record a letter sent to the Chairman of this Committee, Chairman McCain, dated September 4, 2003. It is sent by two pages, two and a half pages, of groups that have problems with the subpoena process that has developed by virtue of the RIAA versus Verizon lawsuit. I want to note that to the people present and the members, that it contains an eclectic group of individuals, consumer activists, privacy concerns. A women's shelter group, I believe, as well is in this because they are concerned about these identity issues coming forward. Hopefully this is something that we can get dealt with.

This is the second issue, no longer on the subpoena, but this is about really issues of built-in hardware to protect intellectual property rights, and the industries' interaction, difficulty of interacting back and forth on the protection of intellectual property right, but at the same time building hardware that will work and hardware that will work for the consumer. So I am glad to have this panel to develop and to go into this topic in some depth.

We will start with Mr. Lawrence Blanford. He is President and CEO of Philips Consumer Electronics. Mr. Blanford.

STATEMENT OF LAWRENCE J. BLANFORD, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PHILIPS CONSUMER ELECTRONICS NORTH AMERICA

Mr. BLANFORD. Thank you, Mr. Chairman, and thank you, Members of the Committee. I am President and Chief Executive Officer of Philips Consumer Electronics in North America. Philips is a leader in digital television and digital content protection technologies. Philips commends the Committee for holding such a timely and important hearing and you, Senator Brownback and Senator Wyden, for your leadership in this area.

Mr. Chairman, let me be clear. Philips is 100 percent committed to working collaboratively with the studios to develop consumer-respectful solutions that safeguard against what my fellow witness Jack Valenti fears will be the Napsterization of video. That said, what are the essential elements of a digital broadcast content production system around which we in the industry and public policymakers can coalesce?

First, it must work. A solution that does not provide effective protection in our view is not a good solution.

Second, it must respect consumers' fair use expectations, enable consumers to benefit from the incredible openness and flexibility of digital technology and the Internet, and not be so costly and complex that it will slow rather than accelerate consumer acceptance of digital television.

Third, it must not constrain competition or impede innovation. A solution that enshrines by government regulation a particular digital protection technology is usually a bad idea. If that government mandate also carries with it a set of obligatory licensing terms that makes licensors gatekeepers, yet does not contain strong and enforceable safeguards against anti-competitive practices, the resulting solution goes from bad to intolerable.

With these principles in mind, the question then becomes what is the role of government? To begin, in our view Congress should be the first to act to decide the extremely important public policy issues raised in this debate and provide clear guidance to the FCC about how to implement those goals. Among the issues on which Congress should provide guidance are the following: A, should we even be contemplating the encryption of programming that always has been available in the clear the consumers over airwaves they own? And B, where do we strike the right constitutional balance between the property rights of copyright holders and the First Amendment rights of the public to access and use information?

Second, the government should not pick technology winners and losers. Where there is an absolutely unavoidable need for a technology mandate, it should be done with only great care and with explicit Congressional guidance.

Third, if the FCC after receiving a clear grant of statutory authority and appropriate Congressional guidance mandates a digital broadcast content protection regime, it must maintain an ongoing oversight role to safeguard the opportunity for fair, open and unbiased adoption of alternative digital content protection technologies and to ensure that any associated licensing terms and conditions do not interfere with the public's legitimate use of content or harm competition.

Unfortunately, the encryption technology mandate proposal advocated by the Motion Picture Association of America and the 5C companies in the pending FCC broadcast flag proceeding violates every one of the principles I have just articulated. For starters, it does not work. The proposal leaves wide open the so-called analog hole. MPAA itself acknowledges this flaw in its public filings. In the just completed plug-and-play proceeding, MPAA stated:

> "Systems that permit the continued availability of unprotected analog connections fail to achieve meaningful protection of digital content. This is because it is essentially as easy to convert analog to digital for Internet retransmission as it is to retransmit digital content in its native format."

The proposal also fails to address circumvention by software demodulators, basically TV tuners you can download from the Internet. In fact, the proposed solution leaks like a sieve, and yet

its implementation would require consumers to replace and the FCC to regulate virtually every single device in the home network.

Let me just point to the chart to my right. Basically, what would happen is that we would end up erecting enormous cost and complexity barriers to consumers realizing the same hard-fought fair use recording capabilities in the digital realm as they do in today's analog environment. What you can see by looking at the chart, the typical consumer devices down the left-hand side and the points of functionality across the top over which the proposal in front of the FCC would impact.

So you can see that indeed the proposal is not innocuous. It is exceedingly pervasive relative to consumer electronics that consumers enjoy today.

Senators of the Committee, were this proposal adopted by the FCC your staff, say in your State office, would be prevented from e-mailing to you in Washington a digital broadcast clip about a breaking news story back at home. Nor could a loving child e-mail to an ailing parent a digital broadcast clip containing news of a revolutionary treatment for the disease afflicting the parent.

Finally, the encryption technology mandate proposal would provide a small group of companies, through their control of authorized technologies that are mandated by the government, with the incentive and opportunity to constrain competition in digital content protection technology and digital consumer electronics products. Imagine the uproar in Congress if the Department of Transportation were to mandate that General Motors had to seek prior approval from a committee consisting of Toyota, Nissan, Mitsubishi, and Ford before it could implement a new braking system. That is precisely the situation created by the encryption technology mandate proposal.

Along with its specific deficiencies, the proposal suffers from a classic case of mission creep. What began 2 years ago as an attempt to prevent the unauthorized redistribution of pristine high-definition TV programming over the Internet to the public today encompasses all digital video programming, standard as well as high-definition, broadcast as well as cable and DVD, and extends to all unauthorized redistribution, not just to the public and not just over the Internet.

Senator BROWNBACK. Mr. Blanford, let us wrap your statement up if you could.

Mr. BLANFORD. Yes, I will. Thank you, Senator.

In fact, your bill, the Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, cures many of these problems and we commend you on its introduction.

Mr. Chairman, last, there is no imminent crisis. Given the technical limitations on bandwidth compression, we have time to develop and implement more effective pro-consumer alternatives that avoid anti-competitive and anti-innovation consequences. In my written testimony I discuss Philips' hope for watermarking and its commitment to work with the studios on that system. Let us take the time to work together as never before to develop digital broadcast content protection technology solutions that will take us forward, not backward.

Philips will be the first in line in such collaborative behavior.

Thank you, Senator.
[The prepared statement of Mr. Blanford follows:]

PREPARED STATEMENT OF LAWRENCE J. BLANFORD, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PHILIPS CONSUMER ELECTRONICS NORTH AMERICA

Executive Summary

Philips has been a leader in digital television, one of a handful of companies that developed the digital terrestrial broadcast transmission standard adopted by the FCC, and a pioneer in digital content protection technologies for audio and video.

Philips is deeply appreciative of the efforts of this Committee, other Committees of the Congress and the Federal Communications Commission to illuminate the key public policy issues raised by digital rights management, particularly the "broadcast flag" in open, fair public proceedings, removing decisionmaking from back rooms occupied exclusively by private parties with huge financial stakes in the outcome.

Philips is 100 percent committed to working with all stakeholders—the studios, computer hardware and software companies, other consumer electronics manufacturers and, most importantly, consumers—to develop and implement technology solutions that protect high definition and other high value digital broadcast content from unauthorized redistribution to the public over the Internet.

There are three essential elements of a digital broadcast content protection system necessary for a consensus solution. First, it must be effective to prevent the abuse it is designed to stop. Second, it must respect consumers' fair use expectations and their aspirations to utilize digital technology to provide advances in their ability to store, record and make innovative use of digital broadcast content. Third, it must not constrain competition or impede innovation.

What is the appropriate role of government, especially the Congress and the FCC, in digital broadcast content protection?

First, the Congress should decide overarching public policy issues: What is the impact of encrypting free over-the-air digital broadcasts, whether at the source or at the instant of reception, on the historic model of broadcasting which has been "in-the-clear" over public airwaves? How do we balance the competing, constitutionally rooted rights of copyright holders and consumers? If necessary, Congress should confer a specific grant of authority on the FCC and guidance on how to regulate.

Second, the government, whether the Congress or the FCC, should not pick technology winners and losers. Such government technology-specific mandates are hostile to competition and innovation.

Third, the government must be the guarantor of a fair, open and transparent decisionmaking process and must maintain an ongoing oversight role, through enforceable safeguards, to prevent anticompetitive and anti-innovation practices or efforts, either in the approval of technologies or the terms with which licensees are obligated to comply.

Applying these tests to the Encryption Technology Mandate advocated by the MPAA and broadcasters in the pending FCC "Broadcast Flag" proceeding, the proposal fails on every count. It is not effective because it leaves the analog hole wide open and also can be subverted by software demodulators. It levies significantly increased complexity and hundreds of dollars in new equipment purchase costs on consumers to realize the same fair use recording capabilities that they enjoy today while precluding them from being able to send a digital broadcast clip in an e-mail to themselves at their office, to a professor as part of a student presentation, or to a parent or child.

It is a hybrid proposal which at once asks the FCC to mandate, as part of a 20-page government regulation, specified digital content protection technologies, but at the same time effectively delegates the approval of alternative technologies to private parties and direct competitors, acting as gatekeeper with zero safeguards to prevent anticompetitive practices.

There is another far better way, suggested by Senator Brownback's "Consumer, Schools and Libraries Digital Rights Management Awareness Act of 2003." That bill's prohibition on specific technology mandates and its reliance on functional regulation and self-certification would enable competitive and innovative digital content protection technologies to flourish, fulfill the legislative objective of content providers to prevent the unauthorized redistribution of high definition and other high value digital broadcast content over the Internet to the public, and give consumers a choice.

Philips reiterates its commitment to work shoulder to shoulder with the content community on digital broadcast content solutions that meet the criteria I have outlined here. In particular, my written testimony discusses the promise of

watermarking, which many studios embrace, and on which Philips already has made substantial progress. In light of the technical limitations on compression and bandwidth, there is time to do this right!

Introduction

Mr. Chairman, Senator Hollings and Members of the Committee, my name is Larry Blanford and I am President and Chief Executive Officer of Philips Consumer Electronics North America, a division of Philips Electronics North America Corporation, which is the U.S. subsidiary of Royal Philips Electronics of The Netherlands. In the United States, Philips employs approximately 35,000 dedicated workers and sells over $10 billion of goods and services in the areas of consumer electronics, lighting, medical systems and devices, semiconductors, personal care products and domestic appliances.

Philips commends the Committee for holding this extremely timely hearing, as the Federal Communications Commission nears a decision in its "Broadcast Flag" proceeding. Both this Committee, the House Energy and Commerce Committee, through its hearings, roundtable discussions and its carefully crafted September, 2002 staff discussion draft, and the Senate and House Judiciary Committees, have played absolutely crucial roles in ventilating important public policy issues in the digital rights management area, especially concerning the broadcast flag. Congressional oversight has illuminated issues that must be discussed openly and not decided in back rooms by private parties with enormous financial stakes in the outcome.

Similarly, Philips commends the FCC for its fair and open conduct of the broadcast flag proceeding. The Notice of Proposed Rulemaking issued by the FCC in the Broadcast Flag proceeding reads more like a Notice of Inquiry, putting out for public comment virtually all of the fundamental issues associated with protection of digital broadcast content from unauthorized redistribution, including whether the FCC has jurisdiction to regulate in this area.

The efforts of the Congress and the FCC to date have gone a long way toward easing the profound procedural concerns Philips had about the work of the inter industry group known as the Broadcast Protection Discussion Group (BPDG). This hearing and the current intensive phase of FCC deliberations in the Broadcast Flag proceeding now bring us face to face with the serious substantive public policy issues raised by the Broadcast Flag proceeding, which will consume much of my testimony.

Philips Is a Leader in Both DTV and Content Protection Technologies

Philips has a very proud history—and today is at the cutting edge—of introducing world-class products designed to bring consumers the benefits of the latest digital technologies for television and television displays (including the widescreen television format and flat TV). It is a leader in video compression, storage and optical products, as well as in semiconductor technology.

Philips co-invented the Compact Disk, or "CD," the most widely implemented digital technology. Philips is among the leading suppliers of DVD players and DVD recorders, and is a leader in the PC monitor and recordable CD markets.

Philips was a founding member of the Grand Alliance, which pioneered the ATSC DTV standard, adopted by the FCC in 1996 as the digital terrestri.al television standard in the United States, and has been a leader in the development and implementation of terrestrial digital television in the United States.

Philips also has been an active participant in the development of content protection technologies. Philips invented, and offered to the consumer electronics industry, at no cost, the Serial Copy Management System, or SCMS, a "bit flag" technology which, by providing the necessary instruction to the recording device as to whether and to what extent copying is or is not allowed, prevents the unauthorized reproduction of multiple generations of copies of digital audio works from a copyright-protected original (while permitting a single generation of copies). Philips also is actively developing watermarking and fingerprinting technology to protect digital video and audio content.

Philips is committed to seeking content protection solutions that strike the proper balance among consumers, content owners and equipment manufacturers. For years, Philips has been a constructive participant in inter-industry content protection activities, and has dedicated millions of dollars and thousands of hours of effort from its best engineers to groups such as the Copy Protection Technical Working Group (CPTWG) and the Secure Digital Music Initiative (SDMI). Most recently and relevantly, Philips has participated heavily in two inter-industry discussion groups, comprising consumer electronics companies, broadcasters, content owners, IT companies and others, tasked with finding solutions for the protection of over-the-air

digital broadcast content. The Broadcast Protection Discussion Group (BPDG), which was unable to reach consensus on a solution, nonetheless, over vigorous opposition, hurriedly released a Co-Chair's report discussing a proposal advocated by the major Hollywood studios, the so-called "5C" companies—Sony, Toshiba, Matsushita Hitachi and Intel—and the so-called "4C" companies—Toshiba, Matsushita Intel and IBM—which would require all devices to recognize a data bit in the digital television signal—the "broadcast flag"—and respond by encrypting that signal using only "authorized technologies." The only "authorized technologies" were proprietary technologies licensed by authorities consisting of the 5C and 4C companies. That proposal, in essence, is the Encryption Technology Mandate Proposal supported by MPAA in the pending FCC Broadcast Flag proceeding. Today, Philips is a leading participant in another effort—the Analog Reconversion Discussion Group (ARDG)—which is addressing the question of how to protect digital content when it is passed through an analog output (an issue more commonly referred to as "the analog hole")—an essential component of any system that purports to provide meaningful protection for digital content.

Philips' strong record of achievement in technological innovation—and consumer acceptance of these technologies—is directly attributable to the availability and use of open standards, a commitment to preserving consumers' fair use expectations, and a competitive environment that promotes the development and introduction of innovations in technology and products while not overburdening manufacturers.

Digital Broadcast Content Protection: We Must Work Together

This debate is about how best to achieve the twin goals of providing appropriate protection for high definition and other high value over-the-air digital broadcast television content against unauthorized redistribution to the public over the Internet and ensuring that the digital television experience that consumers receive meets or exceeds their fair use and technological expectations.

Philips believes firmly that these need not—and must not—be rival objectives, for each addresses a legitimate concern with long-term implications for the future of digital entertainment and innovation and acceptance by consumers.

Just as with digital music, over-the-air digital television raises understandable concerns for content owners about the potential vulnerability of their content to large scale unauthorized redistribution to the public over the Internet. Philips is supportive of content owners when they seek solutions that provide meaningful and effective protection for their content to ensure its continued value.

At the same time, consumers have been promised revolutionary enhancements to their television experience. In addition to prettier, better, high-resolution pictures and better sound, that means more flexibility, more functionality and more interactivity. At a bare minimum, it also means no loss of functionality from what they experience today, including with regard to recording and time-shifting of free over-the-air television. These promises simply must be kept if consumers are to embrace DTV. Indeed, the legitimate utilization of broadcast content (at a time and place of their own choosing) by consumers should be enhanced by the introduction of digital television.

All of the affected industries-studios, broadcasters, and consumer electronics manufacturers-must work with each other and, most importantly, with consumers, to strike the delicate balance needed to achieve both critical objectives. Such cooperation and dialogue should be characterized by open processes and be framed by a commitment to competition, innovation and the constitutionally-rooted rights of both copyright holders and the viewing public. Philips reaffirms its unwavering dedication to developing collaboratively digital content protection solutions. Unless all stakeholders commit to that course, we risk, at best, a legal and political quagmire, and, at worst, consumer rejection of DTV. Neither is a risk we can afford to take if we are serious, as we must be, about moving the transition to DTV toward an expeditious and successful conclusion.

The Role of Government

Clearly, the issue of digital broadcast content protection raises fundamental questions of public policy—with far-reaching effects on consumers. Should we be encrypting free, over-the-air broadcast programming, whether at the source or the instant a consumer receives it, because it is now transmitted digitally? If so, how does that affect the fundamental broadcasting model in the United States? Will the technology choices preserve consumer fair use rights and enable consumers to exploit the enormous flexibility of digital technology and the openness of the Internet while effectively protecting copyright holders' property interests? Are there safeguards in place to prevent practices, through technology selection or licensing terms, that restrain competition and inhibit innovation?

Government has an essential role to play in answering these overarching public policy questions and in ensuring that the public interest will not become captive of private, parochial interests seeking competitive advantage for their business models or technologies in the marketplace. Specifically, if over-the-air television content is going to be protected in light of digital technology, Congress should be the first to act. This is the only way to ensure that digital content protection measures, whatever they may be, reflect and adhere to the broad policy parameters Congress deems necessary to protect the interests of consumers, content owners, competition and innovation.

Moreover, Philips believes that the Communications Act confers no authority upon the FCC to regulate in this area absent an unambiguous grant of statutory authority by Congress, similar to that which enabled the Commission to adopt requirements for the V-Chip, closed captioning, competitive availability of navigation devices and cable compatibility. In fact, FCC adoption of the Encryption Technology Mandate Proposal currently before it—which would require the issuance of 20 pages of regulations dictating the design and manufacture of virtually every consumer electronics device in the home and mandating the use of "authorized" encryption and decryption technologies—would run directly contrary to Congress's recent policy decision, in Section 1201(c)(3) of the Digital Millennium Copyright Act, *not to require* consumer electronics or computer products to respond to particular technological measures. In fact, this provision—which explicitly required the use only of one, analog technology—Macrovision—was a core compromise that permitted passage of that legislation, and represents a clear policy direction adopted by Congress. Any determination to undo that compromise and change the policy direction adopted by Congress in that Act must necessarily be made by Congress, not the FCC.

The Brownback Bill

Senator Brownback's legislation clearly recognizes the importance of having Congress, not the FCC, take the first step toward, and lay out the appropriate ground rules for, digital broadcast content protection. Philips strongly supports Senator Brownback's efforts and leadership in this area, and commends him and his staff for the legislation that we are focusing upon today.

Senator Brownback "gets it right." By that I mean that he clearly recognizes that protecting digital content and protecting consumers' fair use expectations necessarily must go hand-in-hand, and that digital content protection solutions must be developed in fair and open processes, address narrowly-defined goals, and above all, not impede or diminish consumers' fair use expectations, especially in the DTV arena. These are not, from a public policy perspective, mutually exclusive. In fact, they are and must be complementary.

Importantly, the approach taken by the Brownback bill focuses on functional regulation. It relies on self-certification rather than government selection of technology "winners and losers"—a critical element to protecting, indeed driving, robust competition and innovation in digital broadcast television content protection software and hardware markets. In so doing, it respects the policy determination made by Congress in Section 1201(c)(3) of the DMCA. In this regard, it contains common elements with the House Energy and Commerce Committee's September 2002 staff discussion draft which envisions pro-competition and pro-innovation safeguards regarding the broadcast flag and expressly commends self-certification.

By contrast, proposals that would have the government put its imprimatur on specific technologies would have precisely the opposite effect, harming competition and innovation, upending the compromise struck in the DMCA, and threatening consumer acceptance of DTV.

The "Consumers, Schools and Libraries Digital Rights Management Awareness Act of 2003" is worthy of the Committee's support and Philips hopes that the Committee will act quickly toward its enactment.

The Encryption Technology Mandate Proposal Advocated by MPAA In the FCC's Broadcast Flag Proceeding Fails Every Test

Unfortunately, the Encryption Technology Mandate Proposal made by the Motion Picture Association of America to the FCC is neither an effective content protection solution, nor does it enable digital television to meet consumers' expectations.

The Encryption Technology Mandate Proposal Erects Unacceptable Cost and Complexity Barriers to Consumer "Fair Use." Proponents of the Encryption Technology Mandate Proposal claim that its approach preserves consumers' fair use recording capability for over-the-air broadcast content. However, this claim conveniently omits the fact that, under the proposed system, in order for a consumer to replicate today's "freely copiable" over-the-air television environment—wherein multiple devices within a consumer's home network seamlessly receive and send content to and from

each other for recording and/or display—consumers first must replace virtually every existing digital device in their home with those that contain the same "authorized" encryption/decryption technology. That is simply the nature of encryption systems: they rely on an "unbroken chain" of devices that all exchange content using the same encryption and decryption technologies. And, as illustrated by the chart below, virtually every single device within the home would be regulated under the Encryption Technology Mandate Proposal:

FCC-REGULATED DEVICES UNDER THE ENCRYPTION TECHNOLOGY MANDATE PROPOSAL

DEVICE	DEMODULATOR	MODULATOR*	DOWNSTREAM PRODUCT**
INTEGRATED DTV SETS	✓		✓
DTV MONITORS			✓
CABLE SET-TOP BOXES	✓	✓	
DBS RECEIVERS	✓	✓	
PERSONAL VIDEO RECORDERS (*E.G.*, TIVO, REPLAY)	✓	✓	✓
ADVANCED PVRS (INCORPORATING TWIN-TUNING, VIDEO EDITING AND OTHER CAPABILITIES)	✓	✓	✓
DVD PLAYERS		✓	✓
DVD RECORDERS	✓	✓	✓
D-VHS RECORDERS	✓	✓	✓
COMPUTER WITH DTV TUNER CARD	✓	✓	✓
COMPUTER WITHOUT DTV TUNER CARD			✓
NETWORK ROUTERS/SWITCHES			✓

* DEVICES IDENTIFIED ✓ IN THIS CATEGORY COULD INCLUDE MODULATORS AND THEREFORE BE SUBJECT TO FCC REGULATION.

** DEVICES IDENTIFIED ✓ IN THIS CATEGORY COULD BE USED AS A "DOWNSTREAM PRODUCT" WITHIN A CONSUMER'S HOME NETWORK. FOR THE CONSUMER TO UTILIZE THE DEVICE ON THAT NETWORK AND BE ABLE TO ACCESS FLAGGED DIGITAL BROADCAST CONTENT, HOWEVER (*I.E.*, AS OPPOSED TO ITS BEING A "STAND-ALONE" DEVICE), THE DEVICE WOULD BE REQUIRED TO UTILIZE FCC-"AUTHORIZED TECHNOLOGIES," OR COMPLY WITH THE MPAA/5C'S FCC-ADOPTED "REQUIREMENTS."

Moreover, the Encryption Technology Mandate Proposal would stifle use of the Internet for the wholly lawful and desirable purpose of transmitting free, over-the-air digital content from a consumer's home to an office, second home, automobile, or other remote location. These transmissions pose no threat at all to content owners' syndication markets and foreign broadcast rights—the problem they repeatedly claim to be addressing. In fact, it's very possible that permitting such non-public, directed transmissions could benefit broadcasters and content owners by increasing viewership of DTV programming and its associated advertisements.

The MPAA Encryption Technology Mandate Proposal places fundamental public policy decisions in the hands of a self-selected group of private interests. Under the MPAA Proposal, each device that handles broadcast DTV content over a digital

interface or from a digital recording would be subject to a regulatory regime triggered by the mandatory use of "authorized technologies." These "authorized technologies" would be subject to private control, such that the major Hollywood studios would have "veto power" over their selection, and thus their success in the marketplace. Specifically, to become an "authorized technology," the technology would have to meet one of four criteria for approval:

- *Criterion 1:* approved by three major studios or two major studios and a major television broadcast group;
- *Criterion 2:* licensed by ten major device manufacturers and approved or used by two major studios;
- *Criterion 3:* at least as effective as a technology already approved, subject to objection by major studios and/or major television broadcast groups; or,
- *Criterion 4:* listed as permitted under a license applicable to an already approved technology.

These criteria, which proponents claim to be market-based, are in fact neither market-based nor objective, and will harm competition in both the. markets for digital content protection technologies and consumer electronics products.

The first two criteria require at least two of the major motion picture studios to grant approval. Criterion 1 also requires an additional major studio or major television broadcast group to approve, but since three of the four major broadcast networks are owned by major studios, and the remaining "broadcast groups" are dependent on studios for programming, this criterion is essentially a studio designation mechanism. Criterion 2 at least affords device manufacturers a role, but requires licensing by ten major device manufacturers before a technology will be accepted, and still necessitates approval by two major studios, highlighting studio dominance of the selection process. Criterion 3 would appear to allow a role for the FCC in the addition of alternative technologies, but that role is very tightly circumscribed, with deference to the views of studios and broadcast groups, and relies on vague criteria the baseline for which is established by the pre-approved 5C and 4C technologies and license terms. Moreover, the technologies that MPAA and 5C argue should be exempt from analysis are proprietary, making it difficult, if not impossible, for a developer of new technologies to learn the standards against which it will be judged. Criterion 4 explicitly turns licensors of previously approved technologies into gatekeepers, and allows them to leverage their control over those technologies to new technologies. It is perhaps the most dangerous of the criteria from a public policy point of view, paving the way for leveraging market power into adjacent markets and technologies.

Thus, the criteria for selection of authorized technologies are not market-based—they are studio-based.

In addition, under the Encryption Technology Mandate Proposal, device functionality is dictated by compliance rules set by the approved technologies. Those rules permeate to every device in the chain other than the receiving device. The power to establish and change compliance rules (in ways that differ from those set by the FCC) is a key place where the Proposal would place the power over fundamental public policy decisions in private hands. Rules to which devices must conform should be set by those who answer to the public, not by private groups of self-interested parties.

In fact, we have already seen significant changes to the rules, and others are being "negotiated" even as we speak. The private control that these select parties can exert does not promote consumers' ability to utilize and enjoy DTV, nor does it promote a competitive and innovative marketplace. It does just the opposite.

The Encryption Technology Mandate Proposal contains no safeguards to prevent anticompetitive abuses by technology licensors. In fact, under this scheme, content owners and digital content protection technology licensors (the 5C and 4C companies) would have both the incentive and ability to abuse their control of so-called "authorized technologies" and the licenses that accompany them to the competitive disadvantage of their direct competitors. Unlike the far-preferable "functional regulation" and self certification approach taken in the Brownback bill, the Encryption Technology Mandate Proposal's "pre-anointment" of the 5C and 4C content protection technologies sets a very dangerous precedent for government selection of technology winners and losers.

Let's look at one recent instance. Just as an open inter-industry group—the Analog Reconversion Discussion Group, or ARDG—is addressing technical solutions to the so-called "analog hole" issue, the 4C companies (three of which also are part of 5C), have made sweeping changes in the compliance rules applicable to one of the "authorized technologies"—CPRM. These changes obligate consumer electronics de-

vices licensed to make recordings using CPRM to search all analog content reaching the device for rights information transmitted using a marking technology called CGMS-–A. No similar obligation is imposed on computers or devices used with computers.

These changes to the CPRM compliance rules provide a stark demonstration of the concerns identified by Philips and confirm that the Encryption Technology Mandate Proposal would grant the providers of a government-anointed technology:

- The right and ability to change the relevant rules unilaterally, without advance notice, public scrutiny, FCC scrutiny, or even licensee input or consultation;
- The ability to preempt public discussion of basic public policy issues (in this case, the analog hole), despite the ongoing consideration of the issue by the FCC and a multi-industry working group;
- The ability to distort competition in technology markets, by tying their selected technology to inferior or ineffective technologies at the expense of superior technologies (such as watermarking), in which others own relevant IP;
- The ability to distort competition in product markets by adopting changes in the rules governing their selected technology that further their own competitive interests;
- The ability to discriminate without justification between consumer electronics products and computer-related products;
- The ability to attempt to extend the power of their license agreements into functions of a device that do not in any way make use of the licensed technology, in a manner contrary to basic principles of IP licensing.

What is particularly perplexing is the fact that many in the industry, including content companies, have observed that CGMS–A is easily strippep or forged, thereby depriving the content of any protection. This is precisely the kind of behavior that threatens to deprive technology innovators, device manufacturers and consumers of the benefits of robust competition and innovation in digital content protection technologies and equipment.

The Encryption Technology Mandate Proposal Fails to Provide Meaningful Protection Against The Very Threat It Seeks to Address. At the outset, there is a very real question about the nature of the threat the content community seeks to address. Early in the debate, nearly two years ago, the objective of the studios and the major broadcast networks owned by studios was clear: prevent the unauthorized retransmission of high definition and other high value digital broadcast content over the Internet to the public because failure to do so would result in HDTV and the highest value digital programming migrating from free, over-the-air broadcast television to pay services, namely cable and direct broadcast satellite. The Encryption Technology Mandate Proposal pending before the FCC, however, is much broader. It applies to all digital broadcast transmissions, standard as well as high definition, and it applies to all unauthorized redistribution, with no limitation to the Internet and no limitation to the public at large. This "mission creep" of the Encryption Technology Mandate Proposal raises the fundamental question of whether this proposal is aimed at saving broadcast television or securing control over consumer electronic devices and how consumers use them.

Even if one accepts the greatly increased scope of the proposed regulations as legitimate, most incredibly, the proposed system *just doesn't work.* In fact, it leaks digital content like a sieve—leading many to point out that the proposed system, while locking the front door, leaves the rear door—and perhaps a few windows—wide open. This is due, most notably, to its failure to protect digital content that has been passed through analog outputs, which can easily be redigitized, stripped of its protection, and sent off to the Internet.

This is not an oversight on MPAA's part, but rather reflects a recognition of the fact that restrictions on analog outputs would doom the DTV transition to certain failure by causing the obsolescence of hundreds of millions of legacy devices. Nevertheless, because it does not protect analog content, the Encryption Technology Mandate Proposal fails to achieve its core goal of effectively preventing unauthorized redistribution of digital broadcast content to the public over the Internet. In fact, MPAA itself has admitted this, stating in the FCC's just completed "Plug and Play" proceeding that systems". . . [that permit] the continued availability of unprotected analog connections . . . [fail] to achieve meaningful protection of digital content."[1]

[1] Comments of MPAA on the FCC's Notice of Proposed Rulemaking in the "Plug and Play" Agreement (CS Docket 97–80, PP Docket 00–67) {March 28, 2003) at 2.

The proposed system has the potential to leak in other ways as well—including through the expected use of "software demodulators." Because the proposed system cannot protect digital content in a pervasive or robust manner, there is simply no sustainable public policy rationale for its adoption and implementation, especially in light of the substantial cost and complexity impact it would have on consumers.

For these and other reasons, and like so many other groups—including major public interest groups, software companies, IT and computer companies, libraries, consumer electronics companies, advocates for persons with disabilities, privacy groups, and literally thousands of individual consumers—Philips believes that adoption of the Encryption Technology Mandate Proposal would be a grave mistake. We can and must work together to explore alternatives that are both consumer friendly and effective.

There is Time To Explore Alternatives

Importantly, there is time to find such an alternative. The state of consumer broadband technology—both in terms of bandwidth and digital compression—largely mitigates the immediacy of the threat of widespread redistribution of high definition digital broadcast content over the Internet.

First of all, the vast majority of consumers do not have the necessary bandwidth to engage in widespread uploading and downloading of HDTV content to and from the Internet. In fact, today and for the foreseeable future, sending broadcast HDTV over the Internet in any reasonable amount of time requires such a level of compression as to necessarily degrade the signal well below even today's analog television resolution.

In fact, as revealed in the chart below, using today's Internet technology, it would take at least 25 hours using even an advanced (*i.e.,* 1.5 Mbps) broadband connection, and 28 days using a more common dial-up modem, to retransmit a 2-hour HDTV broadcast movie in its native resolution, even assuming that the connections operated at their maximum speed, which they rarely, if ever, do. Even a 2-hour SDTV broadcast would take approximately 5 hours to retransmit in its native resolution using a perfect 1.5 Mbps broadband connection, or 142 hours over a 56 kbps dial-up modem.

Current Transfer Speeds for HDTV and SDTV

Signal	Upload/Download Connection	Time to Transfer a 2-Hour Program
HDTV	**1.5 mbps (broadband—max/atypical)**	**25 hours, 44 minutes**
HDTV	1.0 mbps (broadband—typical)	38 hours, 36 minutes
HDTV	56K (dial-up—never actually achieved)	689 hours, 17 minutes (28.7 days)
HDTV	53K (dial-up—actual max)	728 hours, 18 minutes (30.3 days)
HDTV	50K (dial-up—typical)	772 hours (32.2 days)
SDTV	**1.5 mbps (broadband—max/atypical)**	**5 hours, 20 minutes**
SDTV	1.0 mbps (broadband typical)	8 hours
SDTV	56K (dial-up—never actually achieved)	142 hours, 51 minutes (5.9 days)
SDTV	53K (dial-up—actual max)	150 hours, 56 minutes (6.3 days)
SDTV	50K (dial-up—typical)	160 hours (6.7 days)

And, importantly, no meaningful advances in digital compression technology are envisioned in the foreseeable future that would provide uploads and downloads of high resolution content at any reasonable speed. Even assuming that a twice as efficient compression scheme as MPEG2 were developed (and it has not been), the transmission times are still too lengthy to make widespread broadband Internet distribution of high definition content an imminent or significant problem. Thus, to the extent content owners are concerned that the existence of digital television receivers suddenly dramatically increase the risk of massive unauthorized redistribution to the public over the Internet of their "highest value" content, Philips would respond that such concern is unfounded and should not drive us to accept content protection solutions that do not achieve minimally acceptable levels of competence and consumer friendliness.

Watermarking Offers A Better Answer

Given the fact that we have time to do so, we owe it to consumers, in particular, to work together to seek a more holistic solution that provides effective and *pervasive* protection for digital broadcast content from unauthorized redistribution to the public over the Internet—including after it has been passed through an analog output—and that has as light a touch on both devices and consumers as possible. Phil-

ips believes that a system, based principally on watermarking, instead of encryption, offers such a solution.

It could preserve the functionality of legacy equipment and permit seamless interactivity between both existing digital devices and those designed to recognize the watermark. Unlike the "chaining dependencies" that afflict an encryption system, devices in this system function independently of others, thus avoiding any need to replace an entire system. Rather, a consumer will add compliant equipment in the normal course of upgrading. A watermarking system can preserve fair use without imposing unfair costs on consumers.

It could effectively and pervasively address concerns about Internet redistribution of digital content, including content that has passed through an analog output, by making content that has traversed the Net incapable of being re-recorded or displayed. By recognizing when a watermark has been copied—which is what occurs in Internet retransmission—this system could prohibit a compliant device from either recording or displaying that content, essentially making the content useless to the recipient.

Finally, unlike the Encryption Technology Mandate Proposal and other encryption approaches, which can impose multiple layers of encrpytion/decryption requirements (including licensing costs) on every digital interface in every device in a home network, a watermarking-based system could be far less invasive, less co:: tly and less complicated to regulate.

This is not to say that a solution based upon watermarking a technology that content owners strongly support—is achievable overnight. The complexity of the business, technical, and legal issues at stake necessarily require a fully cooperative effort be undertaken, in an open process, by all stakeholders. Just as the stalemate over DTV-cable compatibility was successfully ended when the cable and consumer electronics industries negotiated in good faith for months to develop an agreement, so too will DTV content protection only be achieved in a manner acceptable to all parties when all of those parties agree to work together in good faith.

Conclusion

In closing, Philips calls upon Congress to ensure that the adoption of any digital broadcast content protection system meets the core requirements we believe are essential to consumers and to the successful transition to digital television: meaningful competency in protecting against unauthorized retransmission of high definition and other high value digital content to the public over the Internet, preservation of consumers' fair use expectations without oppressive costs and complexity, and clear and enforceable safeguards to ensure robust competition and innovation in the CE and digital content protection marketplaces.

Philips pledges its full, continued support toward finding solutions that meet these requirements, and further pledges to do its part to make technological solutions available on open, fair and reasonable terms to all interested parties. We look forward to this Committee's continued leadership in this critical arena and I would be please to take any questions you might have.

Senator BROWNBACK. Thank you, Mr. Blanford.

Mr. Jack Valenti, the eternal head of the MPAA, also has a star in Hollywood. Always a pleasure to have you here.

STATEMENT OF JACK VALENTI, PRESIDENT AND CEO, MOTION PICTURE ASSOCIATION OF AMERICA

Mr. VALENTI. Thank you, Senator.

A quick retort to the distinguished Mr. Blanford. What he forgot to tell you was that 70 organizations—big computer companies, consumer elec companies and others—all gathered together. Fifty six of them embrace the broadcast flag. Eight did not. Philips was one of the eight.

And the abstruse and technical aspects of his testimony only confirms my belief and others' that the Congress is not equipped to deal with this kind of technology. That is why you have an expert agency like the FCC to deal with it.

Having said that, I thank you, Mr. Chairman, very much for allowing me to come here to tell you and your colleagues about the

perils of digital piracy, which if it goes unchecked will disfigure and decay America's great intellectual property industry. Now, why is this a national problem? Because intellectual property is America's greatest trade export and it is an awesome engine of economic growth. We are creating new jobs at three times the rate of the rest of the economy at a time when we are suffering a two million job loss. We bring in more international revenues than aircraft, than agriculture, than automobiles and auto parts. We comprise more than 5 percent of the GDP. The movie industry alone has a surplus balance of trade with every single country in the world. I do not believe any other American enterprise can make that statement at a time when we are hemorrhaging, this Nation is, from a $400 billion deficit balance of payments.

Now, piracy is the darker side of digital subversion. To the almost one million people in this country who have jobs in some aspect of the intellectual property—I mean, the movie business, 99 percent of whom do not make big salaries. They are good citizens, they are good neighbors, they have kids to send to college and mortgages to pay. Their livelihoods are put to hazard if we do not find some way to stop this increased velocity in digital stealing, a casual disregard for other people's property.

Now, let me tell you how bad it is. Outside estimates say that some 500,000 movies are being illegally uploaded and downloaded every day on file-swapping sites. I call them file-stealing sites—Kazaa, Morpheus, Grockster, Nutella, eDonkey, Imesh, and the list goes on. And if we do not stop that, then I think we are going to watch and be witness to the slow undoing of an industry that is the envy of every single country in the world.

I believe that if you impose—well, first I want to say that no one knows the future. The future is wrapped in shrouds and it is vapory and blurred. But what we do know, Mr. Chairman, is that all the technology that we find so magical today will seem primitive 18 months from now. That is why I think to impose an absolute ban on technical mandates is, I respectfully submit, is not good government policy. It is not in the national interest to ban what you cannot see, to prohibit what you do not know, to turn your back on what you cannot measure. That is not good.

Now, the broadcast flag about which Mr. Blanford talked is a classic example of a beneficial technical mandate. What does it do? It has one simple design, that is all. It says that you cannot redistribute a digital over-the-air program back to the Internet, that is all. And by the way, the customer will never know there is a broadcast flag. He can do anything he is doing in the future that he is doing now, copy to his heart's content, except if he wants to take that digital program and shoot it back to the Internet where it is easy prey to thievery. Cannot do that.

So that is why I think that the broadcast flag is good. Now, without the broadcast flag, without it, free over-the-air high-quality programs digitized in the future are going to migrate from free broadcasting to pay services, where they can be better protected. No sane business executive is going to allow his high-quality program in digital form to go out unprotected, naked and alone, easy prey to thievery. Not going to do it, and that is an example of, I think, good business sense.

Now, our anxieties are about the future. If we could stop time and motion right now, Mr. Chairman, and leave everything as it is, I think we could get along OK. But the fact is that time and change are very restless and they resist containment, and it is going to be moving with such velocity.

CalTech has just announced an experiment called FAST, F-A-S-T. I am going to be giving a lecture out there in 10 days and I am going to visit those laboratories personally. FAST brings down a DVD-quality movie in 5 seconds. Internet 2 is another experiment, which has deployed 6.7 gigabytes, 6.7 billion bytes, halfway around the world, 12,000 miles, in 5 minutes.

It is that kind of change that we are looking at and where, if you impose a ban on technical mandates, who is going to save us?

Now, we love the technology of the Internet. We think it is the greatest and most glorious delivery system yet known, and we want to use it to put thousands of our movies up there, our new movies, our classics, all genres, 10, 15,000, so that the customer will have an absolute abundance of choices. But Mr. Chairman, those valuable works have to be protected. The Congress should not close a door on possible new technologies, possible, that have a potential to salvage the future, new designs that will give more choices to consumers and at the same time keep alive this great intellectual property industry which, as I said, is an awesome engine of economic growth.

Thank you, sir.

[The prepared statement of Mr. Valenti follows:]

PREPARED STATEMENT OF JACK VALENTI, PRESIDENT AND CEO, MOTION PICTURE ASSOCIATION OF AMERICA

The Perils of Movie Piracy—and its dark effects on consumers, the million people who work in the movie industry, and the nation's economy

Some facts, worries and a look at the uncharted future

The peril of piracy, to the nation and to the almost one million men and women who create, distribute and market movies

No nation can lay claim to greatness or longevity unless it constructs a rostrum from which springs a "moral imperative" which guides the daily conduct of its citizens. Within the core of that code of conduct is a simple declaration that to take something that does not belong to you not only is wrong, but it is a clear violation of the moral imperative, which is fastened deep in all religions.

That is fundamental to how this Nation fits itself to honorable conduct. Anyone who deals in infirm logic to certify that "stealing movies off the Internet is okay, nothing wrong about it since everybody does it, and no one gets hurt," is obviously offering up a defunct mythology to cover their tracks.

Piracy, or "stealing," is the darker side of digital subversion. Digital theft has an inevitable leaning toward a future darkly seen by those who create, distribute and market films. For the almost one million men and women who work in some aspect of the movie industry—99 percent of whom don't make big salaries, who are good citizens and good neighbors, with mortgages to pay and kids to send to college—their livelihood is perilously in doubt if digital stealing goes on, increasing in velocity with a casual disregard for other people's intellectual property.

Piracy is a National Problem because Intellectual Property nourishes the American economy

Piracy is a national problem. It must be a high priority of the officials who comprise the Federal Government. Intellectual property (movies, TV programs, home video, books, music, and computer software) is an awesome engine of growth which nourishes the national economy. Not only is intellectual property America's *largest trade export,* bringing in more international revenues than agriculture, aircraft, automobiles and auto parts, but it is creating new jobs at *three* times the rate of

the rest of the economy, and is responsible for over five percent of the GDP. The movie industry alone has a *surplus balance of trade* with every single country in the world. No other American enterprise can make that statement—and at a time when this country is bleeding from a $400 billion-plus *deficit* balance of trade.

The movie industry sits on a fragile fiscal bottom. Only one in ten films ever gets its investment returned through theatrical exhibition. Films have to journey through many market venues—premium and basic cable, satellite delivery, home video, network and individual TV stations, international—in order to try to recoup the private risk capital that brings a movie to life. If a film is kidnapped early in that journey, it's obvious the worth of that film can be fatally depleted long before it can retrieve its investment.

At this moment, the movie industry is suffering from a loss of some $3.5 billion annually from hard-goods piracy—DVD, VCD, videotape. We are every hour of every day fighting that theft all over the world. As yet, we have not put a loss-figure on digital piracy. We are working on it. We do know from outside estimates that some 400,000 to 600,000 films are being stolen *every day,* and it is getting progressively worse.

The movie industry is trying to explain to and educate youngsters and not-so-young about the value of copyrighted material

The movie industry is laboring to find rebuttals to piracy. We have launched an education project through TV public service announcements, trailers in theaters, an alliance with one million students via Junior Achievement to 'explain and educate' why copyright is central to intellectual property growth, and why filching movies in digital form by uploading and downloading on the Net, is not only just plain wrong, but has a malignant effect on the future of American consumers.

We are also launching a long-term technological research project enlisting the finest brains in the high tech industry to discover ways and means to baffle piracy, technologically. We are constantly looking for innovative and robust ways to protect American creative works which, I am proud to report, finds a hospitable reception on all the continents, where our films are patronized and enjoyed by all creeds, cultures and countries.

That is why I am here today—to tell you of the immeasurable economic and entertainment value of American films—and to ask for your help in the never-ceasing fight to combat theft of our movies.

No one can predict the shape and form of the future

I don't know, nor does anyone else, the shape and form of the future. We do know that the technology we find so magical today will seem primitive 12 to 18 months from now. The ascending curve of change is mind-bending. But no one can chart the digital future.

That is why to impose an absolute congressional exile on so-called "technology mandates" is not good public policy. No one can forecast what future technology mandates will be needed. That's why *it is not in the national interest to ban what you cannot see, to prohibit what you do not know, to turn your back on what you cannot measure*

An absolute ban on technology mandates for access control or redistribution control technologies would injure the discretion of the FCC. It is an agency created by Congress to regulate in the public interest. To do that it needs the tools to do the job, to carry out its legislative command. Expert agencies like the FCC were created to take on the burden of detailed, abstruse regulations that Congress has agreed it is not equipped to do. To tie the FCC's hand in advance is surely not in the public interest.

I agree that the proposed ban on technology mandates cheers those whose mantra is "all content must be free," including pornography and material stolen from its owners. But their view collides with the public interest.

The FCC *should have the authority* to adopt regulations that serve the interests of consumers. That may very well include technical mandates that would create a safe environment in which valuable content would be made available in vast amounts to consumers.

The Broadcast Flag is a good example of a technological mandate that will serve consumers.

The Broadcast Flag is designed simply to stop digital over-the-air broadcasts from being re-directed to the Internet for anyone to pilfer, easily, swiftly. By the way, consumers will never know there is a Broadcast Flag, unless they try to re-distribute a program to the Internet. The Flag enjoys cross-industry support. Without such a mandate, companies that agree to abide by the Flag would be at a disadvantage from companies that did not. In the end, as it always happens, it is the con-

sumer who would get it in the neck. Why? Without a Flag, high-value content would surely migrate from free over-the-air broadcast, which would not be able to protect content from piracy, to pay systems which offer some protection. Sane business executives would never allow their finest programs to go over-the-air, unprotected, hapless prey to digital pirates.

Of course, in the realm of technological mandates, all companies competing in the digital arena have singular preferences. For example, Philips supported the "Plug & Play" agreement at the FCC. And with some qualification, so did the Consumers Union. Philips has also developed a watermarking technology to solve the so-called analog reconversion problem—which occurs when a protected digital signal is converted in the consumer's home TV to analog and back to digital—wherein all the encrypted protection is stripped away, leaving a movie naked and unprotected against illegal copying. To implement Philips' watermarking as a standard across the board would require a technology mandate.

Our most anxious concerns are not about the present, but the future. Is the Congress familiar with experiments now going on that will reshape and enlarge the ease and speed of digital thievery? Cal Tech reported one experiment called "FAST," which can download a quality DVD movie in *five seconds!* Another experiment, "Internet-2," has dispatched 6.7 gigabytes halfway around the world in *one minute!* (A DVD-movie contains some 4.6 gigabytes.) What is experiment today will be commonplace in the community three to four years from now. Which means that the glorious enticement of FREE and easy uploading and downloading movies, with little risk, will be far more intense than it is now.

Pornographic Content on the Internet, so easily available to children

This Committee must be sensitive to a most unwholesome fungus which infests "peer-to-peer file swapping sites" such as Gnutella, Morpheus, KaZaa, iMesh, E Donkey, Grockster, etc. That disfiguring fungus is pornography on a scale so squalid it will shake the very core of your being. As easy as it is to illegally download movies, it is equally easy to bring home this foul pornography. Any 10-year-old can do it—and probably does. Do parents know this?

While searching for pirated material on these P2P sites, MPAA technicians discovered large caches of pornography disguised as child-friendly fare. This awful content is "meta-tagged" or coded to searches children are likely to undertake, like "Disney," "Harry Potter," or "Spy Kids." Is it the intent of this Committee to ban expert agencies from mandating technical remedies yet to be found to allow parents to fence off this foul material from their children?

What the movie industry needs

We need the Congress to understand and appreciate the vast worth of copyrighted intellectual property. In the global film arena the United States is preeminent. We need the Congress to heed our warnings that unless there is put in place various baffle-plates of protection, we will bear witness to the slow undoing of this huge economic and creative force.

Which is why I urge the Congress not to close the legislative door on any new technological magic that has the capacity to combat digital thievery which—if unchecked—will drown the movie industry in ever-increasing levels of piracy.

Senator BROWNBACK. Thank you. Thank you, Mr. Valenti.

Dr. Edward Felten is a Professor of Computer Science at Princeton University. Thank you for joining us.

STATEMENT OF EDWARD W. FELTEN, PROFESSOR OF COMPUTER SCIENCE, PRINCETON UNIVERSITY

Mr. FELTEN. Thank you.

I would like to offer a computer technologist's perspective on the issue of technology mandates. In my view, the best future for both the entertainment and technology industries is to embrace innovation, to concentrate on making the legitimate entertainment experience as attractive as we can.

Now, innovation is inherently experimental in nature. We try many things and most of them fail, but we learn from the mistakes. And the process of innovation is unpredictable. We do not know which approaches will turn out to work. We do not know

which will turn out to fail. Because of the experimental and unpredictable nature of innovation, it is especially sensitive to being derailed by regulation.

This is particularly true in areas where the technology is immature, as in digital rights management technologies, the technologies that are designed to attempt to prevent copying and redistribution of content. Now, the goal of DRM technology ought not to be to control legitimate consumer use of content within the home. It ought to be to prevent the wholesale infringement that Mr. Valenti so rightly worries about, in other words to prevent Napsterization of content.

What we are worried about, then, is that someone, a single person somewhere, will rip the content to a digital file and distribute it worldwide across the Internet, of course in violation of the law. It follows then that a DRM technology in order to be effective and to prevent this threat must do more than prevent 95 percent or 99 percent of the would-be infringers from ripping the content and redistributing it. It needs to work against every single person out there who has the knowledge and the willingness to break the law to redistribute the content.

That is a very high bar that the technology must meet, and today's technologies are not up to that challenge. We do not come anywhere close to having a technology that can really provide the level of protection that Mr. Valenti and the people in the industry would like to see. We may never have technologies strong enough to prevent—to act by themselves to prevent this threat.

But if there is a hope of better DRM technologies which can more effectively protect the content, that hope lies in further experimentation and further trying of new technical approaches. So it is particularly important to leave the field open for innovation in this area. The worst case outcome in my view is a mandate which locks in today's state-of-the-art with its insufficient protection while preventing the exploration of new approaches that can provide better protection in the future.

Now, I recognize that mandates may be a reality despite their effect on innovation. If we must have technology mandates, there are things we can do to limit their impact on innovation and to keep as open as we can the possibility that we will have better technologies in the future. I would suggest four guidelines to that end:

The first is that the technologies ought to be aimed squarely at stopping infringement and not at controlling legitimate uses of content by consumers at home.

Second, it is important that the evaluation criteria be simple and neutral and applied in a neutral fashion and be based on technical performance or lack thereof.

Third, I think it is important that a mandate process allows the possibility that no satisfactory technology is found to exist. The process ought to be willing to hold off mandates until a sufficiently strong technology comes along, rather than insisting on imposing a mandate because the schedule calls for it.

Finally, it is important I think to ensure that a mandate applies to as narrow a class of device as possible so as not to have impact on devices that are fundamentally unrelated to the problem. It is especially important that mandates try to avoid impinging on the

design of general purpose technologies such as telecommunications, computers, or the Internet.

Now, the common thread in all of this is the desire and the need to keep the field open for further innovation and further discovery. The technologies that all of us would like to see will come into being only if we keep that field open.

The key to progress is not to limit technical innovation, but to embrace it.

Thank you.

[The prepared statement of Mr. Felten follows:]

PREPARED STATEMENT OF EDWARD W. FELTEN, PROFESSOR OF COMPUTER SCIENCE, PRINCETON UNIVERSITY

Digital technology presents an unprecedented opportunity for the entertainment industry—and an unprecedented challenge. As the price of storing and distributing digital content drops, new services and business models become possible. New types of copyright infringement become possible too; and unfortunately infringement has become all too common. The debate is not about whether this infringement is harmful—we all know it is—but rather about how we should respond to it.

Entertainment companies are understandably concerned about the rise in infringement, and they have proposed technology mandates as one response. While well intentioned, these mandate proposals are of dubious technical merit. Worse yet, they may cause serious harm, by curbing innovation in information technology and consumer electronics. The worst case—which is very possible—is that mandates will retard the development of legitimate technologies, while failing to make any dent in infringement. If it is not possible to avoid mandates altogether, the next best alternative is to limit their scope carefully so as to reduce the harm they cause.

Technology, like the rest of our culture, relies on a community of creative people striving to combine old ideas with new to advance a common body of knowledge. Although textbooks portray technical progress as an inexorable advance along nearly preordained lines, in practice the process of discovery is anything but predictable. It is only through trial and error—with many zigzags and false starts—that we know which way to go. Technology moves fastest in an open and chaotic marketplace of ideas, unconstrained by mandates.

The Digital TV Transition

The transition to digital television (DTV) will greatly increase the clarity and visual resolution of TV programming. This change will reduce piracy, by increasing the quality difference between legitimate and pirated programming.

Consider the mechanics of DTV piracy. Full-resolution DTV images require an enormous amount of hard drive space to store and an enormous amount of bandwidth to transmit. A three-hour TV movie in ATSC format occupies about 26 Gigabytes (*i.e.,* about 26 billion bytes) of storage. To store just one such movie requires a hard drive that costs about $50—enough money to buy two or three DVD copies of the same movie. To transfer this file across the Internet to one other person, assuming both parties have fast home broadband connections, takes about two days. Few would-be pirates would go to this much trouble, when the same movie is available, sooner and at a lower price, on DVD or pay-per-view instead.

A pirate would choose instead to compress the video file, to make it smaller at the cost of reducing visual quality. A file small enough to transfer quickly over a broadband connection will have fairly poor visual quality. Whether would-be infringers are willing to download these infringing files depends on how the files' quality compares to that of legitimately obtained content.

Today's analog television offers mediocre visual quality, so highly compressed files may be an acceptable visual substitute (for customers who ignore copyright law). However, DTV offers a much better visual experience, making the degraded quality of compressed files much more evident. The highly compressed files offered by pirates will therefore be less attractive after the DTV transition than they are today.

The DTV transition will make legitimate content better, without affecting the quality of pirated on-line content. The result will be to raise the demand for legitimate content. Because of this, technology mandates make even less sense in the future DTV world than they do today.

Innovation and Regulation

The main effect of mandates would be to impede legitimate technical progress.

Innovation is inherently unpredictable. If we know how to do something, we are already doing it; so a technology advance is by definition a surprise. The path forward is not a straight one. We move forward by trial and error, as new insights teach us how to build on past failures.

To foster innovation, then, we must keep the field clear for surprising developments, so that experimenters and entrepreneurs can pursue whatever avenue of progress they discover. Closing off these avenues through overregulation carries a high price, in missed opportunities and inventions that are never made.

It is tempting to imagine that we can concoct a regulatory regime that is truly technology-neutral, not favoring one technical approach over others but discriminating among products based only on their effectiveness. In practice, though, any regulation will encode certain assumptions into its definitions, its terminology, and its criteria. Those assumptions might seem innocuous when the regulation is written, but over time they will channel and limit progress. Existing approaches will move ahead, but new, innovative technical approaches will be stifled if they conflict with the regulatory assumptions. Since we cannot predict the technical future, we will not be able to write regulations that keep the road clear for future inventions. The winning products, and the winning technical approaches, will be chosen not by the market but by the regulators. Inevitably, this will retard technical progress.

Regulation and General Purpose Technologies

Regulation has an especially harsh effect on general-purpose technologies such as personal computers and the Internet, which are capable of performing powerful operations on data without needing to understand that data in detail.

The classic example of a general-purpose technology is the telephone network, which can carry a conversation about any topic, between any two people, and can do this without the network itself having to understand what those people are talking about. The telephone network is designed for the simple, general-purpose task of transmitting sounds from one place to another. It is indispensable precisely because it is general-purpose—because it can be used to talk about any topic whatsoever, and because it transmits faithfully every pause, inflection, and nuance in the speakers' voices; and it is feasible to build a flexible, inexpensive, and easy-to-use telephone system only because that system does not try to understand what it is transmitting.

Personal computers and the Internet are also general-purpose technologies, as they are designed to operate on data of absolutely any type, without the need to understand that data. As with the telephone, the general-purpose nature of these technologies makes them both more useful and much easier to build than the special-purpose alternatives.

Regulation poses a special danger to general-purpose technologies, because those technologies are capable of such a wide range of uses. Any regulatory ban on devices that are merely *capable* of certain disapproved uses will necessarily ensnare general-purpose technologies, even if those technologies are not designed for or primarily used for nefarious purposes.

Consider, for example, a hypothetical regulation that bans technologies that can be used to negotiate drug deals. This regulation, though presumably well intentioned, would amount to a ban on telephones and the telephone network. Someone who did not understand how telephones work might reply that the solution is to redesign the telephone network so that it cannot be used to talk about illegal drugs. But such a mandate would be contrary to the nature of the telephone network, which is fundamentally incapable of understanding how it is being used. Even if it were somehow possible to build such a restricted telephone network, the regulation would still fail to achieve its goal, as drug dealers would just switch to talking in code, perhaps discussing purchases of "sugar" and "flour." General-purpose technologies will always be capable of both good and bad uses. To eliminate the bad uses is to eliminate the technologies themselves.

This is not to say that nothing can be done about telephonic drug dealing, or about any other misuses of general-purpose technologies. My point is that mandates are not the right solution to these problems, which are best addressed through other means, such as traditional police work.

A Technical Perspective on Mandates

An analysis of technology mandates must start with a clear understanding of what the mandates are trying to achieve. There are two possible goals: they might be intended to control consumers' use of content, or they might be designed to prevent "Napsterization," or widespread copyright infringement. To put it more bluntly, a mandate may try to change the rules of our copyright system, by transferring cer-

tain rights (in practical terms) from the public to copyright owners; or it may simply try to better enforce the traditional copyright system.

It is easy to see how controlling legitimate use serves certain private interests; but mandating such technological control amounts to a significant change in public policy. Other witnesses are addressing the implications of this transfer in more depth, so I will not dwell on it here, except to say that such a policy change, if it is to be made at all, should not be introduced through a regulatory back door.

If the goal is to prevent Napsterization, then the protective technology must be especially effective. Network redistribution is such a serious threat because it allows a single illicit copy of a work to become available to hundreds of millions of people all over the world. To prevent Napsterization, then, it is not enough to prevent most consumers from copying most of the time. As long as *even one* consumer has the technical knowledge to "rip" and redistribute the content, along with the inclination to do so in spite of the law, the content will become available to everybody—it will be Napsterized. To prevent Napsterization, a protective technology must be so strong that not even one would-be pirate can defeat it.

Today's anti-copying technologies don't even come close to meeting this challenge. At best, they control and limit the activities of ordinary users; but a would-be pirate with a moderate level of technical skill can defeat them with moderate effort. Today's technologies do not, and cannot, prevent Napsterization.

Most independent technical experts believe that no technology will ever prevent the capture and redistribution of digital content by determined pirates. Certainly, this view is consistent with the checkered history of anti-copying technology. If this view is correct, then—like it or not—technology is not the answer to the digital copyright dilemma, and the result of mandates will be all pain and no gain.

Even if a technical antidote to Napsterization is in our future, that antidote will come about only through continued research and experimentation. Restricting technical progress by over-regulating will only lock in today's level of ignorance, delaying the day (if it ever comes) when we know enough to solve this technical puzzle. If we are not careful, we will mandate the use of ineffective technologies, while preventing the creation of better ones.

Reducing the Harm Done by Mandates

I have argued above that technical mandates retard innovation and provide few if any benefits in return. My hope is that we will have no technical mandates at all.

If we must have mandates, they should be structured carefully so as to minimize the harm they cause. To that end, I would suggest four guidelines.

First, any mandate should be aimed at preventing infringement, and not at controlling consumers' legitimate, fair uses of content. The mandate should be limited to technologies that leave fair use and the right of first sale intact.

Second, technologies should be evaluated according to simple, neutral technical criteria. Keeping the criteria simple and neutral will reduce their influence on the direction of technical progress, and will keep the barriers to entry low so that new technical approaches can be tried. The criteria should be based on results achieved rather than on the use of specific technical methods.

Third, the mandate should allow for the possibility that no satisfactory technologies exist, rather than simply assuming that a suitable technology can be found. If nothing works, the mandate process should be willing to admit that fact and wait for better technologies to develop, rather than locking in a bad solution.

Fourth, the set of devices subject to the mandate should be as narrowly defined as possible, so as to minimize the regulatory impact on unrelated markets. A device should not be regulated merely because it might conceivably be modified or reprogrammed for an infringing use. It is especially important to protect general-purpose technologies, which by their nature are especially susceptible to regulatory harm.

Conclusion

Copyright infringement is a serious problem that has no easy solution. We should resist the "quick fix" of technology mandates, which will do little if anything to reduce infringement, but will impose a regulatory drag on the very industry whose progress might yield a better solution to the piracy problem. If we must have technology mandates, they should be narrow and carefully focused. The path to a better future lies not in limiting technical progress but in embracing it.

Senator BROWNBACK. Thank you, Dr. Felten.

Mr. Murray, Christopher Murray, Legislative Counsel Director for Consumers Union, welcome.

STATEMENT OF CHRISTOPHER MURRAY, LEGISLATIVE COUNSEL, CONSUMERS UNION

Mr. MURRAY. Senator Brownback, Senator Inouye, and Senator Lautenberg. I would first like to thank you for your kindness and tenacity in hanging through the lunch hour and listening to our testimony today. I know that this can perhaps be an opaque subject because it is a little bit technical. I will try to be a little controversial for the sake of keeping us all awake.

I love gadgets. I love movies. I love all of the technology that consumers use today, and that is what our magazine, "Consumer Reports," tries to rate for consumers. We try to look at products and see where there is a horse race and see if there are ways that technology can be made in better ways and in worse ways.

I think it should be obvious from the fact that we produce a magazine that without copyright I would not have a job, and I would not be able to be here before you today. So we are 100 percent committed to the protection of intellectual property, and we are quite concerned about the piracy problem that I see facing both the movie studios and the music industry today. I think it is an immense problem.

I want to drill down just for a few minutes into the broadcast flag particularly because that is the nearest term thing on the FCC's docket. A decision is perhaps in the 8- to 12-week range or even sooner by some accounts. And I think that this is an underappreciated docket over at the commission, because it has the potential to mess with consumers' televisions and we know that there are few things that raise consumer ire like messing with their televisions.

I am going to suggest that the broadcast flag is a solution to a problem that we do not yet have, with technology that we have not yet seen; and that, furthermore, engineers that I trust and respect tell me it is the least effective and most costly way to solve this problem, assuming that it ever does become a problem. I think that is a reasonable assumption, that the problem we are talking about will become a problem.

But as policymakers I think it is important for you to distinguish what the problem is. Is there a problem of redistribution on the Internet of high-definition digital television? I am going to submit that the answer is no. When people redistribute content on the Internet, they scale it down to postage stamp size so that it is reasonable to redistribute on the Internet. Otherwise you would be there for years trying to redistribute that content.

Now, I can do that same kind of redistribution without a digital source. I can take any analog signal that comes today over rabbit ears television and for less than $100 I can go to Radio Shack and buy a device that will allow me to convert that signal to something that a computer can read and that can then be redistributed on the Internet.

So again, what I am not saying is that there is no piracy problem here, but that we must distinguish what the exact piracy problem we have is. I do not want to be too shrill about this, but, Senator Brownback, you mentioned the Laurie Kraner study from AT&T Labs which cited the fact that about 80 percent, 77 percent, of the content that is currently on the Internet is the back of the truck

problem. Now, that is not to diminish the scale of that problem. It is simply to say let us go after the problem where it exists.

While I do not support tech mandates generally, I think were the government to be issuing tech mandates we should issue them in a space where there is a problem currently. Internet redistribution of music is a huge problem. It is not clear to me exactly how much it is cutting into sales, but I think we can all consent with the fact that it is at least somewhat diminishing music industry sales. That is a problem I think we should be aiming to solve in the near term. Internet redistribution, again, of high-definition digital television is not currently a problem.

The second thing I said is that it is a solution to a problem that does not exist, with technology that we have not yet seen yet. We have been told that this technology is going to allow consumers to do the same fair use and reasonable things that they have always done. I can take a tape of a show, a new show perhaps that I was on, to my grandmother's house, show that to her. I can take a tape of "Friends" to my friend's house and we can watch that together.

What I do not understand is how we are going to on the one hand protect that content from piracy in a robust fashion and on the other hand not preclude some of those uses. Now, it may—excuse me. It very well may be that I am just not smart enough to understand how they are going to do that. But that is my point. I have not seen the technology. I think it would be extremely unwise for the FCC to buy this pig before they take it out of the poke.

I would also submit that it is Congress and not the FCC that is going to have its head handed to it when consumers get really upset about the fact that perhaps they cannot do the things that they are currently today used to doing with their television sets.

The other thing that I said is that engineers I trust tell me that it is the least effective and it is the most expensive way to do this. Let me offer an example. Imagine that we are the National Security Agency and we want to communicate securely with only the people that we want to get that communication. There is a couple ways we could do that. One way would be we could encrypt that information at the source and then we could send it out and not so much worry about where it is going to be picked off because it is going to be scrambled when people get it.

The other way that we could do it, were we the NSA, is we could broadcast that information in the clear and then go around and make sure that every radio that is produced in the world cannot pick up that information or that once they pick up that information that they have got to do something in particular with it. Now, that is obviously a more costly way and probably not the wisest way to do it, and it is not the way that we run our intelligence operation.

I will wrap up quickly. On the cost point, the reason this is such an expensive proposition is because, as has been pointed out here, this is intending to regulate a very large swath of our economy. Not only—actually, let me just quote from MPAA's broadcast flag comments at page 14. Quote: "An effective comprehensive solution must be mandated by the commission for pertinent products."

In case we were not clear on what pertinent products are, in the parentheses that follows they say: "Although the commission's notice refers to consumer electronics devices, it is essential, and we

assume the commission intended, that computer or IT products be regulated as well as so-called consumer electronics products." That is an immense scope.

I want to help solve this problem when this problem comes up and I think we should be forward-looking about solving this problem. But let us do it in an effective way. Let us not give hackers a huge target of an unmoving object that they can then hack and then we have precluded a whole next generation of technology of DRM, as Professor Felten pointed out, from emerging because we have mandated the wrong one.

If we mandate the wrong technology, you are going to have people back here asking, not once for consumers to pay this transition, but twice they will have to pay for this transition.

My final sentence. Forgive me for running over. The beauty of the computer is that it can be a typewriter and a television and a recipe book, but it is not the function of recipe books and typewriters and televisions to be computers. We should strive to have devices that have not just features but potentials.

Thank you.

[The prepared statement of Mr. Murray follows:]

PREPARED STATEMENT OF CHRISTOPHER MURRAY, LEGISLATIVE COUNSEL, CONSUMERS UNION

Chairman McCain, Ranking Member Hollings, and Senator Brownback, I am grateful for the opportunity to represent Consumers Union,[1] the publisher of *Consumer Reports* magazine, and Public Knowledge[2] before your distinguished committee today.

Consumers Union is deeply concerned about piracy, and believes that copyright is crucial to the creation of content. Indeed, we wouldn't have a business without the revenues that copyright allows us to generate through the production of our magazine.

We also take seriously that copyright law strikes balances that benefit the public during the term of copyright ownership—that even unlicensed use of copyrighted works, according to fair use and other principles—benefits citizens generally even in some instances where it does not directly benefit[3] the copyright owner. That is why, for example, we have such a strong tradition of public libraries in this country.

These carefully crafted balances are threatened when new technologies make it possible for a single individual to share, in effect, thousands of copies of copyrighted works with millions of users. Music is particularly vulnerable in this scenario because the file sizes of digitized music have grown small enough that even Internet

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* and *Consumer Reports Online* (with approximately 5 million paid circulation) regularly carry articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[2] I am especially grateful for the immense contribution to this testimony of Mike Godwin, Senior Technology Counsel for Public Knowledge. Public Knowledge is a public-interest advocacy organization dedicated to fortifying and defending a vibrant information commons. This Washington, D.C.-based group works with wide spectrums of stakeholders—libraries, educators, scientists, artists, musicians, journalists, consumers, software programmers, civic groups and enlightened businesses—to promote the core conviction that some fundamental democratic principles and cultural values—openness, access, and the capacity to create and compete—must be given new embodiment in the digital age.

[3] Of course, it may indirectly benefit copyright holders, as for example in the movie "High Fidelity," when John Cusack's character, a record-store owner, plays tapes of music he loves and inspires shoppers to buy new records. The shoppers get a "free performance," but the artist gets new sales.

users with relatively slow connections to the Internet can still find and download a favorite song in a short period of time.

Statistics from the music industry indicate that record sales have declined over the last two or three years. While some of that decline might be blamed on business decisions by the record companies (given that they have released fewer albums over that time than they did at other times when sales were stronger),[4] or the war, or the recent economic malaise, our instincts tell us that much of this phenomenon is traceable directly to the free downloading of music files from the Internet, via peer-to-peer software or other mechanisms.

Couldn't we simply outlaw peer-to-peer software, or at least impose stronger legal restrictions on it? The answer to this is mixed: peer-to-peer activity on the Internet (a network of computers in which any two can share resources, including but not limited to content and other data) is a central part of the Internet design. A better approach, we think, is to look at ways our legal system can adapt itself to reduce the large-scale trading of music online—from one music fan to ten million strangers, for example—while at the same time exploiting new technologies that both deliver more music to more music fans, that pay more artists more money, that encourage the growth and exploitation of the open-architecture Internet, and that strike a fair deal that benefits artists, publishers, and ordinary citizens in general as we enter the first fully digital century.

As consumer advocates, we necessarily favor policies that ensure artists and publishers' getting paid for their creative work. We are willing to work with the record companies and the studios to come up with creative ways solve their piracy problem. What we won't do, and what we believe the Congress shouldn't do either, is attempt to set in stone the business models of the past while moving forward into the digital world. Ordinary citizens and consumers are forced to adapt to the rapid changes brought about by digital technology, and publishers, record companies, and studios will have to change too. Indeed, already many of them are showing signs of positive change, through the immense public success of Apple's iTunes Music Store (and its quickly responding imitators) to the decision by many studios to deliver movie content to theaters digitally—yet safely—because the content is protected by "digital-rights-management" (DRM) technologies.

As always, those who truly understand and embrace the future of technology are quickest to succeed at new models—especially if their competitors, like King Canute knew he could not,[5] sit in their thrones at the edge of the sea and order the tide not to come in. Do not take this example (a story incidentally drawn from the public domain) to mean that we believe obedience to the law and the balances struck by the law are unimportant—take it instead to mean that we believe our legal responses should be thoughtfully applied in a targeted way that not only does justice in particular cases but also communicates to the general public a sense of fairness, of proper scale, and of balance.

We accept the need for the deterrent effect of properly targeted enforcement efforts. We also stand opposed to measures, whether they are driven by our legislature or by our regulatory agencies, that attempt to slow down, or throttle, or centralize the digital technological innovation that has been—perhaps even more that the creative works of the movie studios and recording artists—a driving force in our economy for the last two decades. We believe there are ways to capture that ever-increasing technological momentum through approaches that ride the tide of technological innovation rather than seeking to slow or halt it.

The open architectures of the Internet and personal computers have revolutionized and benefited American lives already in countless ways. We now have an entire generation of children whose reflexive approach to answer a question may be to ask Google about it, then to trace down the answer on the World Wide Web.

Although the same computer and network technology has given us the new problems of copyright protection, it would be a tragedy if the measures we took to protect copyrighted works made the Internet less open, or the personal computer less useable—except when the user pays the appropriate toll.

Consumers want cool, convenient, connected gadgets. New technology has always forced us to continually rethink our laws, to reexamine the balance of copyright—from the printing press to the photocopier, from VCRs and MP3 players to personal video recorders like TiVo and Replay TV—and the United States has always embraced that new technology and that is a large part of the formula for our success. New devices have continually transformed the balance between creators and users, but historically we have erred on the side of allowing technology to flourish even

---

[4] See *http://www.soundandvisionmag.com/article.asp?section_id=2&article_id=453* and the underlying study cited by the article (see above) by George Ziemann, *MacWizards.*

[5] *http://www.zyra.org.uk/canute.htm*

when there was potential leakage, for the sake of capturing the substantial benefits of that new technology.

If content-protection measures are put on the table that do not centralize the process of innovation, that give consumers new functionalities, give them better products at better prices, we would support them. Unfortunately, many of the current proposals—especially the broadcast flag scheme—require a top-to-bottom redesign of the architectures of digital tools and perhaps even the Internet itself. The cable-compatibility "plug-and-play" proceeding at the Federal Communication Commission, depending on its details (which have not yet been published), could have a similar chilling effect on both innovation and access to information and even on the revenues of artists, who are already exploring new ways of showing and selling their creative works online through our dynamically open and evolving Internet.

The broadcast flag and certain aspects of the plug-and-play regulation currently before the Commission present the possibility that a small set of companies will be given a de facto veto on new business models based on political criteria. A much better approach would be to develop, collectively, a set of neutral technological criteria for standards that protect broadcast and cable-carried content—ideally one objective enough to provide predictability to innovators while open-ended enough to inspire ongoing innovation in ways to both protect and present content through digital systems.

Make no mistake about it. Closing the architecture of the Internet or of the personal computer will not merely harm consumers in terms of the value they receive when they buy new systems. Nor will the damage be limited to the computer industry, which has relied on open systems to fuel a generation of astounding innovation in digital products. Perhaps the worst aspect is that certain content-protection approaches, because they focus more on limiting consumer uses of traditionally distributed content than on creating new business models and new kinds of offerings, will ultimately hurt creators and publishers as well, and may even slow the already lagging transition to digital television.

There are other approaches, including more nuanced "digital-rights-management" approaches, that may not only work better than the content-protection standards currently being developed at the FCC, but also may have positive consumer effects.

Imagine, for example, how computer-based DRM could enable a person with disabilities to view a first run movie—on a one-performance-only ticketed basis—through their home theater system, rather than struggling with accessibility issues at a movie theater or simply waiting for the new film to become available on cable or DVD. Or imagine how the Internet could be used to present in-classroom performances of current films with educational value—in ways that both protect the value of the copyrighted work and widen the audience for it.

We believe DRM can be overly restrictive as well, but that the leavening effect of allowing a variety of DRM solutions to compete in the marketplace, rather than a narrow, and possibly obsolete scheme being mandated by Congress or by a regulatory agency, will help ensure that consumer flexibility in access to, as well as use of, new content will remain part of our longstanding copyright-law traditions.

In a minimally regulated free market for copyrighted works, the consumer wins. The example of DRM in spreadsheet software in the 80s is instructive. Initially, LOTUS 1–2–3 was strongly copy-protected and had a high pricepoint (and probably therefore had a higher need for protection because the incentives to circumvent were so great). Eventually a competitor (Borland, headed by Phillipe Kahn) came into the market with a product that was sold at a much lower price and unprotected. Because the product had a reasonable price—one that more consumers could afford to pay—the need for over-restrictive DRM was lessened, and software consumers generally find today that such DRM as continues to be used is far more humane than the harsh DRM regimes of the 1980s.

Please note that nothing we say here should be taken to mean that there is no room for DRM in the market—indeed, properly calibrated and flexible DRM schemes may serve as a consumer-engagement tool. In fact, we encourage the providers of DRM technologies to devote some fraction of their energies to making public-domain works more available through their digital-media platforms, with as few restrictions (or even fewer) than those in traditional analog publishing.

Today, the consumer's experience of DRM is all too often that it blocks something he or she might wish to do, and that he or she might have no problem doing with the work's analog counterpart. For example, it may be easy and cheap to photocopy a page of a book for an English lesson than it is to extract that same text from the digital version of that same book—even when the work itself is in the public domain.

We believe that if consumers had more positive experiences in purchasing and using DRM-protected works, and knew from experience that the DRM-imposed limi-

tations on their use came from publishers' choices and not from the technology itself, this rationalizing of the content market in itself would both give a human face to digital content platforms and serve to persuade many content vendors, still all-too-fearful of the digital world, to loosen the restrictions they impose through DRM on digital works.

The FCC's Broadcast Flag and "Plug and Play" Orders

The broadcast flag dramatically expands the FCC's regulatory authority and would have the agency regulate personal computers[6] in ways it never has before. What is now a decentralized industry—where the way entrepreneurs now get their products to market is they build them and they sell them—will now come under the purview of the Federal Communications Commission. If Congress wants the FCC to turn itself into the Federal Computer Commission, then the broadcast flag is the quickest way to do it I can imagine.

We have always joined the FCC in wishing for convergence between digital computer-based tools and the consumer-electronics market, but we dare not accept convergence at the price of mandating a single closed-architecture approach for every computer that wants to be an avenue for television and movie content. Already, new innovative offerings from companies like Hewlett-Packard and Gateway, not to mention TiVo, have made clear the potential for open-architecture computers to serve at the heart of our home entertainment systems and protect content as well.[7]

The studios have acknowledged that the broadcast flag is an incomplete solution,[8] and perhaps not the most robust way to protect content. However, rushing into a scheme that won't actually work to protect content against piracy and then having to go back and redo this again means that consumers may be forced to pay for this technology transition not once, but twice. When we find out that the broadcast flag doesn't work, and then we're told that we're going to need "just this one more thing" again, consumers are going to be faced with another generation of legacy technology, more stuff that they have to throw out. When that happens, they're going to come to Congress for an answer, not to the FCC.

The broadcast flag requires great swathes of the digital environment in the home and in the outside world to be redesigned to monitor for the flag. This cannot be done without great costs, both in allocating design and manufacturing resources and in removing flexibility and value from digital products offered to consumers. Furthermore, the flag scheme isn't even a complete solution. As they have told us, shortly after passage of the flag, the studios will be at the Commission asking for a fix to their "analog hole" problem.

Congress has been told before by studios that if Congress will just give them this one thing and they'll roll out digital television—just give them hundreds of billions of dollars worth of digital spectrum for free and they'll roll out DTV right away—but broadcasters have never given in return any enforceable commitments, and they still look as far away from giving back their analog spectrum as they did at the beginning of this transition.

At the very least, I do not see how or why Congress should allow the FCC to commit to a vast new regulatory scheme without an enforceable timeline for the DTV transition. And I do not see that enforceable timeline on the table right now.

The FCC's broadcast flag rulemaking would also be ill-advised to proceed without Congressional input as to what kind of reasonable consumer uses any such technology mandate must protect. It is inevitable that any protection scheme will involve some choices regarding what uses will continue into this next generation of technology and what uses will not be allowed. If consumers turn on their expensive new DTVs in three years and discover they cannot do many of the lawful and reasonable things they used to be able to do with older technology, it will be Congress—not the FCC—who will be held to answer.

We have seen no technology that demonstrates it is possible to protect fair use and other reasonable consumer uses, while at the same time protecting content from

---

[6] MPAA Broadcast Flag comments at p. 14: "An effective comprehensive solution must be mandated by the Commission for pertinent products. (Although the Commission's notice refers to 'consumer electronic devices,' it is essential, and we assume the Commission intended, that computer or 'IT' products be regulated, as well as so-called 'CE' products.)"

[7] See *Ex Parte Communication* from Microsoft and Hewlett-Packard, *In re Implementation of Section 304 of the Telecommunications Act of 1996; Commercial Availability of Navigation Devices,* CS Docket No. 97–80; *In re Compatibility Between Cable Systems and Consumer Electronics Equipment,* PP Docket No. 00–67, August 8, 2003.

[8] "The Broadcast Flag is only one part of the solution to the problem of widespread unauthorized redistribution of copyrighted content. Other steps include addressing analog reconversion and unauthorized peer-to-peer file trafficking." *See* Joint Reply Comments of the Motion Picture Association Of America, Inc., *et al.,* at 12.

piracy. Before the Commission begins to demand that such a wide range of consumer electronics have the flag in it, they should insist upon a demonstration of the actual technology and show us how it will work.

We support measures to protect content that generally work well, such as encryption or "scrambling" content at the source. That is the approach taken by the DVD market, and even the efforts of a few computer hackers who succeeded in defeating these protection measures had no effect on the DVD market, which continues to grow rapidly. Once again, we favor protection schemes that allow variety and flexibility for consumers—DVDs' content protection does not yet do this, but, unlike the broadcast flag, for example, DVDs make up for this lack in flexibility in other ways, typically by offering additional features. CU believes the market in sales of digital entertainment will continue to evolve, given the right competitive environment, and avoiding a one-size-fits-all government-imposed solution.

The FCC's cable "Plug and Play" agreement (also known as the cable "encoding rules"), which ostensibly sought to "ease the digital transition for consumers" by mandating that digital televisions be compatible with the content protection systems that cable operators are using and will use. But in the process of supposedly facilitating the digital transition, the FCC excluded computers—a device present in approximately 70 million consumers' homes that is capable today of displaying a digital signal.

The Plug and Play order ensures that cable televisions will have content protection built into them, and ensures that the outputs on digital televisions will not be able to hook up with computers or any devices that are not "secure." "Plug and Play" used to mean just that: consumers could buy a device, plug it in, and it worked. Now "Plug and Play" means something quite different. It means, rather counter-intuitively, that consumers' "Plug and Play" TV sets won't work until they get a special card from their cable operators. And in an especially ironic twist, consumers won't be notified that their "Plug and Play" sets won't Plug and Play (because they'll need the security card from their operator) until after they purchase those TV sets. This is a guaranteed recipe to provoke consumer anger.

Depending on the details of the final order, Plug and Play sets the digital TV transition back by not contemplating computers as "unidirectional content receivers" whose generally open architecture, modifiable by the owner, hasn't prevented companies like TiVo from figuring out how to protect content. Furthermore, there are approximately 70 million devices on the market that could receive a digital signal today: personal computers (with a tuner add-on). But the FCC has specifically excluded computers from this agreement. It is ironic that the FCC has trumpeted the coming convergence of the functionalities of computing and television, yet when presented with an opportunity to do something concrete about that convergence, failed to contemplate computers within the scope of the order.

Conclusion

Article 1 Section 8 of the United States Constitution tells us that the goal of copyright is *"To promote the Progress of Science and useful Arts;"* The reason that the Framers put Copyright law into the Constitution was not to protect a small class of citizens who happen to be writers or artists. It was to benefit everybody by encouraging writers and artists to create more. That very same clause says that we have to reward inventors because we know that the health of the Nation is built on technological openness and new frontiers.

The greatest industrial innovation we've seen in the last half century has been cybernetics, the use of tools that process information. Not a year goes by that computing technology does not revolutionize another sector of industry, science, and the arts. We have to find a way to harmonize the creativity of the content producers and the creativity of the engineers and scientists and computer programming that doesn't involve a prohibition of thinking new thoughts and building new devices, but rather embraces an exploration of all the new things that haven't been created yet.

The incredible changes that we've seen in the world are about the fact that literary and artistic creators and engineers and scientific creators have been unfettered and they've found new tools for content. Sometimes these things do shake things up, but we're good enough and clever enough to deal with that.

There are all sorts of ways to protect content that don't involve creating content prisons. We could have digital tools that are interoperable, open, and mutable—and protect content at the same time. Why not set our sights instead on how best to put tools in the hands of inventive men and women, set our sights on how to keep computers open, included in the long-awaited world of convergence, and protect content all at the same time?

The beauty of the computer is that it can be a TV or a typewriter or a recipe book, but recipe books and TVs and typewriters can't be computers. We should not force

computer manufacturers to choose either to continue being open, general purpose devices or to become closed platform media appliances.

Why turn the clock back on computers merely to return to the world of the 1980s? Why aren't we looking forward to a 21st century where individuals get to use the content they pay for more flexibly on more platforms in ways that even better fit their lifestyles and schedules? The best way to allow that is to permit the convergence of communications and computing technologies with mainstream media devices. But the FCC's decisions on the broadcast flag and cable Plug and Play could potentially set us back two decades.

Without computers there would be no TiVo, without the World Wide Web there would be no online programming guides, no radio broadcast over the Internet. There are so many things that computers have enabled—we must aim as high as we can see, aim to have devices not just with features, but with potentials.

Senator BROWNBACK. Thank you, Mr. Murray, and thank the panelists. That is a very good discussion and quite illuminating.

Mr. Blanford, everybody wants to protect the intellectual property rights and recognizes the great stake that our economy has in this, as Mr. Valenti put forward so articulately. And I know that Philips Consumer Electronics wants that technology—or wants that intellectual property right out there as well, because without that you are not going to sell as many devices, either, here or anywhere around the world.

I put forward in the proposal a self-certifying process. How do you see this process working to be able to protect Mr. Valenti's companies' intellectual property right?

Mr. BLANFORD. Mr. Chairman, we believe self-certification would certainly be to the extent that we need technology to do this, and we would concur that technology would certainly play a role along with a number of other mechanisms, including new business models. Self-certification would certainly allow companies such as Philips and others to develop appropriate technologies to meet objective standards to protect the technology without having to work against a specific mandated technology, which we believe if mandated could provide significant anti-competitive effects.

We are very, very concerned about the nature of one technology that would prevent companies like Philips from innovating.

Senator BROWNBACK. Give me an example? Can you give me an example of what you are talking about there?

Mr. BLANFORD. Yes. I believe that certainly an example, a recent example in fact, in the so-called 5C–4C technologies that are proposed here—and let me, if I might, just quickly correct Mr. Valenti because it is related to your question. He referenced a large group that had agreed to the use of those particular technologies. In reality there was a much smaller group that was meeting behind closed doors that we attempted to participate in and were shut out of.

This is a bit of old news in that a year ago we went before the House Energy and Commerce Committee and, with members from both sides of the aisle there, asked that they get this whole issue out of the back room and into an open and transparent vehicle. They chose the FCC and we applaud that, and we are supporting the FCC in this whole discussion and debate. So that is point number one.

With respect to your specific question, already even while this is still under debate in the FCC there has been a unilateral move by the 4C companies to modify the 4C license that is embedded inside

of the potential broadcast flag mandate, without any ability for us to respond to that or to affect it. So we are very concerned about that.

Senator BROWNBACK. Mr. Blanford, my time is short on this. I just want to make the point here, and I want to make sure that this is where Philips Consumer Electronics is, is that you are committed toward protection of these intellectual property rights that Mr. Valenti's companies represent?

Mr. BLANFORD. We absolutely are committed to do that.

Senator BROWNBACK. But you just have a concern that we are going to put some sort of technology mandate, either through the FCC or other route, that you cannot comply with as a consumer electronics company; is that correct?

Mr. BLANFORD. That is correct, or to comply with it it puts us at a competitive disadvantage, similar to the example I used in my opening statement. If you have several companies who are in fact in control of the technology, they know where it is going, and if they can make changes they can—they have the advantage of building into their equipment well in advance of changes in those technologies, those protective technologies, ahead of the rest of the field. That would put us at a severe competitive disadvantage. So that is certainly an issue for us.

Senator BROWNBACK. Mr. Valenti, Dr. Felten is a wise man sitting next to you, he knows the computer industry, and puts forward this concept that we really cannot mandate this technology right now because we do not know for sure where it is going. I have been around here enough to see that when we put something in as a static situation today and things start changing on us tomorrow, we are in trouble because we cannot seem to catch up fast enough with how the changes are taking place. That is the proposal I put forward in this bill: no tech mandate and let us let the industry work with this and work this out.

What is wrong with that model of thinking about dealing with this issue and protecting the intellectual property rights of your industry?

Mr. VALENTI. Well, the principal thing, Mr. Chairman, that gives me a Maalox moment is the fact that you keep waiting, saying you cannot do anything because technology is changing, changing, and changing, and by the time of 2026 that you decide to do something we are dead.

What I take issue with, if for example Mr. Murray says, well, wait until there is a problem, that means you do not put a burglar alarm system in your house until it has been ransacked, then you put the burglar alarm system in. We are trying to look to the future, to save ourselves. I see what has happened to the music industry. It has been pillaged and it is going downhill, and I do not know what is going to happen there. I want to make sure that does not happen to the movie industry by trying to look ahead.

I am not looking for——

Senator BROWNBACK. If I could be real quick, what is wrong with Dr. Felten's line of his saying, here are the ways we need to go at this? He seems to have been pretty thoughtful about that and concerned about your industry as well.

Mr. VALENTI. I am not going to debate computer science with Professor Felten, because I am technologically illiterate. But I have experts around me who I think have the same capacities that he has and that Philips has, and they tell me something different. They tell me that you can make a standard and then on top of that standard people can build their own proprietary interests. Philips can build on that, Microsoft can build on it. But there has to be a standard to allow us to begin now to protect our property.

We are looking at—the digital age will be on us in 2, 3, 4, 5 years. You cannot wait 5 years from now before you begin to set in place the kind of rebuttal that you need to save this industry.

Mr. MURRAY. If I could respond briefly.

Senator BROWNBACK. Mr. Murray.

Mr. MURRAY. I am not saying do not put a burglar alarm on the house. I am saying do not leave the front door open and then say that the problem is the burglar alarm is not there.

Mr. VALENTI. I do not know what that means. What are you talking about?

Mr. MURRAY. The broadcast flag, what it does—my example with the NSA, which I did not really take home. What the broadcast flag does is it transmits all the information in the clear. It is unencrypted. Anybody that can figure out how to just kind of snatch that signal out, that is the front door that is wide open. What it does is it forces us to, instead of closing the front door, it forces us to re-architect all of the consumer electronics and information technology industries.

That is all I am saying, is it is an extremely clunky solution to a problem that could be solved by closing the front door.

Senator BROWNBACK. Dr. Felten?

Mr. FELTEN. Just briefly, Mr. Murray talked about waiting until there is a problem. I think we also need to wait until we know there is a solution. I remain convinced that we do not know how to protect this content, and the broadcast flag as proposed seems not to be the right solution.

The industry, all of the affected industries, are free and they are trying to come up with new solutions and new ideas. I think the best course is to simply allow that to happen. Once we see a technology that can prove itself, then we can move forward to adopt it.

Mr. VALENTI. Senator, I am not here to offer any mandate right now, not at all. We do not have any legislative plans to put before you at all. As a matter of fact, the movie industry is launching a well-funded technological research program that we hope over the next 18 months we can come up with some solutions, enlisting the best brains in the high tech industry, people like Professor Felten and others, to try to find the solutions.

On the broadcast flag, 56 of the most respected companies in the world in the high tech industry believe the broadcast flag as it is now mandated, now designed, will work for over-the-air free broadcasts. What we are trying to say, Mr. Chairman is the broadcast flag embeds a sequence of digital bits in the program, that is all it does. And if you want to send a picture of your baby to your grandmother you can, because the broadcast flag is a sequence of digital bits embedded in a television program, and if a program

comes in that does not have those bits then the flag does not work. It only works with high-value digital over-the-air free broadcasts.

I promise you, sir, that if we go into the digital world and we cannot protect digital free broadcasts they are going to migrate. That is an absolute necessity.

Senator BROWNBACK. As I understand, Mr. Valenti, the 56 companies embraced the concept of a flag that could be used to protect DTV, but they did not necessarily support the MPAA's proposal for the details behind the flag that you put forward. Now, is that correct?

Mr. MURRAY. If I could say, that was never put to a vote in either of the two fora, the Broadcast Protection Discussion Group or the Copy Protection Working Group, to the best of my knowledge.

I would also like to not stand for the proposition that I am saying wait until there is a problem here to protect this content, because that is not what I am saying. I am saying we do have a very real piracy problem, but that piracy problem is being used to sort of get the camel's nose under the tent here where there is not a problem. What I am saying is, if we are going to solve a problem let us get an effective solution on the table. And I agree with Professor Felten: We do not see one yet.

Senator BROWNBACK. Senator Inouye has been patient to allow me. Please. That is pretty much good for me.

Senator INOUYE. In 1959 soon after Hawaii became a state, I found myself, at the request of the State Department, going to the Far East. When I landed in—I will not mention the country. When I landed in my first visit to Asia, I was presented with a gift and the gift was a book, "Advise and Consent." That book had not been published yet in the United States. Later on it became a best seller. The movies had not been made yet.

But here was a book that was counterfeited somewhere in Asia, and the people who presented that to me were rather proud that they were able to steal this from America and give it to me, about the U.S. Senate. Since then I have been quite concerned about intellectual piracy, not just abroad but here.

I have been here for a little while now and every time this matter comes up you have a whole flock of people opposed to it, saying: No, it is too soon; the technology is not ready; you are going to violate rights and everything, etcetera, etcetera, etcetera. Now, if this continues, Mr. Valenti, what is the reasonable future of your industry?

Mr. VALENTI. Well, I think it is put to hazard, Senator. I cannot tell you, but we see what is happening to the music industry. And when you have a 30 percent drop in sales and a continuing drop—it is getting worse—I can see when CalTech's experiment becomes commonplace, when Internet 2, 3 to 4, 5 years from now is in the marketplace, where you can bring down movies in minutes and even seconds, you can imagine what will happen to the kind of thievery that will go on.

As a matter of fact, most of the thievery that is going on now is in colleges and universities, where they have high-speed, large-pipe, high-velocity broadband systems where you can bring down movies a lot faster than you can with a 56K modem.

So I see distress, I see shrinkage, and I see a lot of desolation among the one million people who work in this movie industry. Some of them are going to lose their jobs, there is no question about that, unless we begin to act now. I am not saying today, but I mean an open mind by Congress, not putting any bans on the FCC.

Right now on this broadcast flag, we can argue all we want. There is a concept there. The FCC is deciding now whether or not this implementation ought to take place. That is what its job is to do. Congress set it up to do detailed scientific work that the Congress does not have the capacity to do.

Senator INOUYE. The bill being considered this morning bans technology mandate. Is there a technology mandate that is now under consideration by the FCC?

Mr. VALENTI. Well, yes. The broadcast flag by definition is a technological mandate, yes, sir.

Mr. BLANFORD. With associated encryption technologies, the so-called 5C–4C, Senator.

Mr. VALENTI. I do not know whether this body knows what 5C–4C is. Sometimes when they use acronyms, the people I work with use acronyms, I throw up my hand in frustration and make them spell out exactly what it means.

Senator INOUYE. You know, I am still waiting because people have been all unanimous against intellectual piracy, but I still have hope, but when will this happen? And I am just hoping something will happen.

You have been talking at times on pornography. What are your thoughts on that?

Mr. VALENTI. Well, Mr. Chairman, I am in a business where I have seen a number of pornographic films in my time, and I thought that I had seen it all. But I urge Members of the Congress to get their staff to go on Kazaa, as our people have done, and where you can see "Brittany Spears" or "Disney" or "Harry Potter," which are key words, and what you bring down is material that is so squalid it will shake the very foundations of your comprehension.

The Suffolk County prosecutor convicted 11 people for child pornography on the Internet and he said that the kind of destructive material they saw was the worst in all his 30 years of prosecution. It is unspeakable, where children are doing sexual acts. It is bestiality. It is unbelievable. And guess what, Senator. Any 10-year-old can bring it down and, guess what, probably does.

I think this thing is a national sin and I urge this committee to get their staff to go on there so you can see for yourself this unwholesome squalid material. And it is on all these file-sharing sites.

Mr. BLANFORD. Senator, I would agree with Mr. Valenti's comments about how grotesque it is. But what we are talking about here is broadcast television. I do not think we are talking about pornography being broadcast by our major networks. We are talking about broadcast television and we are talking about whether or not broadcast television that is broadcast should first and foremost, which had been free to air for as long as I know the existence of

television, now being encrypted when they enter the consumers' homes.

So I just want to maybe bring us back on the subject at hand.

Senator INOUYE. How would you solve this?

Mr. BLANFORD. I think what we have argued is that we need, first of all, some time. We are absolutely committed to solving this. The technologies proposed right now do not solve it, for the reasons already commented on here at the table. We think that there could be some superior technologies. We are working, we are actively working on them. Watermarking is one that we are working on at Philips and there are other companies working on it as well.

I think at the end of the day the issue is going to require a host of activities, including education, potentially law enforcement, technology, and new business models. But I again would first bring the Senators back to a fundamental issue that I think the FCC does need guidance on, and we believe in the process that is going on over there, but it is should broadcast television, which has been free to air for all of these decades, fundamentally now be encrypted going forward?

As was already pointed out at the table earlier, you can take broadcast television today in analog form, digitize it, and send it out over the Internet. Yet I do not think we are talking about trying to take today's television and tie it up. This is a fundamental philosophical issue that I do not—I mean, technologists can potentially address this, I think, once Congress provides some direction to the FCC.

Mr. VALENTI. There is a bit of sophistry going on here and let me just break in. What Mr. Blanford is saying is off the mark. We are not encrypting anything. We are putting some little sequence of digital bits in a television program that the customer will not know anything about. It will not bother him at all, unless, unless he tries to take that digitized program, not analog but digitized program, and send it back to the Internet, where it is open and naked and prey to everybody.

That is all it is. It is a very simple thing. And by the way, the experts that I have consulted—and I think they are as wise as the people at this table—tell me this is not a big deal. And the cost is not, as Mr. Blanford said, in dollars; it is in cents.

Mr. BLANFORD. Let me just——

Mr. VALENTI. Let me just finish and then I will let you go.

Mr. BLANFORD. That is fine, go ahead.

Mr. VALENTI. I bought this mike and I am going to use it, as President Reagan once said.

Senator BROWNBACK. Please proceed, Mr. Valenti.

Mr. VALENTI. The only point I want to make is that the broadcast flag is for digitized programs coming into the home. It will not invade, torture, or shrink anything the consumer is doing now, not one bit.

Take off.

Mr. BLANFORD. Thank you very much, Mr. Valenti. I really do appreciate you handing me this mike that you paid for.

Let me just make a comment. We see it very differently. Every consumer will have to replace in essence every piece of equipment in their home in order to work with the new broadcast flag-enabled

equipment. That was what this chart that I presented earlier is all about.

Let me just give you a simple example that may bring this home. Here is the example. A consumer makes a recording with a new broadcast flag-enabled DVD recorder. What happens? The consumer finds that the disk will not play on the DVD player that they already own. The only way to solve the problem is to replace all of the DVD players in their home that they have today. That means that American families will have to replace all 40, 45 million DVD players that are now in the country and in consumers' homes.

This is not innocuous. This is massive, absolutely massive.

Mr. VALENTI. Now, the thing is Mr. Blanford again is dealing in sophistry. You can play it back on the machine you recorded it on. No problem. You recorded it and you play it back on that machine.

The other thing is, though, that he is saying that you have got to replace——

Mr. MURRAY. But can you take it to another location, Mr. Valenti? Can you take it upstairs?

Mr. BLANFORD. You can play it back on that machine, but you cannot play it back on the other three DVD players that you have in your home. Go ahead.

Mr. VALENTI. But you can play it back on that machine.

Mr. BLANFORD. That is correct.

Mr. VALENTI. So you do not have to replace it then, do you?

Mr. BLANFORD. You have to replace the other DVD players.

Mr. VALENTI. No, but you have a machine you can play it on.

Mr. BLANFORD. If you want to always watch your DVD in that location, that is fine.

Go ahead, jump in here.

Senator BROWNBACK. Mr. Murray.

Mr. MURRAY. The only thing I wanted to add regarding whether or not this is going to be a problem in the future, I really—if there is a piracy problem, the broadcast flag does not solve that piracy problem.

Here is what I am saying about the future: We have got a track record with this industry. We were told in 1982 that the VCR was a huge threat. I hope Mr. Valenti will forgive me for reading from his testimony from the House Judiciary Committee on April 12, 1982:

> "The question comes, what is wrong with the VCR? One of the Japanese lobbyists, Mr. Ferris, has said the VCR is the greatest friend that the American film producer ever had. I say to you that the VCR is to the American film producer and the American public as the Boston Strangler is to the woman home alone."

He continued on: "We are going to bleed and bleed and hemorrhage unless this Congress at least protects one industry that is able to retrieve a surplus balance of trade and whose total future depends on its protection from the savagery and the ravages of this machine."

The VCR has become one of the most lucrative slices of the movie industry's copyright pie. If they had shut it down then, one of the

main sources of revenue that not only these companies but this country enjoys would have been precluded. I am just suggesting that perhaps their foresight is not 100 percent, as, humbly, I would suggest mine is not. But that is why we should not lock in a tech mandate on this.

Mr. VALENTI. Mr. Chairman, I would like to say that——

Senator BROWNBACK. Just a second.

Mr. Inouye, do you have any other questions, Senator Inouye?

Senator INOUYE. This is so interesting.

[Laughter.]

Senator BROWNBACK. It is entertaining.

Mr. VALENTI. Mr. Chairman, if I may. I hope that Mr. Murray some time in his life says something that somebody quotes it back 28 years later. Frankly, I think that is a memorable phrase, and it is the only thing I have ever said that has lasted 28 years. So I am very grateful that I said it.

Mr. MURRAY. Touché.

Senator BROWNBACK. I think the point, though, is that we are trying to balance what the industry, the hardware industry, can do and the protections of intellectual property rights. And this has been a long, ongoing battle, as Senator Inouye has noted during his tenure here in the Senate.

So what I am trying to put forward in a bill is a sensible—what I hope is a sensible approach to deal with this, to protect the rights along with being able to move this on forward. So I would hope that all would look at that as trying to balance what we do, because we want to protect intellectual property rights. At the same time, we want to do something we can get done and make sure that we maintain some malleability to be able to maneuver in the future and not lock it down at a technology freeze point when the technology, as several of you noted, will change and change rapidly in the near future.

It has been a very informative panel, engaging as always, and I thank you all very much. Thank you, Senator Inouye, for attending.

The hearing is adjourned.

[Whereupon, at 12:38 p.m., the Committee was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Today, the Committee returns its attention to the vexing problem of digital piracy. While roughly 18 months have passed since our last hearing on this subject, I regret to say that the problem of digital piracy is getting worse, not better.

Without question, advances in digital technology and the growing popularity of decentralized file sharing services such as Morpheus and KaZaa (cuh-zah) are resulting in an enormous drain on the music business and other content industries. According to one recent analyst report, each month there are 2.6 *billion* illegal downloads of audio files. Not surprisingly, CD sales have dropped 26 percent since 1999. At the same time, the yearly numbers of blank, recordable CDs sold at retail increased by 40 percent in 2002, and now outsell prerecorded CDs by 2 to 1.

In addition, even though today's limits on broadband capacity make it much easier to download a 3 minute song than a 30 minute television show or a 2 hour movie, the movie and television industries already face a significant threat. Today, MPAA estimates that over 600,000 video files traded *per day* over the Internet. Moreover, in the first 5 months of 2003, 16 million blank DVDs were shipped, perfect for burning large video files. In addition, over 70 million copies of DIVX, a compression technology that permits more efficient storage and distribution of video content, have been downloaded. As one analyst surmised recently, Hollywood has roughly a "two-year window" before it experiences the same rampant piracy problems that currently plague the music industry.

Despite clear evidence of the problem before us, there are an alarming number of industry groups who continue to stick their heads in the sand. The latest chapter is being written by those wishing to re-open the compromise struck between the content community and Internet Service Providers (ISPs) through the passage of the Digital Millennium Copyright Act of 1998. Under Title II of that Act, ISPs received liability protections in exchange for assisting copyright owners in identifying and dealing with subscribers who steal copyrighted works. As many of my colleagues are aware, claims raised today about the privacy implications of the DMCA are currently being litigated in courts across the Nation.

As the author of consumer privacy legislation that was favorably reported out of this committee last year, I recognize the importance of these issues. As such, I welcome the exploration of ideas to protect the personal information of innocent subscribers. But in doing so, we must be wary of solutions that prevent copyright owners from swiftly identifying those stealing copyrighted works. On that score, our message should be clear, we will not condone piracy under the guise of protecting privacy.

In addition, today's hearing also allows us to examine the proper role of government in facilitating the implementation of copy protection solutions. As I have noted previously, Congress and the FCC have a long history of working with industry to adopt technology mandates that benefit consumers.

In 1962 under the All Channel Receiver Act, Congress mandated that all television receivers include the capability to tune all channels (UHF and VHF) allocated to the television broadcast service. More recently, in 1998, Congress required that all analog VCRs recognize a standard copy control technology (known as "Macrovision"). In the former case, the Federal Government and the FCC took the lead. In the latter case, industry first agreed upon the "macrovision" standard and Congress validated the agreement in legislation. So, whether Congress or industry has led the way, the results have benefitted consumers and industry, by providing Americans with wider access to programming and content.

At present, the FCC is considering yet another technology solution known as the "broadcast flag" designed to spur the digital television transition and provide consumers with ready access to high value, digital television content. This technology has already been endorsed by a large cross section of industry participants and has been awaiting Commission action since the fall of last year. As a result, it is my

hope that the FCC will act swiftly, responsibly, and consistent with the public interest to ensure that consumers receiving over-the-air signals are not left with second class content.

Given the importance of these issues, I look forward to hearing from our panels today.

○