S. HRG. 108–252

THE DARK SIDE OF A BRIGHT IDEA: COULD PERSONAL AND NATIONAL SECURITY RISKS COMPROMISE THE POTENTIAL OF PEER-TO-PEER FILE-SHARING NETWORKS?

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JUNE 17, 2003

Serial No. J–108–17

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
91–213 DTP WASHINGTON : 2003

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa	PATRICK J. LEAHY, Vermont
ARLEN SPECTER, Pennsylvania	EDWARD M. KENNEDY, Massachusetts
JON KYL, Arizona	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin
JEFF SESSIONS, Alabama	DIANNE FEINSTEIN, California
LINDSEY O. GRAHAM, South Carolina	RUSSELL D. FEINGOLD, Wisconsin
LARRY E. CRAIG, Idaho	CHARLES E. SCHUMER, New York
SAXBY CHAMBLISS, Georgia	RICHARD J. DURBIN, Illinois
JOHN CORNYN, Texas	JOHN EDWARDS, North Carolina

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

THE DARK SIDE OF A BRIGHT IDEA: COULD PERSONAL AND NATIONAL SECURITY RISKS COMPROMISE THE POTENTIAL OF PEER–TO–PEER FILE–SHARING NETWORKS?

TUESDAY, JUNE 17, 2003

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The committee met, pursuant to notice, at 2:08 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senator Hatch.

Chairman HATCH. Sorry I am just a bit late. I understand Senator Feinstein has another appointment, so we are going to take her first, even before I make opening remarks. It is good to have you here, Tom, as well. We will take your statement first, too, after Senator Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thanks very much, Mr. Chairman. I Chair a Senate Cancer Coalition and we have got a very interesting meeting that starts just about now to begin. But I feel very strongly about this issue, so I very much appreciate an opportunity to testify.

This hearing is on peer-to-peer networks and security risks. Now, peer-to-peer software is a technology that allows Internet users around the world to share files with each other very easily. All you need is some software, which can be obtained free, and an Internet connection, and your files are instantly made available over the Internet. This technology can be used to help researchers share information or files seamlessly across borders or to help business people share documents. In other words, there are good, positive, legitimate reasons for this.

But as with many new technologies, there are also serious risks. One such risk is the recent explosion of illegally shared copyrighted files over the Internet, most of it occurring through these relatively anonymous peer-to-peer networks. Using this free software, one Internet user can simply put his or her entire music collection onto a computer and then open that computer up to the entire rest of the world, allowing anyone else with an Internet connection and similar software to find the music, to download it onto their own

computers, and to listen to it at will without compensating the copyright holder, something that we have spent a lot of time on.

Meanwhile, these peer-to-peer networks are also facilitating a new era of easily obtainable pornographic material, including child pornography. MediaDefender, a company that will testify today, has estimated that more than 800 universities are hosting child pornography on their networks.

Of most concern, however, is the use of peer-to-peer file sharing by government employees. According to recent studies, the vast majority of peer-to-peer users have no idea of the breadth and scope of data they are sharing with users. A Federal employee intending to simply download and share music files, therefore, could easily make available every file on his or her computer, without intending to do so or even realizing it after the fact. This could include personal correspondence, private financial information, and even proprietary and sensitive government documents.

For normal users, this lack of security presents the real threat of identity theft. Stored credit card information, financial documents of all kinds, personal information, like birthdays, mother's maiden names, you name it, all of this is often stored on an individual's computer and all of it can thus be compromised if the user is not careful when setting up peer-to-peer software.

For government users, the situation is far worse. Not only personally sensitive information can be stolen, but information vital to the functioning of government, as well. Confidential memos, Defense Department information, law enforcement records, all could be available to any Internet user with some free software and the desire to go looking.

The scope of the problem is unclear. Nobody really knows how many government employees are using this software and what level of risk there truly is. But one thing seems clear. The risk is not worth it.

According to recent reports, it appears that many government employees are indeed using time at work to set up peer-to-peer software on government computers. They search for, they obtain pornographic data of all kinds. That is illegally downloaded and distributed, copyright material, as well. Each of these activities reduces work productivity. Many of these violate the law. And most importantly, the entire process opens those computers and computer systems to invasion by outside entities.

The House and the Senate have already prohibited the use of this technology on Congressional computers, as I understand it, for these reasons. I am in the process of preparing a letter to the Cabinet heads of each Secretary asking them to look into this problem and work toward addressing it within each of their organizations, and I would like to give this to you. Perhaps you and others on the Committee might wish to either take it over or sign onto it at your pleasure.

But there can be no doubt that the widespread use of these new technologies represents a grave security risk to this nation and should be treated as such.

So, Mr. Chairman, this should be a very interesting hearing. I am sorry that I can't stay. I am very interested in the topic and

look forward as a member of the Committee working with you and see what we can come up with.

Chairman HATCH. Thank you, Senator Feinstein. We appreciate your hard work on this Committee and your interest in this subject, so we will let you go so you can keep your appointments.

Senator FEINSTEIN. Thanks very much.

Chairman HATCH. Thank you.

[The prepared statement of Senator Feinstein appears as a submission for the record.]

Chairman HATCH. Representative Davis, we are honored to have you come over from the House. We welcome your testimony.

STATEMENT OF HON. TOM DAVIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Representative DAVIS. Thank you very much. As you know, we have held hearings on the House side and look forward to working with you on what can be done about this important issue.

I associate myself with Senator Feinstein's remarks. I agree with what she said.

As you know, our Committee on Government Reform, which I Chair, has been investigating some of the risks associated with the use of these programs. File sharing programs are Internet applications that allow users to download and directly share electronic files from other users who are on the same network. These programs are easily installed and permit the sharing of files containing documents, music, or videos, free of charge.

Now, file sharing is surging in popularity. The most popular file sharing program, Kazaa, has been downloaded almost 240 million times, making it the most popular software program downloaded from the Internet. File sharing programs are increasingly popular with kids. Research has shown that more than 40 percent of those who download files from peer-to-peer networks are under the age of 18.

The technology underlying file sharing programs is not inherently bad, and it may turn out to have a variety of beneficial applications. However, as our Committee has learned, this technology can create serious risks for users.

Most of the news coverage on file sharing focuses on one issue, the ability of users to trade copyrighted music, movies, and videos. Our Committee is investigating other aspects of file sharing. In March, we began our investigation by holding a hearing to examine the extent to which pornography, including child pornography, is traded on these networks. Last month, we held a second hearing to review the personal privacy and computer security risks posed by the use of these programs.

At our first hearing, we learned that peer-to-peer networks have become an increasingly popular mechanism for trafficking in pornography, including child pornography. In fact, it seems as if many of these programs have become digital pornographic libraries where all sorts of pornographic materials can be easily accessed for free.

At the Committee's request, the GAO searched file sharing programs and found hundreds of pornographic images, more than half of which was child pornography and graphic adult pornography. Research performed by another witness at our hearing found that

nearly six million pornographic files were available for downloading on one popular peer-to-peer network over a two-day period.

These findings are very disturbing. Many of these pornographic images are appearing on our children's computer screens whether they ask for it or not. Innocent searches for files using the names of popular cartoon characters, singers, and actors produce thousands of graphic pornographic images, including child pornography.

At the hearing, we issued a report detailing our findings and I would urge parents to review it in order to become familiar with these issues. We also developed a list of non-technical actions parents can take to reduce or eliminate their children's exposure to pornography on these networks. This list is available on the Committee's website.

Last month, we held a second hearing to examine threats to personal privacy and computer security posed by the use of file sharing programs. Despite the surging popularity of these programs, few people recognize the risks that this technology presents. For example, through a couple of simple searches on one file sharing program, Committee staff easily obtained completed tax returns with Social Security numbers, including the names and Social Security numbers of spouses and dependents; medical records; confidential legal documents, such as attorney-client communications regarding divorce proceedings and custody disputes; business files, including contract and personnel evaluations; political records, including campaign documents and private correspondence with constituents; and resumes with addresses, contact information, job histories, salary requirements, and references.

There are several possible causes for the sharing of personal information over these networks. Users could accidentally share this information because of incorrect program configuration. We learned at our hearing that the installation and set-up process can be confusing and can cause users to unwittingly expose their entire hard drive.

Unintentional sharing of personal information can also result from the sharing of one computer among several users. For example, a teenager sharing a computer with his or her parents may elect to make all the contents of the computer available for sharing without thinking about the types of files stored on the computer.

Users may also intentionally share these files because increased file sharing earns the user higher priority status, resulting in faster downloads of popular files.

Either way, the public should be aware that these programs could result in the sharing of personal information which can open the door to identity theft, consumer fraud, or other unwanted uses of their personal data. Parents, businesses, and government agencies also need to be aware of these risks if file sharing programs are installed on their office and home computers.

And finally, another privacy concern raised by peer-to-peer sharing is bundling of these programs with software known as "spyware" and "adware." These programs monitor Internet usage primarily for marketing purposes, often without the user's knowledge. They also give rise to pop-up advertisements and spam e-mail.

Finally, computer viruses can easily spread through file sharing programs, since files are shared anonymously.

I commend this Committee for looking at these important issues. Computer users at all levels of expertise must understand and appreciate the risks associated with the use of this technology. Because of the privacy and security risks, users must fully understand which files are being shared. File sharing companies must also play a role in helping to protect personal privacy and make the programs safe for use by kids. At a minimum, instructions for installing and configuring these programs should be easy to understand and should be designed with the least technologically savvy user in mind.

Once again, thank you for allowing me to testify.

Chairman HATCH. Thank you, Representative Davis. We are happy to have you here on this side of the Hill and happy to have that testimony. We will excuse you if you need to get back.

Representative DAVIS. I will wait for Mr. Waxman for five minutes and then we will walk over.

[The prepared statement of Representative Davis appears as a submission for the record.]

Chairman HATCH. All right. I will turn to my friend, Henry Waxman, as well. Good to see you, Henry.

Representative WAXMAN. Thank you very much, Mr. Chairman.

Chairman HATCH. We just had a hearing this morning on Hatch-Waxman or Waxman-Hatch. I know it depends on which side of the Hill.

[Laughter.]

Chairman HATCH. I was honored to work with you on that as we have on so many health care issues and I look forward to hearing your testimony on this.

STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Representative WAXMAN. Thank you very much, Mr. Chairman. I was honored to work with you on that legislation and we did a lot of good in the days when we were working together on health issues.

But I come to you today to talk about another issue where I hope we can work together, if we could find some solution, legislative solution, to a problem that is really quite perplexing, and that is what happens when there are peer-to-peer networks and file sharing programs. Chairman Davis and I have worked closely together to bring attention to this technology and the questions it raises.

This technology is in many ways a bright idea, as you indicated in the title of the hearing. It is a unique and innovative use of Internet technology. But it also carries significant risks that most people don't know about. These programs are incredibly popular with young people. They have been downloaded literally hundreds of millions of times, and for teenagers and people in their 20s, peer-to-peer file sharing programs are as common as a computer application as e-mail and word processing programs are for the rest of us.

But my concern is that there is a digital generation gap when it comes to understanding these programs. Parents simply don't have

the knowledge about these programs that their children do, and as a result, many parents are unaware of the special risks posed by these programs. How many parents realize that these programs, if carelessly installed, can make every single bit of electronic information on a family computer available to millions of strangers? Very few.

The Committee's first investigation into peer-to-peer technology looked at one of the risks posed by file sharing programs, the prevalence of pornography. We learned that these peer-to-peer networks operate like a vast library of free pornographic content. Any child that has access to a broad-band connection can easily find and download the most hard-core triple–X videos imaginable in just a matter of minutes at absolutely no cost. They are pushed, this is all pornography is pushed on kids who may be looking for Britney Spears or some other popular artist.

GAO reported at our hearing that kids are bombarded with this pornography even if they are not looking for it. We feel that parents need to be aware of this so they can talk to their kids and be advised that their kids may be having this kind of junk forced on them.

Peer-to-peer programs connect users from anywhere in the world into a vast open, free trade network, where with the click of a mouse, users can share files back and forth with other users across the globe.

Our staffs installed Kazaa—it is the most popular file sharing program—and ran test searches to see what kind of information people were sharing unintentionally, and what we found was amazing. We found complicated tax returns, medical records, and even entire e-mail in-boxes through simple searches using file share programs. We also found that other incredibly private documents, such as attorney-client correspondence relating to divorce proceedings and living wills, were also available. We found that tax returns and other private information could be downloaded by somebody who was using the file sharing at the same time.

We prepared a report on our findings and I would like to submit it to you, Mr. Chairman, for your record and be included in this hearing.

Chairman HATCH. Thank you. We will include it.

Representative WAXMAN. I welcome the interest of your Committee in exploring this new technology. There is much this hearing and future ones can add to our understanding of file sharing programs. We need to work together on this issue. It has become a vehicle for pornographers, for intruders, for new technology that can lead to greater education. There are ups and down sides to this new technology and we need to figure out what is a rational approach to dealing with the down sides to it.

Thank you very much.

Chairman HATCH. Thank you very much. I am very impressed that you two friends would come over here and help us to understand this better, so we appreciate you being here.

Representative WAXMAN. Thank you very much.

Chairman HATCH. Thanks.

[The prepared statement of Representative Waxman appears as a submission for the record.]

STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. We will excuse both of you and let you get back to your busy lives. Thank you for coming.

Our second panel includes four witnesses from the private sector who have taken leading roles in identifying and resolving the security concerns associated with peer-to-peer networks.

Last year, Nathaniel Good and Aaron Krekelberg published a ground-breaking study entitled, "Usability and Privacy: A Study of Kazaa P2P File Sharing."

Our next witness will be Randy Saaf, the President of MediaDefender, Inc., a leading provider of computer security services to private and governmental entities.

Next, we will hear testimony from Alan Morris, the Executive Vice President of Sharman Networks, Limited, the company that owns and operates the Kazaa peer-to-peer file sharing program. Mr. Morris is joined by Mr. Derek Broes, the Senior Vice President and Assistant General Counsel of Brilliant Digital Entertainment, the parent company of Altnet, the North American business partner of Sharman Networks. Altnet has provided a written statement for the record and Mr. Broes may assist Mr. Morris in responding to any questions relating to the activities of Altnet.

And finally, we will hear testimony from Mr. Chris Murray, Legislative Counsel for Consumers Union.

I want to thank you all for being here today and welcome you all here, but I think what I am going to do is first make my opening statement and then turn to you, in that order. We will start with Mr. Good and Mr. Krekelberg and then go across the way.

We are here today to explore some potentially troubling aspects of an exciting technology that rightfully has gained the attention and admiration of millions and millions of Americans, and many millions more around the world, peer-to-peer file sharing networks. Recent developments in peer-to-peer networks have added dramatically to their versatility and, therefore, their utility to many computer users.

Napster, the first peer-to-peer system, permitted the sharing of audio files only, but newer generations of this technology permit the sharing of all types of computer files, including audio files, video files, visual images, documents of all kinds, and computer programs. These advances have been accompanied by a soaring increase in the use of peer-to-peer networks.

Kazaa, the most popular of these networks, is now the most popular download on the "downloads.com" Internet site. Kazaa and other file sharing programs have now been downloaded over 400 million times. Kazaa often has over four million users connected to its network simultaneously.

The demand for other popular P2P programs such as Grokster and Morpheus is growing rapidly, as well, and mostly among minors. Research shows that about 41 percent of those who download files over P2P file sharing networks are between the ages of 12 and 18. These statistics underscore the great appeal and promise of P2P networks as well as the potential scale of any problems that they create. They permit rapid and broad dissemination of information and ideas and they have provided a powerful tool to research-

ers, hobbyists, and interested citizens seeking information and ideas on a wide array of topics.

At the same time, however, they have also opened up our homes, our businesses, and our governmental agencies to potentially serious security risks that are neither widely recognized nor easily remedied. Recent studies involving some of the more popular P2P networks suggest that a significant number of their users are inadvertently sharing personal and highly-sensitive data over these networks, including tax returns, bank account information, personal identifying information, passwords, and e-mail in-boxes.

While the true scope of this problem is still unknown, studies have shown that potentially malicious parties are searching P2P networks for personal e-mails and credit card numbers. This alone is disturbing, but in government agencies, employees' use of P2P networks could also disclose sensitive government data to the enemies of this country. At this moment in history, the implications of this risk or the risks involved are trembling, to say the least.

I am also troubled that many P2P networks require their users to install so-called "spyware" or "adware," programs that monitor, collect, and record information about the Internet browsing habits of a particular user. Such programs can collect and disseminate information about the Internet use and personal information of anyone using the computer on which a P2P networking program has been installed. The invasion of privacy and potential for identity theft inherent in such programs has already attracted justifiable attention from members of Congress and consumer advocates concerned about the privacy and security implications of such practices.

In addition, some of the spyware or adware programs can also wreak havoc on a user's computer by commandeering their browsers, creating conflicts with other software that can crash a user's computer and otherwise interfering with users' control over their own computers.

Finally, the users of P2P file sharing networks may also encounter malicious programs, such as viruses, worms, and trojan horses that have been disguised as popular media files. Indeed, the operators of the most popular file sharing program recently explained to the House Committee on Government Reform that "when files come from anonymous and uncertified sources, the risk of those files containing a virus greatly increases."

If the promoters of these networks acknowledge that their nature increases users' risks of exposure to malicious programs, then they must also recognize their increased duty to protect and educate their users.

I do believe that peer-to-peer file sharing networks are here to stay, but the problems of data privacy, spyware and viruses should remind all of us that the final role of peer-to-peer file sharing networks in our culture remains to be seen.

This technology has great promise, but also some potential pitfalls. If these networks are designed to minimize the risks of file sharing, then the promises of this technology can become reality. If not, then users, network administrators, and others may ultimately conclude that the risks of this technology outweigh its advantages.

I would like to thank all of our witnesses for appearing here today to address these important issues. We are particularly privileged to have with us three of our colleagues whose stellar work in this area has shed much needed light on the significance of the risks, as they have mentioned in their statements, and we appreciate that. They talked about their potential consequences, as well. So I was happy to have Senator Feinstein and Congressmen Tom Davis and Henry Waxman here with us today.

So we are delighted to have all of you here today. We will start with you, Mr. Good and Mr. Krekelberg, and you just take over. We are going to give you only five minutes apiece, so I hope you can all stay within that time frame.

Mr. GOOD. We will try. Thank you, Mr. Chairman.

Chairman HATCH. We will try and be liberal in the use of time.

STATEMENT OF NATHANIEL S. GOOD AND AARON KREKELBERG, AUTHORS OF "USABILITY AND PRIVACY: A STUDY OF KAZAA P2P FILE SHARING"

Mr. GOOD. Good afternoon, Mr. Chairman. Thank you for the opportunity to appear before you here today. In the brief amount of time that we have, we would like to look at a study that we performed on a peer-to-peer file sharing program called Kazaa. In this study, we will discuss how configuration problems could contribute to users of P2P networks inadvertently sharing their personal and private information.

In this study, we addressed two major issues. One issue is that users of P2P systems don't always realize what they are sharing with others on the P2P network. In other words, sometimes people may think they are sharing one thing, but they are actually sharing something completely different.

The second issue is that the kind of problem we have discovered is a problem with the program's usability and the interaction between the application and the user. It is different than other problems that are frequently mentioned in the media because it is something that can't be patched in a traditional sense that requires a redesign of the program's way of interacting with the user, as well as educating the user to the potential problems that could occur.

We felt that the file sharing on P2P systems could be secure and usable if users were made clearly aware of what files others can download, that they are able to determine how to share and stop sharing files, that the system does not allow users to make dangerous errors that lead to unintentionally sharing private files, and that users are comfortable with what is being shared and confident that the system is handling it correctly.

By looking at the interface and performing a user study, we were able to determine that certain parts of the Kazaa application could be confusing to users and relied heavily on unstated assumptions. In some cases, it was possible for the user to think that what they were sharing was completely different than what was actually being shared.

There are too many details to cover in the time that we have allocated, but a majority of the details are in our research paper and written testimony.

On the screen in front of you is Kazaa. Kazaa is the most popular P2P file sharing program on the Internet today. With Kazaa, you can look at any type of file, such as music, documents, videos. Anything that can be stored on your hard drive can be shared or downloaded from others. To do this, one would download the application and type the keywords that one is looking for into the search box. Kazaa then returns the search results to the window to the right of the search screen. Users can download other files or see files from other users.

In any peer-to-peer system, the user has to make two important configuration choices. They have to decide where they are going to store files that they download from the network and what files they are going to share with others. In most peer-to-peer systems, the folder that one chooses to save the files to is also the one that is shared with other users. In addition, all files and folders contained in that location are also typically shared.

So in the next couple of slides, we will be describing some points of confusion that may cause people to share more than they realize and possibly share private information. Again, there are many more details that we could go over, but due to the brevity of this testimony, we will just go over some of the most important ones and focus in on one of the worst-case scenarios.

The first problem we will describe is when users specify the location they would like to store downloaded information to. The problem here is with terminology. There is no indication that these files and folders will also be shared, as well as all files and folders contained in whatever folder you specify. There is also no description of the types of file types that can be shared. In addition, this is the only location where users can disallow sharing with other users.

Another problem that we discovered was with the Search Wizard and the folder list, which were two interfaces that were designed to allow people to specify what they could share with the Kazaa application, and in some cases, Kazaa will bring this up when the user is first running the installation for the program.

In the search interface, Kazaa will look through the user's computer and determine what sort of files that they could share with the network. In this case, it came back with "My Documents" file and thought that there would be something good to share there. Unfortunately, it doesn't tell me what it is going to share there and relies on my assumptions of what Kazaa can do in order to share these programs with other people.

In the next interface is a list for browsing the computer hard drive and its contents and users can check off what area they would like to search, or they would like to share with other users. In addition, there is the "My Shared" folder, which is the default folder that things can be shared in, is checked all the time.

The problem in both of these interfaces is that there is no association between what is indicated as shared in the file import and what is indicated as shared in the downloaded folders. So unless users intuitively know that these two are linked, there is no way for them to know that the download folder is also the sharing folder.

While this chance is rare, the confusion that may arise from this problem could confuse users for other situations, as well. In a 1996

USENIX conference, Matt Bished, a prominent security expert, mentioned that configuration errors are a probable cause for more than 90 percent of security failures. Education of users is one means of helping to reduce configuration errors. In addition, providing help and explanations can sometimes be useful, but has limitations. Users rarely read documentation and frequently gloss over privacy statements and textual explanations embedded in the interface.

We feel that the issues we describe would be most adequately addressed at the application level, where they would be most effective. Thank you very much for your time.

Chairman HATCH. Thank you. We appreciate it.

[The prepared statement of Mr. Good and Mr. Krekelberg appears as a submission for the record.]

Chairman HATCH. Mr. Saaf, we will turn to you.

STATEMENT OF RANDY SAAF, PRESIDENT, MEDIADEFENDER, INC.

Mr. SAAF. I would like to thank you for holding this hearing and inviting me to speak. My name is Randy Saaf and I am the President of MediaDefender. MediaDefender is one of the most well-respected peer-to-peer anti-piracy software companies in the world. We have very sophisticated tools for understanding piracy problems on the peer-to-peer network and security problems and we want to share these tools with this Committee.

Usually, only very sophisticated computer users get involved with network and software. In the case of peer-to-peer networking, that is simply not true. The sheer quantity of users of peer-to-peer networking mean that quite a few really don't know that they are opening their computers up to the whole world.

In the summer of 2000, Napster was hitting its stride as the hottest software application in the world. Napster really didn't have very many security problems. It had roughly 40 million users, but it was mainly used to share MP3 pirated music files. Today, the peer-to-peer networks have over 80 million users and they are used to trade all sorts of rich media files, including documents and software applications.

All the security concerns associated with peer-to-peer networking come from the file sharing aspect common to every program. If a user never changes the default settings in a program like Kazaa, they probably won't have any security problems. The problem is that with the sheer number of users, you are always going to have a certain segment that just want to change the settings or don't understand the settings. Many users of peer-to-peer do not realize that the default folder that they download content to is shared up to the entire peer-to-peer network.

A typical scenario of a security risk might be a child who downloads his music files to his parents' "My Documents" folder that contains all their personal tax and financial information, and that folder then gets re-shared to the entire network.

MediaDefender collected data from the sixth to the ninth of this month. We were invited to participate in this hearing on the fifth, so we only had a few days to collect data, but we wanted to get something that was a representative sampling of a security risk. So

MediaDefender looked for Microsoft Money files shared on the Fast Track-based Kazaa network.

Microsoft Money files are personal tax and financial information and there is really no reason somebody would want to be sharing those on a peer-to-peer network. MediaDefender found 8,034 unique Microsoft Money files being shared on the Fast Track-based network on 6,032 unique IP addresses. The larger implication is that probably almost every one of those people were sharing their entire "My Documents" folder on Kazaa because that is where the Microsoft Money file gets saved by default.

So I want to give a brief demo that I did at 12:00 this afternoon at Kinko's, where I just plugged my laptop in and did a search for ".mny." I search ".mny," click enter, and up comes a screen full of Microsoft Money files, and you will notice each one of them has the Microsoft Money extension. I just randomly selected one and did the feature of "find more from the same user." Now, this is a pretty standard feature in Kazaa. Anybody could do this at home. This is no fancy software involved in this.

Clicking "find more from the same user" brought up 1,500 files that that person has shared on their computer, I mean, presumably in their "My Documents" folder, and you can look at the files. They are just a hodgepodge of different types of files, including pictures, private pictures, phone-type information. Obviously, their Microsoft Money file was in there, which presumably contains all their financial information.

A user could then select all those files and just click "download" and have that person's entire snapshot of that person's life. I mean, I can see from the screen here the person goes to Indiana University and there is probably a whole lot of information you can tell about this person in this relatively quick exercise that took approximately five minutes.

So you can see how the clear extension of this problem could be carried over to businesses and government organizations, because for the same reason people don't understand they are sharing documents at home that they don't intend to, people at government organizations will do the same. People want to download their music and movies on their fast Internet connections at work.

So for this particular study, we looked for as many computers we could find with the search phrases "Madonna," "The Matrix," "porn," and "sex." We pretty much arbitrarily chose those search phrases because we knew they would give us a lot of returns, and I don't think any files with these words in them would have any legitimate governmental purposes.

We focused on three government organizations, Los Alamos National Laboratory, NASA, and the Naval Warfare Systems Command. We chose them because they are obviously sensitive organizations that would have sensitive data. We found 155 computers at Los Alamos National Laboratory sharing files on peer-to-peer networks, 138 computers at NASA, and 236 at the Naval Warfare Systems Command. I am fairly sure that these are unintentional sharing, because I don't think anybody in these organizations would be intentionally sharing pornography files and those types of things on a peer-to-peer network at work.

This was not a comprehensive study. We simply wanted to demonstrate there was a problem and we would recommend to the Committee that further studies be done to actually quantify the extent of the problem. Thank you.

Chairman HATCH. And you just did that at Kinko's today?

Mr. SAAF. Pardon?

Chairman HATCH. You just did some of this at Kinko's today?

Mr. SAAF. Yes. I did this part at Kinko's today. It was pretty much a five-minute exercise, what I went through there. It is very fast.

[The prepared statement of Mr. Saaf appears as a submission for the record.]

Chairman HATCH. Mr. Morris?

STATEMENT OF ALAN MORRIS, EXECUTIVE VICE PRESIDENT, SHARMAN NETWORKS, LIMITED; ACCOMPANIED BY DEREK BROES, EXECUTIVE VICE PRESIDENT OF WORLDWIDE OPERATIONS, BRILLIANT DIGITAL ENTERTAINMENT

Mr. MORRIS. Thank you very much indeed, Chairman Hatch, for inviting us to come today and to help the Committee in its determinations about the very important issues of security and privacy in file sharing.

I am the Executive Vice President of Sharman Networks, Limited. I look after the company's business when Sydney is asleep, and importantly, I look after its licensed activities, along with my colleagues here at Altnet. And in that respect, we are the world's largest distributor of licensed files.

When we acquired the Kazaa Media Desktop, or Kazaa, as it is known, we set ourselves two goals. Firstly, to be the premier distributor of licensed files, and with over half-a-million licensed files distributed a day, I think we have achieved that; and secondly, to set the standards in usability.

If I can talk first about viruses, an issue which is very important, we recognized this last year, and everybody knows the effect viruses can have. So we invested in a fully-featured anti-virus program called BullGuard, and BullGuard has been installed as an active part of the Kazaa Media Desktop for over a year now. So no user of the Kazaa Media Desktop need ever be bothered by viruses. It runs there and it is free.

Secondly, inadvertent file sharing. Since we acquired the assets, we have carried out usability tests. We looked at the work that the guys, Good and Krekelberg, did back in April last year on Version 1.7 and we have constantly modified the user interface, because it is important. It is crucial that people don't inadvertently share files. The latest Version 2.5, which is in public beta at the moment, which I am going to send the guys for their comments, makes it very, very difficult, indeed, for somebody to inadvertently share files.

We have used best industry practice, known as, A) make it intuitive, and B) most importantly, make it safe by default. So if anybody tries to share parts of their hard drive which would be inadvisable, they get a very strong notice, like "Do you want to do this?" So I will be very interested in what you guys think about 2.5.

Thirdly, the issues of privacy. Issues have been raised such as spyware. We have got a very strict new spyware policy. We certainly serve advertising. We use proprietary ad serving technology and we have one application bundled which is used by many Fortune 100 companies, and very clearly by our definition it is not spyware.

User education to us is fundamentally important. We accept that responsibility as the leader in the marketplace and we would distance ourselves, I think, from our competitors, if they don't mind us saying that. So on the website, in very clear English, we give very clear guidance about how people can share safely. And again, guys, we welcome your views on that. We talk about issues like cookies and opt-ins. Spam has been mentioned. We have never spammed. We haven't sent it ourselves. And we have never sold any e-mail addresses.

The other issue that has been raised is that of pornography. We totally abhor child pornography. I am a parent myself. What we have is a fully password-protected adult filter. We can't control what is distributed on the network. It is a digital democracy. But what we do is, by default, there is a series of filters for adult and offensive material which is password-protected and it is there to encourage and support responsible parenting.

So we emphasize user education very strongly. The issue that we all face, I think for every application on the Internet, is the extent to which people, as has already been mentioned here, are prepared to accept that education. A recent AOL study on broadband use shows that many people choose not to update their anti-virus software. They choose not to use firewalls. So it does behoove us as the industry leader, and the rest of the industry, to work with the Committee and work with other agencies worldwide to ensure that user education is of the highest standard.

It is particularly important, because in this always-on world, this wide world of broadband, the risks are much, much higher. It is well recognized, I think, that peer-to-peer is the main driver of broadband. It is the thing that drives the broadband future.

So, Mr. Chairman, we are very happy to work with you, with members of the Committee and other agencies in the areas of improving the interface and in the areas of user education.

Chairman HATCH. Well, I appreciate the comments and we will be happy to have you work with us and help us, if we can.

[The prepared statement of Mr. Morris appears as a submission for the record.]

Chairman HATCH. Let us turn to Mr. Murray and Mr. Broes.

Mr. BROES. My statement has already been entered into the record.

[The prepared statement of Mr. Broes appears as a submission for the record.]

Chairman HATCH. Mr. Murray?

STATEMENT OF CHRIS MURRAY, LEGISLATIVE COUNSEL, CONSUMERS UNION

Mr. MURRAY. Chairman Hatch, I am both grateful and honored by your invitation to testify before the Committee today. Consumers Union, as publisher of Consumer Reports magazine, is an

organization that makes its living based on intellectual property, based on compensation for our creation, as well as our reputation as based on the trust of consumers.

Since the first issue of Consumer Reports arrived in consumers' mailboxes in the 1930s, we have built our reputation, I think, on a love affair with technology and a desire to make that technology work better for consumers. Today's hearing presents another opportunity to scrutinize a technology with both enormous potential and enormous problems.

The potential comes in the form of some really exciting new applications that we see, such as peer-to-peer distributed computing. We have got—Oxford's Center for Drug Discovery is using the power of peer-to-peer distributed computing to help come up with new drugs to solve problems like cancer and I believe they are also working on a cure for smallpox.

We have Stanford's "Folding at Home" project, where they are using normal consumers like you and me, they are using our computers to run protein folding sequences, things that just require enormous amounts of processing power that an average research university or library just wouldn't have the funds to undertake.

And we have got normal consumer uses of peer-to-peer technologies. There is a technology out there called Spam Watch right now where it is a collaborative filtering software whereby users flag a particular piece of e-mail as spam, and then when enough users flag that as spam, they say, okay, we are going to shut this person down to the rest of the network.

But we also have seen today it comes with a dark side. As the Committee clearly understands, both the promise and potential as well as the dark side appear, and the dark side that we see and that we are concerned about is two-fold. Number one, the default settings concern us greatly because consumers are unwittingly sharing documents like tax returns, Social Security numbers, private information, money files, as we saw. But there is also this really prevalent use of spyware and adware that concerns us.

I think one of the, if I can jump straight to my punch line, I think perhaps the most exciting near-term role I can see for Congress in this space is to do exactly what you are doing today, which is open this up to sunshine and make sure that people understand what exactly, what risks they are exposing their computers to. That seems to have had some effect. I guess in their latest build, they are saying that they have remedied some of these problems. I hope that we can continue to move the industry along with default settings, make sure that configurations work for consumers.

As I dug into this a little bit in preparation for today's hearing and I looked at where uses of spyware and adware are happening on peer-to-peer, I realized, number one, it is a rampant problem on peer-to-peer and I am quite concerned about it. But number two, perhaps of even greater concern is I discovered that this is all over the place on the Internet. Mainstream providers, such as Microsoft, AOL's Netscape, Real Networks, have features on their software that millions upon millions of users are using whereby they are being tracked. Their music preferences, their reading preferences, their DVD watching preferences are being sent back to companies, in some cases along with a unique identifier which says, this is

what this particular consumer is watching and reading and listening to.

I think we, like you, are believers that if consumers can get information in their hands, they can begin to make some of the right decisions and we can move the marketplace along far.

And so there are three things, if I can just summarize what I would like to say today very briefly, there are three roles that I think Congress can help play.

Number one, education. Users of peer-to-peer systems need to be aware that what they are doing on their computers can expose them to enormous risks. Part of our education problem is that sometimes the users aren't the same people that would be concerned about risks. If I am a parent, I don't necessarily know that my child is going to be downloading Kazaa or Morpheus or Grokster or whatever application onto my system and potentially exposing my files to great risk, and so that this education process needs to extend not only to the people who are using the application, but to parents in general.

The second role I see for Congress is investigation. I would be very grateful if the Chairman would urge the Federal Trade Commission to look into uses of spyware and adware in the marketplace. I see, again, in peer-to-peer, it is a rampant problem, but it is also a rampant problem in the mainstream software applications base.

And the final role I see for Congress is in the policy arena. Sometimes, there is just no educating around a design problem. Perhaps the role that Congress could fill, the gap that Congress could fill would be to provide consumers with as much notice about what is going into the software that they are using on their computers. If there is spyware and adware that comes along with that software, we think that educating consumers—consumers can only be educated if they know exactly what is underneath the hood of that software. So perhaps we could discuss and work with the Committee on coming up with some solutions in that space.

As I said before, I think any solutions we come up with in the peer-to-peer space are going to necessarily extend to the rest of the Internet because the fundamental architecture of the Internet is that of peer-to-peer. Anytime we try to regulate peer-to-peer as such, I think we are also talking about a very broad regulation of the Internet in general. It is difficult for me to imagine a definition of peer-to-peer that doesn't also include applications such as e-mail and instant messaging.

I am very grateful, as I said, Mr. Chairman, for the opportunity to testify here today and we would be happy to continue the conversation.

Chairman HATCH. Thank you. We appreciate all your testimony.

[The prepared statement of Mr. Murray appears as a submission for the record.]

Chairman HATCH. Let me start with you, Mr. Morris. You make the point that parents or employers who own Internet-connected computers must educate themselves about the operation or design flaws of every peer-to-peer software program that might be downloaded by their children or employees and then reeducate

themselves every time any one of these programs is updated or ordered. Is that one of the arguments you are making, that parents—

Mr. MORRIS. No, the argument I make is that, as the leader, we have a responsibility and we take that very seriously. So when people choose to download Kazaa Media Desktop in all the versions from 1.7 up until now, we have done our very best to make sure it is very clear to people what happens, make it very clear to parents exactly how the parental control filter works, and also make it very, very difficult for people to inadvertently file share.

Now, we hope that sets a standard for other people and we hope that other peer-to-peer providers follow our lead, but we can't, obviously, legislate for them.

Chairman HATCH. No, but is it true that anti-virus software distributed with Kazaa is disabled by default when the software is installed? Is that true?

Mr. MORRIS. No. It is currently enabled by default.

Chairman HATCH. It is enabled?

Mr. MORRIS. It was previously disabled. It was an optional choice for people. And now, in the latest version, it is currently enabled.

Chairman HATCH. In your written testimony, you state that, "Users control the material they choose to share with others." This leads me to ask, does Sharman Networks accept any responsibility for the files that are shared inadvertently or even illegally over the Kazaa network?

Mr. MORRIS. No. As I said, we have no control over what is the digital democracy, but we do do our very best to, firstly, when somebody downloads the Kazaa Media Desktop, they have a very clear end user license agreement. We like to believe it is written in plain English, unlike some. And that obliges them to state that they will not infringe copyrights. Now, we can't police that. And all over the website, you'll see statements like, "Do not infringe copyright." And certainly with pornographic material, we have the parental control feature, but we cannot police the network. It is physically and technically impossible.

Chairman HATCH. Mr. Good and Mr. Krekelberg, let me ask you this question. I would like to commend both of you for identifying the data security problems potentially associated with peer-to-peer file sharing. In your testimony, you state that these problems are not intrinsic to peer-to-peer technology, but derive from the design of the Kazaa program. Now, do you know whether any similar problems affect other file sharing programs?

Mr. GOOD. As stated earlier when we were giving our demonstration, all peer-to-peer file sharing systems have to do two things. They have to say what you are going to save and where you are going to save it to, and also what you are going to share. So any peer-to-peer file application, you have to address those problems somehow in the interface, and so not only with Kazaa, but other peer-to-peer file sharing programs, you have the same sort of issues that would arise.

Chairman HATCH. Do you have anything to add, Mr. Krekelberg?

Mr. KREKELBERG. The point we were trying to make with that statement is that peer-to-peer technology is not fundamentally flawed where people will just start sharing all their stuff. There are some user interface issues that need to be addressed with most

of these peer-to-peer clients, that users accidentally share things they don't want to share.

Mr. GOOD. In addition, we have looked at some other peer-to-peer file sharing programs and they seem to have similar sort of issues that Kazaa would have.

Chairman HATCH. I am going to submit for the record written testimony from the Business Software Association.

But let me ask you, Mr. Saaf, how often are peer-to-peer networks updated or altered to circumvent firewalls, filters, and other security measures that computer owners might take to protect themselves from the risks that are outlined by your testimony here today? I mean, who makes these alterations and why are they done?

Mr. SAAF. Well, peer-to-peer file sharing networks are frequently updated. I am not sure that they are really updated to circumvent anything per se. Sometimes, they may be. That is really—I would have no idea. I do think that a fundamental issue with the peer-to-peer networking is that you are going to have to get rid of some of the cool things about the peer-to-peer networking to take care of a lot of fundamental problems, like child pornography and security.

The bottom line is, if you leave a peer-to-peer network wide open for anything to be shared, you are always going to run a risk that people are going to share the wrong stuff. So it is going to be this tension of give and take, and I think eventually the peer-to-peer networks may have to give up some of the cooler functionality if they are going to seriously take care of the piracy and child pornography and security concerns.

Chairman HATCH. In your experience, how many peer-to-peer sharing programs install spyware and adware programs?

Mr. SAAF. I mean, most of them. They need to make money to pay their staff. Typically, it is free software, so there has to be some method of getting revenue. But like was stated in other people's testimony, that is not totally uncommon on the Internet. A lot of software does have spyware and adware.

And again, you know, if you don't have as much money to pay programmers to develop cool peer-to-peer applications, then the applications won't be as cool. So if you get rid of the spyware, then all of the sudden the company doesn't have the money to develop the peer-to-peer applications. It is going to be always a tension.

Chairman HATCH. What can these programs do to their host computers?

Mr. SAAF. What can they do?

Chairman HATCH. Yes.

Mr. SAAF. You mean in terms of damaging those computers? Well, the problem with any sort of spyware or adware or really any sort of software that is unregulated or not operated by a big company is it is not always necessarily designed perfectly, and what could end up happening is two or three spyware or adware programs just conflict with each other. You might have a spyware that gets installed with one version of a peer-to-peer networking software and a spyware that gets installed with another version of a different peer-to-peer networking software and those two spywares just don't know how to be graceful with each other, whereas you

are not going to run into those same sort of problems with, like, Microsoft Word and Microsoft Power Point, because those are very well designed programs that have millions of dollars of development in them.

Chairman HATCH. Mr. Murray, do you have anything to add here or what we might do in Congress besides what you said in your testimony?

Mr. MURRAY. Well, that is an excellent question, Senator. Perhaps I could briefly add Consumer Reports' recommendations to users as to what we can do in general to protect ourselves, a couple quick things.

Number one, you should have some form of virus software installed in your computer and you should update that at least weekly. If possible, we recommend for users, especially anybody that has a broadband connection, because a persistent broadband connection presents a lot of the same risks that peer-to-peer does, you can be quite transparent to the world with some very simple hacking tools—

Chairman HATCH. So every time it comes up on the screen, you ought to click onto it.

Mr. MURRAY. The updated—

Chairman HATCH. Yes.

Mr. MURRAY. As annoying as it is, yes, Senator, I believe that is the right answer. You should go ahead and say, yes, update my files, at least weekly is what we recommend. But for broadband users especially, we recommend putting in place a firewall, which can either be a piece of software or actually a physical router with a firewall which goes behind your modem. That can go a long ways towards making your computer opaque to the rest of the world.

If users are going to use peer-to-peer software, we also recommend that they download it from one of the major portals. One of the bigger problems that we are having is that a piece of software such as Kazaa's Media Desktop, there are all of these third-party sites out there which say, hey, if you come to me and pay me a dollar, I will let you have Kazaa, when they, in fact, have nothing to do with Kazaa, and some of the worst forms of spyware and adware that we have seen have to do with these third-party distributors. So we recommend, again, a lot of what goes on in these networks is illegal sharing of intellectual property. So we are not meaning to endorse that in any way, but insofar as there are legitimate uses of these networks, you should download it from a major portal.

Chairman HATCH. I am going to put Senator Leahy's statement in the record. He could not attend this hearing, but he wanted to. He takes great interest in these matters, so I will put his statement in the record immediately following my statement.

Let me just ask one last question. I have heard that with regard to piracy problems and the stealing of music and copyrighted material, that there is now a software or at least a methodology of giving a warning that what you are doing is an illegal act, giving another warning, and then finally just destroying their computer. Are you aware of that, the warning that we are going to destroy your computer if you keep doing this illegal act? Can somebody help me to understand that?

Mr. MORRIS. Derek is one of the foremost experts on security issues in P2P, so I think I would ask Derek to answer.

Chairman HATCH. I have been wanting to ask you a question, so this is a good one for you.

Mr. BROES. First, I should explain my role in this is that Brilliant Digital and Altnet, we are the commercial component to Kazaa Media Desktop. All of the media that we distribute through the network is licensed commercial material, including 30,000 independent artists.

And so our major concern, obviously, is with copyright. In being the largest distributor of digitally rights managed material, we have learned that distributing DRM-ed content is working. We distribute, as Alan mentioned earlier, 500,000 digital rights licenses every single day, and that is growing.

So as far as educating the user is the most critical piece, and as you mentioned, putting up a banner that says what they are doing is illegal is something that we have encouraged in the click wrap agreement with Kazaa Media Desktop, and that is precisely what they do, is warn them that they are in violation of this agreement.

To inhibit the usability of the application at this stage simply pushes users into a deeper, darker tunnel of using peer-to-peer networks. For instance, if they would get very, very frustrated with a specific way, they are going to flee to some networks that are highly encrypted, such as FreeNet. They are going to find ways. They are going to use anonymizers to disguise themselves.

So the issue here and our feeling is that gradually changing user behavior is the approach to this, and that is critical, and this goes to as far as the user education. For instance, today, I have my laptop, which is wireless, and I picked up on a number of wireless networks from a number of companies within the D.C. area, including law firms, where files were accidentally being shared via—in fact, their entire network is accidentally being shared via wireless networks. And these are IT folks that are in charge of these.

This is not a problem that is just localized to P2P networks. This is with technology altogether. We need to take greater care in educating ourselves and practicing—and as a company leading this initiative, we have to practice best practices, and we feel that we lead that, particularly because we are making this a commercial initiative.

Chairman HATCH. That has been very helpful, but—

Mr. SAAF. I would like to address that question, as well, if you wouldn't mind.

Chairman HATCH. Can you destroy their set in a home?

Mr. SAAF. Yes. I think that is not something anybody is really interested in doing.

Chairman HATCH. Well, I am. I am interested in doing that.

[Laughter.]

Chairman HATCH. I am very interested. That may be the only way you can teach somebody about copyright.

Mr. SAAF. What the industry, speaking as an anti-piracy software company, what the industry is mostly interested in is non-invasive solutions to the piracy problem. Nobody wants to destroy files. Nobody wants to go onto people's computers and damage those computers.

Chairman HATCH. But you can? There is methodology you could do that?

Mr. SAAF. I am not really aware of anybody that is exploring methodology in a legitimate way to actually destroy people's computers. It is just not something that anybody is really interested in doing.

What people are interested in doing is non-invasive anti-piracy measures, such as what our company does, is decoying, where we just put fake files on the network. It is extremely non-invasive. It just tries to create a needle-in-a-haystack situation, where the pirated content is difficult to find.

The bottom line is that it is not the 30,000 independent artists that are being pirated, it is the top 100 platinum artists that are being pirated on these networks and it is crucial that that be protected on these networks.

But in terms of invasive procedures, nobody is—I am not aware of anybody that is really pursuing invasive technology.

Chairman HATCH. Okay.

Mr. MURRAY. Senator, if I can perhaps try and respond. I am not the biggest technology expert on the panel by any means. My understanding is that there are viruses out there that could have the effect of doing what you are describing there, and if a company that were enforcing copyrights chose to use such means, they would have such means available.

Chairman HATCH. Well, I would think that in order to do that, you would have to have a law passed by Congress enabling them to do that. I mean, there are a lot of other issues involved there, but I was interested that there is technology available. You could actually warn the person, warn them again, and tell them, "if you continue, we are going to destroy your machine." I was interested in that because that would be maybe the ultimate way of making sure that no more copyright is pirated. But—

Mr. MURRAY. That does seem to be what Representative Berman's bill contemplates.

Chairman HATCH. Pardon?

Mr. MURRAY. Insofar as I understand it, that seems to be what Representative Berman's bill in the House contemplates, is that sort of action.

Mr. SAAF. I would take issue with that and disagree with that. As Representative Berman's bill, our company is the primary company that bill was directed towards and the bill very clearly does not allow any sort of invasive procedures. It is a very—I recommend anybody actually look at the actual context of the bill before drawing conclusions. There are sensationalists, like it is directed towards hurting people's computers.

Invasive procedures are not being pursued by any legitimate anti-piracy software company right now. That is just a fact.

Mr. BROES. Well, I can add a piece to that. I was the CEO prior to being at Altnet, was the CEO of Vidius, which was actually the company that was hired by the RIAA and the MPAA to do the evaluation of the Fast Track network prior to the lawsuit that was filed. We practiced and we developed technology that was considered interdiction. In fact, we were one of the first, I think even before MediaDefender. We did spoofing.

What we found it to be is actually very ineffective, not cost—it is not cost effective at all. It actually cost us more to interdict and to spoof than it was worth, than the progress that we were making, for the reason that the peer-to-peer networks are a democracy. When you spoof a file and you put it out there, the intent is to try to seed the network with millions of these spoofed files, and what happens is users, once they find out that that file is a spoofed file, they remove it out of their shared folder. So they are no longer sharing that folder, which means that the company is now faced with the burden of seeding the network once again with that same spoofed file. That costs money and bandwidth.

Our approach to this has always been a positive, kind of a glass is half-empty, half-full. If this glass here represents all of the pirated content on the Internet or all of the pirated content on peer-to-peer network, if we took a gallon jug of milk and we filled that full of legitimate content, then I kept pouring that into that network, eventually, it is going to be filled with milk and not water.

So my point is that if we continue to take digitally rights managed files, which is a positive approach curbing user behavior, we will find that users find it more difficult to find the pirated content and the viruses and everything else because we have populated the network with legitimate content that is available for a price.

So I have practiced personally as a company and as the CEO of a company the tactics that you are speaking of and I can tell you that it actually makes the problem more difficult.

Chairman HATCH. That is interesting. Well, we would like you to consider helping us to understand what are the best methodologies that we can use or what would be the best thing Congress could do to help to avoid and prevent piracy of copyrighted materials throughout the country and the world. Write to us and help us to understand this better, because there is no excuse for anybody violating the copyright laws. Those laws are what protect our artists and our novelists and you name it, anybody who can qualify for a copyright, in what they are trying to do. And if they get a copyright, that ought to be respected.

And if we can find some ways to do this short of destroying their machines, I would like to know what it is. But if that is the only way, then I am all for destroying their machines and letting them know.

[Laughter.]

Chairman HATCH. After you have a few hundred thousand of those, I think people will grow up and realize. But we would have to pass legislation permitting that, it seems to me, before somebody could really do that with any degree of assurance that they are doing something that might be proper.

I am very interested in this area, and naturally, we have had everybody in the entertainment world come to us and say, "Please, help us to find a way around these piracy situations because it is just costing billions and billions of dollars." I have seen first-run movies out within an hour after the movie is shown for the first time on a pirated basis. Of course, you can imagine what happens in the publishing world and the recording world. It is just awful.

So we could use your help on that. Congress can't do everything, but if there are some things we can do with regard to copyright, we would like to do them.

This has been a very interesting panel. I really appreciate all of you coming and taking your time to help us to understand this better. I commend you for the success that you have made and for the great work that you are doing in the respective areas of the industry that you represent. So thank you for being here.

With that, we will recess until further notice.

[Whereupon, at 3:17 p.m., the Committee was adjourned.]

Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Written Questions from Senator Leahy
Answered by Nathaniel Good and Aaron Krekelberg

1. **You studied 12 individuals who were each tasked with using the KaZaA user interface. These individuals were to decipher which of their files was being shared. The percentage of people you studied who could not tell which files were being shared, 10 out of 12, is very disturbing. Kazaa might respond, however, that the subjects you chose could have been relatively new to file sharing. Could you please explain how you chose your test subjects?**

We randomly selected test subjects from around our office area. The area we were in consisted of people who knew how to use a computer, but with varying degrees of expertise. In Human-Computer Interaction, it is known that most major flaws in an application can be identified with five or less subjects, but in our study we decided to have twelve subjects for added validity. We had people who were researchers in P2P systems, as well as people who had never used P2P before. To get a better understanding of each participants experience with P2P systems, we asked each participant to take a short questionnaire in which they answered several standardized questions on their experience using a computer and their experience with P2P file-sharing programs. Questions were presented in the QUIS format, a standardized format for asking experience and usability questions developed at the University of Maryland. Each of these users were presented with the single task of identifying which files and/or folders were being shared by the Kazaa application, if any.

From the pre-experiment questionnaire we learned that all users had the highest level of computer proficiency as determined in QUIS (over 10 hours of computer usage per week), and 10 of the 12 had used file-sharing applications before. We also learned that the majority of the users (10 of the 12), assumed that P2P file sharing applications only shared certain types of files (such as music and videos) and did not know that the applications could share any type of file on the hard drive. Despite the fact that our sample had "computer savvy" users by QUIS standards and the majority had experience with P2P, surprisingly, almost all users were unable to correctly determine which files were being shared by the application. This result suggested that problems in the user interface were a primary factor in users confusion over sharing in Kazaa.

2. **In your study you mention one shortcoming in Kazaa's user interface: that is does not tell the user how the program is selecting folders for sharing. It also does not tell the user that if a folder is selected for sharing, them every file in that folder is available for downloading. Are you aware of a file-sharing program that has a more adequate user interface?**

We have looked briefly at other popular file-sharing clients, and they seem to all have similar properties to Kazaa. Kazaa versions before the current 2.5 release are representative of most P2P user interfaces, and they seem to have similar issues with folder and file selection. Bearshare seems to have a slightly superior

interface for selecting files and folders in that it disallows some folders and files from being shared, but this seems to be done mainly to prevent users from sharing temporary files or partially downloaded files on the network.
Essentially, all file sharing applications support the user doing two functions:

1) Determining where to store files that are downloaded from the P2P network.
2) Determining what files are to be made accessible to others on the P2P network.

One commonality between almost all file-sharing programs is that the folder that stores files downloaded from the P2P network is also shared with users of the P2P network. Another commonality is that this folder can typically be any folder on the machine, and that all files and folders beneath it are also shared. There also seems to be a common trend to allow any kind of file to be shared, although this tends to not be stated explicitly in the interfaces.

The latest version of Kazaa (ver 2.5) has made an effort to increase security and prevent users from making fatal errors. The default location for sharing files is fixed, and additional folders that are to be shared have to be indicated in a different interface. Some terminology has also been clarified; such the "traffic" tab has been renamed to "sharing". In addition, warnings are provided if users accidentally select their entire hard drive for sharing, although dismissing the warnings still allows the user to share their whole hard drive. Although files and folders still share all types of files if selected, there are many more warnings in place to educate users about their actions and possible consequences.

3. **I notice in your study that you list four usability guidelines. How did you develop these guidelines?**

We created a modified list of usability guidelines adapted for Peer-to-Peer File sharing applications based on a list of security guidelines provided by Whitten and Tygar in their paper "Why Johnny Can't Encrypt". We extended them to take into account the unique demands of continuously connected systems that distribute personal files.

4. **What specific changes to Kazaa's user interface might resolve some of the problems your test subjects encountered?**

A simple rule to follow in designing a secure user interface is that the more important something is, the more obvious it should be. There were many problems that we uncovered with the KaZaA user interface, but the most serious had to do with the application making assumptions that did not match up with the users assumptions. In the pre-experiment survey we discovered that only 2 of the 12 users were aware of the fact that any kind of file could be shared through the application. These hidden assumptions manifested themselves in many parts of

the application, and contributed to users being confused about what it meant to "share" files. There are several things that could be done to address this:

- Prohibit or curtail sharing of files that can be sensitive.
    - People tend to think of files in terms of what they are used for rather than where they are located. Having levels of control based on application type, and making these specific and obvious in the interface would be very important and help prevent fatal errors.
- Bring important functionality and information to the "top" of the application
    - During our experiment we found it interesting that although the number of files being shared is currently displayed on the bottom corner of the screen, none of our subjects noticed it during our trials. This suggests that information such as whether file sharing is enabled or not, and what files are currently being shared and downloaded should be easily visible and prominently positioned in the default interface.
- Provide a more rigorous interface that explicitly supports users' efforts to make exceptions to recursively shared folders, or otherwise warns users that they have not checked sub-folders in a folder that is being selected for sharing.
    - The latest version of Kazaa partially supports this by providing warnings to users about selecting folders that have sub-folders in them, and by "expanding" out the folder selected so users can see the sub-folders being shared. This is a strong improvement over previous versions, but still assumes that users know what is in the subfolders and what file-types are going to be shared. A safer way of handling this would be to select single folders instead of all sub-folders automatically. A drawback to this approach is that this would make sharing some folders tedious and time consuming, as each individual sub-folder would need to be shared.

Responses of Alan Morris to Written Questions Posed by Senators Hatch, Biden and Leahy

Questions from Senator Orrin Hatch
To Alan Morris
Following the Hearing, "The Dark Side of a Bright Idea: Will Personal and National Security Risks of P2P Networks Compromise the Promise of P2P Networks?"
Held On June 17, 2003

1) How does your Family Filter identify adult content? Could it be adapted to screen out other types of objectionable content, such as unauthorized copies of copyrighted material?

The family filter is an important tool to help parents exercise responsibility, and Sharman incorporated it precisely to aid parents and protect users from files they may not wish to see. It is a dumb filter, though. By this I mean that it simply excludes files that match a standardized list of offensive keywords. It excludes those words most commonly used for such material in searches on the major Internet search engines. There are intractable and well-documented problems with trying to make this filter do something it was never designed for – i.e. block unauthorized copyrighted files. Primarily, it is plainly technically impossible – by this I mean there is no way that a filter that can only check for the existence of a word from a list could detect the complex data necessary to identify an unauthorized copy of a copyrighted file. The problems that make this mechanism unsuitable for blocking infringing files also make the entertainment industries planned "software bullets" so irresponsible. For example, Titles cannot be copyrighted – only the performance -- so it is not possible to rely on the string of words that form the title. What if a proud parent puts up a creative film clip of his kids play-fighting called "Gladiators" – are we to ban freedom of expression on the off-chance it may be infringing material?

2) In your testimony, you stated that the Family Filter is enabled in a default installation of Kazaa. I have attached a copy of a screen capture taken from a default installation of Kazaa showing that when a user searches on that default installation for the term "nude," a pop-up menu appears and its default option disables the Family Filter. Please explain why this is consistent with your claim that the Family Filter is enabled by default in Kazaa.

By default the Adult Filter is enabled and may further be password protected by parents – you appear not to have used the password protection – hence the pop-up. It should be understood that whilst it is estimated that the filter will exclude

approximately 90%+ of sexually offensive material it cannot be extended to cover every term with even a remotely sexual connotation. Now, whilst nude is not a term that is generally used by purveyors of offensive materials, as it is an everyday word, variants of nude (which for decency I will not repeat here) are included. Of course nude is used legitimately in, say, describing works of art. However, as the filter is a simple one, we veer to the conservative. So rape is included in the proscribed list although this means that something like the famous paintings; "The Rape of the Sabine Women" would be proscribed. Therefore, as the filter is enabled by default we need to alert users who, whilst not wishing to see offensive material might, for instance, wish to search for a treatise on Nabakov's Lolita, but would find the word Lolita blocked by the filter. This is the effect you saw.
As the KMD family Filter is password protected parents can ensure the filter is not circumvented by their children in any circumstances. Parents can of course add additional words to the filter using the Blocklist box.

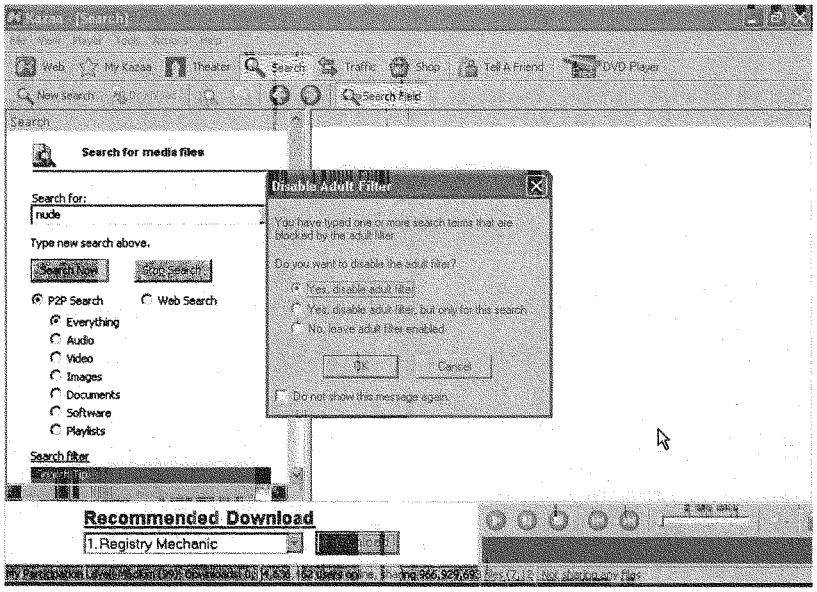
3) You stated in your testimony before the Committee that Kazaa's Bullguard virus protection is available free to your users. Is that free use indefinite, and if not, how may days can Kazaa users use Bullguard for free before they are required to pay for its continued use?

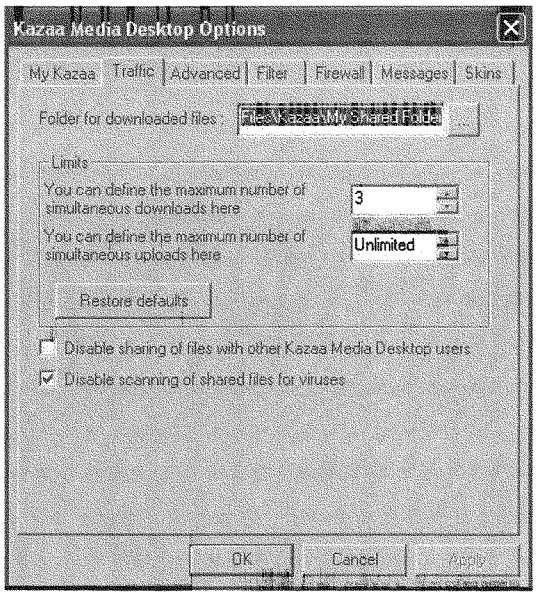
Yes, you are right that Sharman thought the general issue of viruses on the Internet was so important that we determined to provide fully featured and free anti-virus protection for users of KMD when they share files. Its use is totally free and the protection is planned to be indefinite and always has been. You seem to be confusing this free protection with Bullguard's totally separate, generous 30 day free trial offer for the full version of its software (i.e. protection for the user when using any application, not just KMD). Of course, the free anti-virus protection is not conditional upon buying the full version.

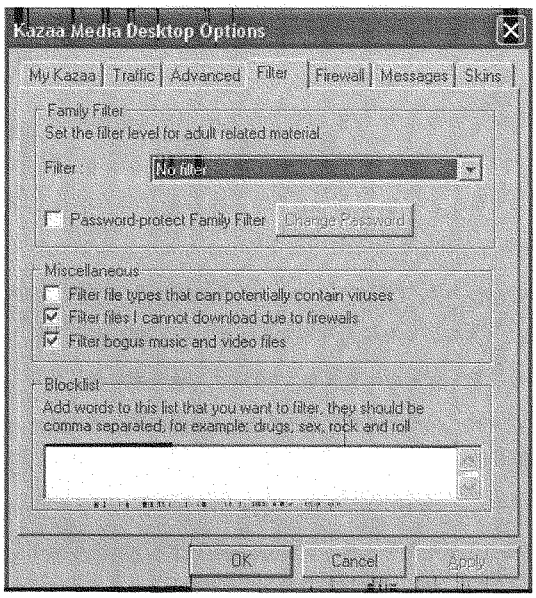
4) At the hearing, you stated that the virus protection in your software was enabled by default. I have attached a copy of a screen capture taken from a version of Kazaa downloaded from your website on June 6, 2003 and installed in default configuration. Please explain the "check" in the checkbox labeled "Disable scanning of shared files for viruses," and identify the first date on which a copy of Kazaa downloaded from your website would install by default with virus protection enabled.

To put our efforts in context, Web browsers and e-mail clients – the most prolific means of transmission of viruses, much more so than p2p, - do not supply free, fully featured anti virus software as we do! So, Sharman is pleased to go the extra mile to protect the security of its users. When we first included the free Bullguard anti virus software, at a real cost, over 12 months ago for users of KMD, we were unsure as to whether users, for reasons of efficiency, would want two anti virus programmes running – namely BullGuard and any other anti virus programme they already may have had – hence the default check in the "disable scanning of shared files for

viruses" you saw in old versions of KMD. We discovered that millions of people worldwide were choosing to enable Bullguard and this furthered our belief that many people were not fully protected on their own account. So, we decided, at our own cost, to supply an improved BullGuard p2p to all users from v2.5 onwards (available from 24th June 2003 from www.kazaa.com). Of course, users still have the option, quite rightly, to disable the free AV protection if they wish. It is worth commenting that this latest use of p2p to deliver large numbers of complex virus definition files in a timely and reliable way is tribute to the importance of p2p as an elegant distribution vehicle.







Sharman Exhibit A

Questions of Senator Joseph R. Biden, Jr.
Committee on the Judiciary Hearing on
"The Dark Side of a Bright Idea:
Could Personal and National Security Risks Compromise the
Potential of Peer-to-Peer File-Sharing Networks?"
June 17, 2003

Questions for Alan Morris:

1. As you know, the Good / Krekelberg study found that some Kazaa users are sharing sensitive documents, at times unwittingly. Your testimony indicates that Version 2.5 of the Kazaa Media Desktop includes changes designed to prevent inadvertent file sharing. Please explain exactly what changes the new version of KMD makes to prevent users from sharing files outside of the "My Shared Folder". When will the beta testing of Version 2.5 be concluded? Is it your view that the current version of KMD does not contain adequate safeguards to prevent users from sharing certain sensitive files?

Thank you for drawing attention to the continuing work we have done to make the interface safe and user friendly.

Let me first say that version 2.5 of the KMD contains more safeguards to prevent users from inadvertently sharing files than any of its leading competitors and is being constantly improved. We are never complacent, and constantly strive for an excellent interface and strongly believe we have made it very difficult for people to inadvertently share files.

As I stated in my testimony, the Good/Krekelberg study was carried out in mid-2002 on KMD version 1.7.1. Immediately afterwards we made significant changes to make inadvertent sharing more difficult and have continued to do so since then. Version 2.5, which went on general release on Tuesday 24th June 25, 2003 (at www.kazaa.com) is the latest and most effective incarnation of this process. The screen shots and description in the attached Security document show just how much effort we have put into making the interface intuitive and safe by default.

In addition we are particularly encouraged by the Committee's initiative and based upon our learning from the hearing; we have decided to implement further security and privacy upgrades in our normal post–release build (v2.5.). Witnesses identified that they were able to search for a Microsoft Money file by searching for a file with a ".mny" extension, thereby finding individuals who had inadvertently exposed private files, for instance by sharing more than the default shared folder. They then used the "Find More from Same User" feature to expose all of that user's files. To enhance user privacy and eliminate this identified problem, in our next post release build, we are making the long standing, but apparently little appreciated, function "Find More from Same User" disabled by default – so removing the chance of people looking at the entire contents of a

user's shared folder without the user's knowledge – an obvious privacy and security enhancement identified by the Committee. We are also bringing the Messenger function into line with other Instant Messaging programs by disabling incoming messages by default, thus eliminating the possibility that user's may receive unsolicited instant messages unless they choose to accept them. It seems to us inappropriate that someone may receive unsolicited messages, particularly in view of general concern, and the Committee's concern, over spam. Of course we are also taking the opportunity to further increase the education about safe sharing in the help guide. This release will be available shortly.

2. The terms of agreement KMD users must accept before using your software specify that users agree not to use KMD to infringe the intellectual property rights of others. Section 15.1 of the terms of agreement states that user rights under the license terminate if any terms of the license are violated. Are you aware of KMD users using your software to violate U.S. copyright laws? How many KMD users have had their rights under their license terminated, pursuant to section 15 of your terms of agreement, due to copyright law violations? How does Sharman enforce the termination of these rights? Are KMD users found to be in breach of the KMD terms of agreement banned from using your software in the future?

As you correctly note we believe it important that users of the Kazaa Media Desktop positively agree to the Plain English EULA and in so doing agree not to infringe lawful copyright. You will appreciate that whilst we cannot enforce this amongst users of freely distributed software it is an important principle to state. We have never denied that some users may infringe copyright and it is widely known we have no knowledge or control over the use or actions of users. In this regard, we are similarly situated to other responsible companies. Sony had no knowledge or control over what its customers chose to do with its Betamax video cassette recorder and Microsoft has no knowledge or control of what websites are being accessed by the tens of millions of individuals using its Internet Explorer software application. Similarly, Microsoft, Yahoo and AOL, to name but a few, have no knowledge of control over the hundreds of millions of files (many of which, it is commonly understood, are shared in violation of applicable copyright laws) copied and distributed in violation of applicable end-user agreements as attachments to messages transmitted with their instant messenger and email applications. We would never suggest that because a law cannot be policed it should not be observed. By distributing more than ½ million DRM licensed files a day we make a massive positive contribution to the encouragement of legal file sharing.

3. You made little mention in your testimony of the harms posed to copyright holders by activities taken by KMD users that violate copyright laws. You are opposed to the use of so-called "software bullet" technology that I understand is under development to try to curb some of these abuses. Please outline for me the steps Sharman has taken to mitigate the harms posed by KMD users

who violate copyright laws. What future plans does Sharman have to deter illegal activities by KMD users?

I clearly mentioned that we believe unequivocally that infringement of copyright laws is wrong. Yes, you are right; consumer groups, the communications and computing industries, legislators and we are concerned about the use of harmful, indiscriminate, unfettered and illegal software initiatives by companies and trade bodies in furtherance of their monopoly position. From the day Sharman Networks Limited acquired KMD and www.kazaa.com we determined to make it both the most user-friendly and safe P2P experience and the most effective distributor of licensed media. We are now the world's largest distributor of licensed content – surely the most positive way of rewarding content owners? Further, to the extent that there may be infringement, it is not at all clear what effect this has on copyright owners. Hard questions need to be asked as authoritative third party studies into digital distribution and p2p suggest a net promotional benefit to artists and copyright owners. Whilst not seeking to justify infringement by users of various P2P applications, it does seem to give the lie to claims that music sales are effected adversely by p2p when most commentators point to the economy, the cyclic nature of sales, CD burners and other digital tools for infringement apart from file-sharing, and the music industry's own lack of success in innovation, pricing and distribution.

Indeed it has been calculated that had the entertainment industry joined with Sharman and Altnet 12 months ago, they would have earned millions of dollars for themselves and artists and saved millions in legal fees. In the meanwhile Sharman Networks Limited continues to drive forward its licensed content whilst discouraging infringement.

4. In your testimony, you note that "preferential queuing for a requested file depends on the ratio of uploaded to downloaded megabytes". I am concerned that this "Participation Level" component of KMD creates an environment wherein those users who are downloaded from most often receive preferential treatment when they seek to downloaded files from other users. You testified that "making lots of files available, *that others are not likely to be interested in*, provides no benefit" (emphasis added). Would you agree that making "lots" of files available that others *are* likely to be interested in does provide users sharing popular files with a benefit? Would you agree that users are likely to be interested in the most popular copyrighted song files, for example? If so, doesn't your "preferential queuing" policy encourage the sharing of popular song files? How does Sharman justify this approach?

The Participation Level, as you rightly say, encourages positive sharing and is not, as has been suggested, deliberate or inadvertent sharing of whole directories. It was instituted as a response to user demand for a fairer mechanism. I cannot comment on the notion that somehow this encourages sharing of infringing versions of files that the entertainment industry are popularizing as we have no control over what is shared.

Anecdotally though, it is widely recognized that p2p users are discriminating and not necessarily led by the traditional industry model of promoting a limited number of artists at the expense of the many. Indeed Sharman and Altnet have been responsible for the user driven success of many artists through their distribution of DRM files. More importantly we are positively encouraging sharing of licensed files by a points program - similar to a frequent flier program - for the sharing of licensed Altnet DRM files

Written Questions from Senator Leahy
to Witnesses at the Hearing on Peer-to-Peer Networks
Senate Committee on the Judiciary
June 17, 2003

Questions for Alan Morris

For each of your answers, please indicate whether or not the answer will change in the new version (version 2.5) of Kazaa Media Desktop ("KMD"). For answers that will change, or that have changed, with the release of a new version of KMD, please indicate what your answer is for each of the versions. For answers that are different for Kazaa, KMD, Sharman Networks, or Altnet, please indicate what your answer is for each of these entities. Please do so even for questions that specifically name one of these entities. If you use any term of art, please define that term of art.

I. General

1. Do you agree that Kazaa, as the world's most popular peer-to-peer software, has an obligation to propagate a product that neither threatens a user's privacy, nor circumvents the various legitimate tools that people use to keep certain kinds of software and activities off of their systems?

II. Inadvertent File-sharing

The amount of inadvertent file-sharing that is occurring on Kazaa is disturbing. Your software apparently is leading many of its users to share materials that they almost surely would not knowingly share with the millions of other Kazaa users.

1. Does Kazaa in any way encourage users inadvertently to share personal information, and what steps is Kazaa taking to stop inadvertent file-sharing?

2. I understand that most people who have looked into this agree that this problem is created by misleading information in Kazaa's user interface. In fact it appears that your setup program is designed to encourage users to make the user's personal documents available to the public. Your setup window entitled "File Import," for example, is where the user decides which folders to share. Nowhere does this window tell the user that if a folder is selected, every file in that folder will be made available, whether it is an audio file, or a tax return. Also, in this window the "Search Wizard" option is highlighted, presumably to encourage the user to select it. This option automatically searches every drive available to a user's computer, and makes available any folder that has even one media or image file in it. This option is responsible for much of the inadvertent sharing of personal information on Kazaa. Why does Kazaa share every file in a folder with just one "qualifying" file in it?

3. Why does Kazaa not inform its users that, if a folder is selected for sharing, that in fact every file in that folder will be shared?

4. Why is the Search Wizard option highlighted, and by highlighting it, is Kazaa not encouraging users to give up their privacy, whether they know it or not?

5. One important aspect of the "Import File" window is not readily apparent to the user. Even though the Search Wizard is automatically highlighted, the default setting is actually not to use that option. Neither is the default the other option visible in this window. If the user simply clicks "OK," in this window he or she actually gets a third option. This is at best confusing, at worst deceptive. The standard practice in windows such as this is that the highlighted option is the one you would get if you click "OK." It is even more confusing if clicking on "OK" gives the user an option that is not even listed in that window. By deviating from the standard in this way, Kazaa is able to make many users think the Search Wizard is the default. It also allows you to claim that the "default" setting does not make personal files available, when in fact your software is geared to encourage users to do exactly that. Why does Kazaa deviate from the standard manner of informing the user what the default option will be in setting up file-sharing?

6. Why does Kazaa recursively search a user's drive for qualifying files, and make the entire contents of those folders available? Why does Kazaa not inform its users that it does this?

7. Why does Kazaa not allow its users to turn recursive searching off?

8. In the "File Import" window of KMD's user interface, if the user chooses to take matters into their own hands and specify which folders will be shared, the user interface again is misleading. The window entitled "Browse for Folder" says that the user is choosing a "folder" for sharing, but does not inform the user that all of the folders selected and any sub-folders, plural, will also be shared. It also does not inform the user that by selecting a folder as the Download Folder, that folder also becomes the "upload folder," which is to say that every file in that folder will be available for sharing by

everyone else on the network. Given the propensity for error in file-sharing, why does Kazaa use this misleading language?

9. When a user selects C:\ as the download directory, that will typically share the entire hard drive. If the C drive is chosen as the download directory on startup, Kazaa understandably warns the user about this, but if the download directory is *later changed* to the C drive, Kazaa does not warn the user, and in fact the sharing of the entire drive is not apparent in Kazaa's Folder Select window. Why does Kazaa not warn users when they change their download directory to share the entire hard drive, and why is the fact that a drive is being shared not apparent in the Folder Select window?

10. In other ways Kazaa makes it difficult or burdensome to limit the sharing of files. For example, whereas an entire folder can be shared automatically if the Search Wizard finds just one qualifying file in that folder, to disable sharing the user must proceed file by file. Why does the My Media folder not allow users to stop sharing folders, but rather require that they disable sharing individually on a file-by-file basis?

11. One way users could be made aware of inadvertent file-sharing is if they could see that certain of their personal documents had been uploaded by others. KMD effectively prevents the user from discovering this, however, by "erasing" the transfer file interface each time the program is restarted. Given the fact that this is one of the few ways a user can tell what files have been uploaded from his or her computer, why does this not make it needlessly difficult for a user to keep track of his or her personal information?

12. At least one recent study has shown that the typical KMD user is in fact misled by Kazaa's user interface. Nathaniel Good and Aaron Krekelberg studied 12 individuals, 10 of whom had used file-sharing programs in the past, and all of whom spent considerable amounts of time on a computer. Those 12 went through Kazaa's entire interface. In the end only 2 of the 12 could tell which folders were being shared. The other 10 could not. Do you feel that 10 out of 12 users making an error that could seriously compromise their privacy is an acceptable number?

13. KMD's default settings seem to encourage the inadvertent sharing of files in other ways as well. For example, one default setting launches KMD when the computer starts. In fact, the default setting that achieves this seems purposefully worded so as to confuse the consumer. The option listed next to it is simply "family filter": in this option if the box is checked, the family filter is on. If it is unchecked, the family filter is off. The other option in the group is "Launch Kazaa Media Desktop after installation": if this is selected, KMD starts after installation. Both of these are very straightforward. The last option is different in syntax and logic. It reads, "Do not start Kazaa Media Desktop when the Computer starts." This asks the user to decipher two negatives, and figure out that to keep Kazaa from offering constant access to personal files the entire time the computer is on, the user must check this box. Moreover, the option appears right beneath an option that creates a quick launch button for KMD, further implying that some action is required on the user's part before KMD will launch.

Why does the auto-launch option deviate from the straightforward wording of the other options, and why is the default setting that Kazaa will start when the computer does?

14. In the "My Kazaa" window, there is an option, already checked, called "Launch Kazaa Media Desktop automatically." Does this option mean that KMD will launch automatically the first time, after installation, or does it mean that KMD will start automatically every time the user's computer is turned on? If this option is effectively the same as the option described above (which launches KMD on computer startup), this could lead to confusion. In the case of a conflict between the user's responses to these two seemingly identical options, which option will take precedent?

15. Another KMD default is that sharing is enable on launch. Most KMD users presumably would like to control the amount of information they are sharing. Of course, they would also like to have access to as many different files as possible on the network. You have deliberately struck this balance strongly in favor of maximizing the amount of information available. You have done this in many of the ways listed here, but perhaps most strikingly by the simple fact that KMD's default setting is to share files, not protect them. What factors went into the decision to make sharing files the default setting?

16. Kazaa strongly encourages its users to make their computers and their bandwidth available for use by the Kazaa Network. In particular, KMD encourages users to serve as supernodes and to allow the maximum use of their bandwidth in the service of the network. The "advanced" tab of the KMD Options suite leaves the maximum bandwidth available for other users to download files from the user's computer, allows the user to function as a supernode, and selects "optimal" bandwidth when the computer is idle. Unlike all the other options, KMD tells the user only to change these default settings if the user "know[s] what they mean." If understanding these options is so important before changing any of them, does Kazaa explain these options to its user? Where does Kazaa offer an adequate explanation? Why does Kazaa specifically warn the user to retain these defaults, but not the others?

17. KMD users often find files by doing what is known as a keyword search, which will return any files that contain the word or words the user wants. However, once a file is found on a particular computer, an individual can do a search of everything on that computer, regardless of its subject. This makes Kazaa a powerful tool to discover a great deal of information about another user. At the same time, this function does not seem to greatly enhance an individual's ability to search for files related to a particular topic. For instance, if you type in the word "resume," and find someone's resume available, you can then select that person and get all of their files, including financial information like tax returns and medical documents. In light of the massive potential for misuse, why does Kazaa offer this function, and what is Kazaa doing to limit this type of data mining?

18. Why does Kazaa require its users to offer Kazaa for download, as opposed to uploading the program to those who would like to install it? Was any legal

consideration taken into account in deciding to have current users offer the software for download?

III. Firewalls and Security

Firewalls are important tools that allow parents to keep their children safe from online materials they have deemed harmful. They also allow network administrators to maintain some control over what activities take place on their network. Universities and government agencies use firewalls extensively to protect against unwanted sharing of sensitive information, and to keep programs that use a great deal of bandwidth from tying up their systems.

One common form of firewall controls access to a computer or network by limiting the ports that are available to the outside world. Port 21, for example, is a file transfer protocol port. Port 80 is the standard world wide web port, and so a firewall that intends to prevent file transfer protocol information from entering or leaving a system would block port 21, but would leave port 80 open. Because world wide web access is so important, even in the most restrictive firewalls it is almost always left open.

KMD uses the fact that port 80 is traditionally left open to get around this type of firewall. The window entitled "Kazaa Media Desktop Options" defines the ports that Kazaa will use to share information. Port number 1560 is the default port. But the default is that port 80 is the alternative port if port 1560 is blocked. This means that Kazaa is almost completely immune from port-blocking firewalls because so few will block port 80. In effect, if an administrator or a parent wants to stop Kazaa, he or she must block the Internet entirely or use a more complex and expensive form of firewall.

1. Why is port 80 chosen as the alternate port?

2. Did the fact that port 80 is left open by most firewalls play any role in Kazaa's decision to use that port as the alternate?

3. Does Kazaa have any other functions or attributes that allow it to circumvent any security measures?

4. What steps is Kazaa taking to respect the rights of parents and network administrators to use firewalls effectively?

IV. KMD's End User Licensing Agreement

I have a number of questions about the manner in which KMD's End User Licensing Agreement ("EULA") informs KMD users of their rights and responsibilities, as well as the dangers of using KMD.

1. The EULA states that "if you are a minor you will become eligible to use Kazaa Media Desktop upon your parent or guardian reading and accepting the terms of this License." Why does Kazaa not state explicitly that minors *may not* accept the EULA, and why does Kazaa not confirm the age of the individual who agrees to the EULA, in light of the fact that there are relatively simple ways of doing so, such as requiring credit card information?

2. The EULA states that "your rights under this license will terminate immediately and without prior notice if: you violate any term of this license, including violating any applicable laws or rights of any third party including the intellectual property rights of any such third party. You may be subject to legal action if you continue to use the Kazaa Media Desktop in violation of this License." Why does the EULA terminate under these circumstances? Has Kazaa ever taken any action under this provision of the EULA?

3. Why does Kazaa place four different sets of important terms, including the EULA, the privacy statement, adware and spyware, and usage of resources information , in one window, as opposed to encouraging the user to consider each of these important documents separately?

V. KMD's Privacy Statement

1. KMD's Privacy Statement states that, although KMD will occasionally request personal information about its users in furtherance of surveys or contests. It states that "[c]ontact information will be shared with the contest or survey sponsors to notify the winners and award prizes or otherwise in accordance with the Terms and Conditions of each competition or survey." This implies that the primary use of the information collected will be to notify winners. Is it typical that the information is used only to notify winners, or are other uses common?

2. You state that "Usage of a cookie is in no way linked to any personally identifiable information while on our site or using KMD." Are the cookies you install ever linked with personally identifying information?

3. You state that "Sharman Networks has no ability to supervise, control or know your activity." Does this statement include information collected by the adware/spyware that Kazaa installs? Does it include such content restrictions as the family filter? When Gnutella left the Sharman Networks, you forced Gnutella users off of your network by pushing an update to the other Sharman users, but not Gnutella users. Would the ability to remove a user from the network be included in "supervision or control" of usage?

4. KMD states that "[u]sers are given the opportunity to 'opt-out' of having their information used for purposes not directly related to our site at the point where we

ask for information. For example, the KMD options screen has an 'opt-out' mechanism so users who don't want any marketing material, can keep their email address off our lists." In fact, may a user opt out of the installation of the adware/spyware that collects user information? Does choosing not to give one's email address actually prevent the receipt of "marketing material"?

5. KMD states that "Other users may download files that you have stored in the My Shared Folder and other folders you have specifically selected to be shared." Does this adequately describe the availability of folders that have been found by the search wizard? Does it adequately describe the effect of recursive searching?

6. KMD states that "the Cydoor component uses your Internet connection, which was designed to take up the minimum amount of bandwidth on your line." Does this mean that Cydoor was designed to use minimal bandwidth, or that the Internet connection was designed to use minimal bandwidth?

7. In describing the effect of Cydoor's storage of banner ads on a user's hard drive, KMD states that "[e]ach ad banner on your hard disc is about 10Kbytes." Why does KMD not tell the user how many ad banners are stored on a user's drive at any given time?

VI. Virus Protection

1. You have stated in the recent Senate Judiciary Committee hearing and in other testimony that Kazaa offers powerful virus protection and in fact you state that Kazaa takes "every opportunity to encourage responsible and safe peer-to-peer usage through user education as well as via the default configuration of the software." Indeed, the front page of the KMD website attempts to alleviate a potential users' security fears. It states with respect to KMD's anti-virus software, "once enabled, Bullguard Lite provides virus protection when using KMD." However, KMD's default is for Bullguard to be turned off. In addition, elsewhere you warn the user not to change the security settings. Thus, Kazaa actually discourages the user from turning on the virus protection you have described and on which your users rely. In light of this default setting, KMD's warning not to change it, and the fact that there have been at least eight major virus outbreaks on Kazaa, does Kazaa adequately protect its users from viruses?

2. Has Kazaa performed any analyses of the propgagtion of viruses over the network?

3. Does Kazaa take any steps to control or monitor viruses on the network? Please describe any such steps.

VII. Spyware and Adware

Spyware and adware are data collection software that collect all sorts of information about the user, like where he or she is going on the Internet, what search terms they enter, and html content. Spyware is typically defined as software that is installed on a user's computer with no notice to the user. Adware is installed with some notice. I understand that your position is that Kazaa does not install "spyware," because there is a reference to this software buried deep within your license agreement. However, it seems from the license agreement that the user must actually seek out the relevant information about the programs that Kazaa installs on its users' computers. In addition, the software you install is set to run the entire time a user is on his or her computer, not just when they are using Kazaa.

1. Why does KMD not explain in clear terms what the user is agreeing to, and what this software will do?

2. Why does KMD not explain how difficult it will be to remove the spyware/adware?

3. What steps is Kazaa taking to ensure that users can quickly and easily uninstall this software?

4. Why does KMD not explain that the spyware/adware continues to run even when Kazaa is not running?

5. WhenU.com, the distributor of SaveNow, one of the spyware/adware programs that are automatically installed with Kazaa, is explicitly not available to those under 13 years of age. Since Kazaa requires the installation of a WhenU product in order for it to be launched, Kazaa in effect requires that its users be at least 13 years of age. Nonetheless, Kazaa does not require proof of age. Do other applications that bundle SaveNow require a proof of age?

6. What methods of proof of age are feasible?

7. The End User License Agreement requires the user to agree to accept any future updates or upgrades to the software. How does Kazaa and/or WhenU update or upgrade the software once it is installed on a user's computer?

8. Is this method of updating or upgrading feasible for updating or upgrading the software the KMD software? Are update or upgrades performed in the same manner for KMD and the adware/spyware that comes bundled with KMD?

I. General

KMD neither threatens a user's privacy nor circumvents legitimate tools. Of course Sharman cannot agree that malicious, indiscriminate and illegal activities proposed by the entertainment industry are appropriate

II. Inadvertent File-Sharing

It is unlikely that large amounts of inadvertent file sharing is occurring on KMD – we have, and are continuing to, invest significant resources in making KMD secure by default. The Good and Krekelberg study in April 2002 was based on v1.7.1 – much has changed since then and v2.5 released on 24th June 2003 at www.kazaa.com sets the industry standard in intuitive, secure operation. Importantly, to the best of my knowledge neither the Good and Krekelberg study, nor the ad-hoc exercise by Mediadefender at the hearing, discriminated between KMD and any other GUI (applications) using the Fastrack protocol. This is particularly relevant as Mediadefender, who claim to work for the entertainment industry, was using a hacked version of KMD, namely Kazaalite, in its presentation before the Committee. Not only is this hacked version in clear breach of applicable copyright law, but the demonstration suggests strongly that many of the instances evidenced are probably from this hacked and very unsophisticated interface, and from other GUIs rather than KMD.

We are further meeting the concerns you express by implementing some important security and privacy upgrades in our normal post–release build (v2.51). We are making the "Find More from Same User" function disabled by default – so removing the chance of people looking at the contents of a user's shared folder without the user's knowledge – an important privacy and security issue, as you rightly comment. We are also bringing the Messenger function into line with other Instant Messaging programs by disabling incoming messages by default. It seems to us inappropriate that someone may receive unsolicited messages, particularly in view of general, and the Committee's, concern over spam. Of course we are also taking the opportunity to further increase the education about safe sharing in the help guide. This release will be available shortly.

III. Firewalls and Security

KMD simply uses the same protocols to reach the Internet as other Internet applications like web browsers and Instant Messaging. It is common practice for

consumer internet applications to implement ways to traverse firewalls in order to assist the setup of the application for the end user.

For instance; Real One Player from Real Networks falls back to port 80 by default when downloading media files and Windows Messenger communicates using TCP over port 80.

One of the biggest areas of mass development today in enterprise computing is in 'web services'. Web services allow applications to talk to each other using port 80 over the internet to perform a whole range of tasks.

IV. KMD's End User Licensing Agreement

When Sharman Networks Limited acquired KMD in January 2003 it immediately took down the website and ensured that not only was there no encouragement to infringe copyright but that more importantly there were strict exhortations not to so infringe. This was reflected in the immediate redrafting of the EULA into Plain English (and French, – hopefully plainly as well!). The clickwrap nature of the agreement means that, like click wrap agreements for most commercially available instant messenger, email and media player applications, it cannot be effectively policed, but we believe the right to terminate in the case of a breach should still be claimed, even if it cannot be acted upon.

V. KMD's Privacy Statement

Sharman Networks Limited is proud of the efforts it has put into its Privacy Statement and its Bundle Acceptance Policy. We rigorously safeguard KMD users' privacy and believe we are setting the standard of best practices for p2p. Sharman and its Advertising partners recognize that they are dependent on the goodwill and trust of the users of the application and so we are rigorous in ensuring that no personally identifiable information is mechanically collected from users, passed on, or misused.

VI. Virus Protection

KMD is the only p2p application, and the only Internet Program of which we are aware, to include free fully functional antivirus software. It has been available free to any user who chose to enable it for over a year and millions of people worldwide have chosen to use it. Initially we chose to let people opt into using BullGuard-lite, in case they used their own Anti-virus software. Realizing that many people are not fully protected on their own account we chose to carry the burden of making it available by default to all users from V2.5. Of course the anti-virus industry accepts that most virus propagation is via e-mails and Instant Messenger services – nevertheless

Sharman has been determined to go the extra mile to ensure the safety of users of KMD when they are sharing files. Of course, Gold Icon DRM files of which we, along with Altnet, distribute over 500,000 a day, are guaranteed virus free.

VII. Spyware and Adware

Spyware and Adware are terms that are loosely used since they were coined in 1998. The Cydoor advertising component is just as integral to KMD as TV ads are to broadcasting and website ads are to major websites. It does not collect or send personal data about users and is simply a very efficient way to serve advertising. Currently KMD V2.5 does not contain any bundled software other than the Cydoor Advertising component and Altnet's application for delivering licensed content (which includes the My Search browser toolbar). Prior versions included WhenU's SaveNow, which has a very prominent disclosure screen during installation of KMD explaining exactly what offers and advertising it provides users. Future versions will contain either SaveNow or a similar application which will have similar prominent disclosures. Of course, users may always elect to uninstall the KMD and any bundled advertising applications, simply, from the Windows™ ADD_REMOVE_PROGRAMS applet in the CONTROL_PANEL.

Comments on Security

By Phil Morle – Director of Technology

Introduction

This document reflects upon the "Usability & Privacy: A Study of Kazaa P2P File-Sharing" paper and a subsequent email from Nathan Good.

Sharman takes its role as a leader in p2p software development very seriously indeed. We understand that we have a responsibility to demonstrate good practice and to set high standards for the rest of the field to follow. We understand that small changes we make affect the experience, security and privacy of millions of users.

For this reason we welcome intelligent research like that done by Good and Krekelberg and always integrate this thinking into our product development plans. It is a very new paradigm and the more people that help us to make the experience safe and secure as well as useful, entertaining, etc, the better.

We do this in context of the 'big picture'. Our process when something like this comes in is to immediately discuss it and compare its findings with our focus group sessions (run by independent third parties), current plans for changes and our understanding of how the product works – what can be done and what cannot be done.

When we received the *Usability and Privacy* study we acted upon it immediately and changed many things that we could do quickly in Kazaa. I will describe those things in this document.

Sharman has not shipped a major release for some months. Version 2.5, with various security changes made to the application, will be shipped this month.

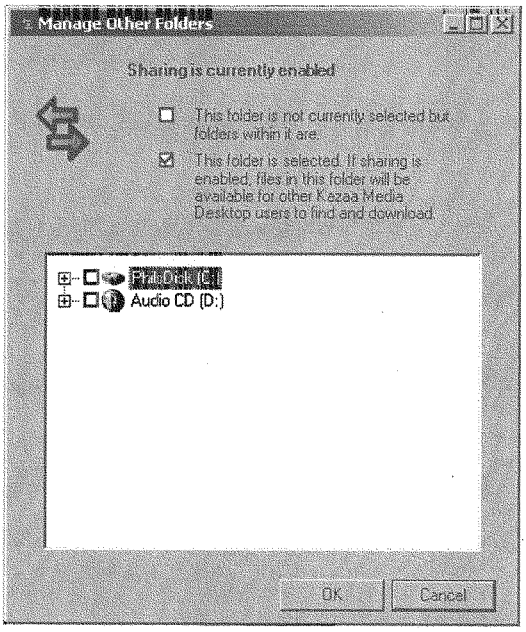
It should go without saying that we are concerned that some users are sharing out their entire hard drives and that we are constantly discussing ways to educate users and improve the user interface to stop this happening.

Changes to Kazaa 2.5

Kazaa File Import has been removed from the start-up process when a user first installs Kazaa Media Desktop. Users must now explicitly choose to share files other than those in My Shared Folder.

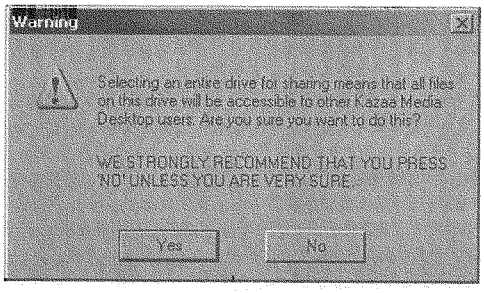
My Shared Folder cannot be moved and has been uniformly named. It is no longer referred to as Download Directory anywhere. That it cannot be moved means that a user can't accidentally share out a pre-existing folder with files already inside.

Find Media To Share has been changed to **What Am I Sharing?** And has been greatly simplified.



Notes on this screen:

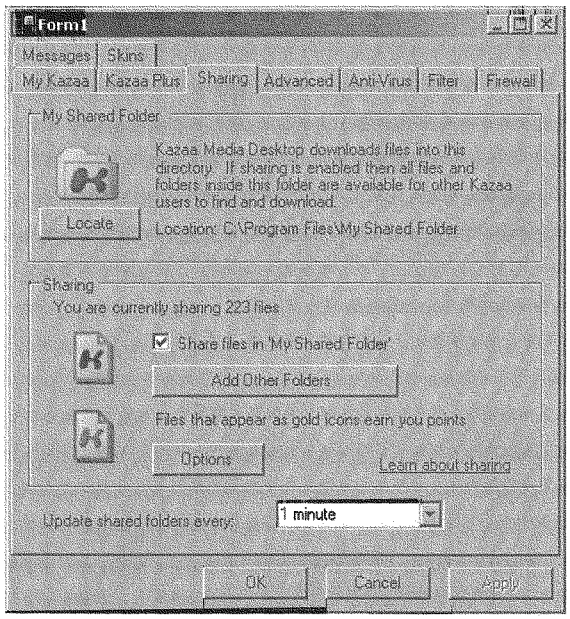
- User clearly communicated if sharing or not. Other choices refer to this choice.
- If a user selects an additional folder to share this does not automatically recurse any more. It asks the user if they would like to recurse or not.
- User cannot select the 'Drives' node
- Ability to search for media files has been removed
- If a user attempts to share an entire drive they see the following strong warning:



- The option to 'Do Not Show This Again' has been removed.

- My Shared Folder moved out of the tree to indicate that when Sharing is enabled, then files in this folder are always shared. It also tells the user where the folder is, but will not let them change its location.

Traffic Tab in Tools > Options has been significantly simplified to show the following:



All sharing options have been moved to this one screen and the language has been simplified.

New Installer now has more information/education and more options for a user to preset Kazaa Media Desktop preferences. Users are encouraged to keep the default settings so that the My Shared Folder is the only shareable location.

SUBMISSIONS FOR THE RECORD

Testimony of Derek S. Broes

Before The
United States Senate Committee on the Judiciary

The Dark Side of a Bright Idea:
Could Personal and National Security Risks Compromise the Potential of P2P File Sharing Networks?

June 11, 2003

Chairman Hatch, Ranking member Leahy, members of the committee:

I am Derek Broes, Executive Vice President of Worldwide Operations of Brilliant Digital Entertainment and its subsidiary Altnet. Altnet offers the largest secure commercial platform for the distribution of digital content over peer to peer software based networks. Under an exclusive agreement with Sharman Networks Ltd., publishers of the Kazaa Media Desktop peer to peer application, Altnet reaches an estimated 75 million worldwide unique users every month (about twice the reach of America Online). With this reach, Altnet has become the largest distributor of rights managed content over the Internet today. Altnet takes the issues before this committee very seriously, and, as you will hear in my testimony today, Altnet is leveraging its role as a market leader by spearheading efforts to make security and privacy over file sharing networks a top priority.

There is something very exciting about technology that allows tens of millions of people across the globe to simultaneously connect to each other. It is a true digital democracy. But as with any democracy, there are challenges that must be overcome and moral and ethical standards to be established. And as with any technology that reaches millions of people, there is a responsibility that every company must assume when creating Instant Messenger, e-mail, Peer to Peer, Online Interactive Games, Chat Rooms, or any technology designed to share digital words or files with anyone, anytime and instantly.

My past experience in the entertainment industry combined with my experience in Internet and peer to peer security technologies gives me a uniquely broad perspective on the issues before the Committee today.

As the former CEO of Vidius, Inc., I built an Internet security company that creates products to monitor corporate networks for security risks associated with file sharing applications that are run on company computers. In most cases, we found the risks to be solvable with simple company policy changes and minor network alterations. In addition to addressing corporate security risks, much of Vidius' work was dedicated to an in depth technical analysis of Peer to Peer networks for such clients as the Motion Picture Association

(MPAA), and the Recording Indusstry Association of America (RIAA) from an anti-piracy point of view.

I firmly believe that it is the responsibility of peer-to-peer file sharing companies to proactively protect the privacy and security of users of their software applications.

This week, Altnet launched with Kazaa the new application it revealed it would release a year earlier. These include an interoperable platform that enables public Peer to Peer applications like Kazaa to work with private and secure platforms like Altnet's to provide incentives through a loyalty points program and payment gateway for users to share and purchase digitally rights managed authorized files provided with permission of content owners instead of files that may be unauthorized.

Altnet has worked very hard to protect the privacy and security of its users. It has accepted responsibility related to the possibility of larger security threats that shared resource applications could pose if they are not managed properly. Much of that lead has come from the team at Sharman Networks who have been particularly diligent in ensuring that standards are set very high for all downloaded applications of its type.

C-net's www.download.com web site is a third party site that monitors downloads for hundreds of companies that provide these downloadable applications and many of the standards for privacy and user security are being established through sites like this.

While there are some unique challenges to making file sharing applications more secure (which I will outline), it is important that we demystify these technologies and realize that the many protective security and privacy technologies are already widely available. By simply adopting standards commonly used on the World Wide Web such as Secure Socket Layer (SSL), the Public Key Infrastructure (PKI), and Authentication Agents, file sharing becomes much more secure. In addition to these, distributors of peer to peer applications should adopt standard user privacy policies, and take care to educate users as to how their applications work, and how to be a safe and responsible user of the application.

Beyond adopting industry standard security practices and policies, distributors of file sharing applications must also address security challenges common to peer to peer and similar infrastructures. A publicized threat with file sharing technology, as well with e-mail and instant messenger technologies is the spread of viruses. As you would expect, when files often come from anonymous and uncertified sources, the risk of that file containing a virus greatly increases. In addition, many file sharing applications provide a tool to allow users to search their hard drives for files to share. If used incorrectly, users could inadvertently give access to their confidential files and folders.

Allow me to review how Altnet meets these challenges from within the Kazaa Media Desktop peer to peer application and how Sharman Networks, The owner and operator of Kazaa have reacted to various privacy and security issues over the past 18 months.

Altnet ensures that only certified and authenticated files can be transferred by the Peer Enabler component of the Altnet application. This eliminates the risk of viruses when users download files from file sharing networks that utilize this technology, such as the Kazaa Media Desktop. Altnet's patented process called "True Names" is one of the founding principle patents that have been used to manage file fingerprints for many years ensuring that files retain their exact attributes when they may be susceptible to tampering as they travel from point to point on the Internet.

Sharman Networks has taken great care to protect users' privacy and security. As they have outlined here today. Altnet takes every opportunity to encourage responsible and safe peer-to-peer usage through user education and via the default configuration of the software. The nature of decentralized peer-to-peer technology means that users are in control of the material they choose to share with others. Our goal is to work with partners that provide them with the education and tools they need for safe and responsible use and to set the bar for security standards and best practice business ethics.

Commercialization of the World Wide Web lead to the creation and adoption of advanced security, privacy policies and protection technologies, and the evolution of file sharing networks will follow the same path as result of trusted business leadership and not legislation.

Beyond implementing these practices and policies, networks with global reach have an even larger responsibility. I'm proud to announce that Altnet and Sharman Networks are working together to implement features to address broader issues of public interest and benefit. With the largest assembled online audience on the planet, the power to make a difference by displaying pictures of missing children, publishing the pictures of the world's most wanted criminals, and issuing Amber Alerts instantly across the network are but a few examples of the initiatives we seek to undertake.

The future technological benefits of peer to peer technology are only now being explored and include the voluntary creation of shared resource networks that will allow massive distributed computing and storage of a scale only dreamed about by the pioneering medical research and astronomy projects that have received publicity to date. These types of applications will give research labs the ability to share processing power with hundreds of thousands of computers and digitally crunch billions of numbers in a nanosecond. The technological benefits of such a program are undisputed. From medical research to rendering Toy Story part 3, Altnet intends to lead

the market by presenting an opt-in resource-sharing program to users that will be defined by the highest principals of disclosure and consent.

If file sharing software companies understand and meet their responsibilities, and content companies support these positive and important initiatives, then companies such as Altnet will have the ability to find an audience, reduce piracy, offer vastly improved efficiencies in digital distribution, create instantly accessible global content sales and marketing channels, provide a variety of public services, distribute a movie, market a recording artist, and sell a game, all while turning a profit and protecting user privacy from within a secure environment. We welcome input from our peers and from this Committee to ensure that we continue to meet the responsibilities we have assumed. Finally, the initiatives that Altnet have been able to develop distribute and deploy to Kazaa users around the world could not have been achieved if it was not for the complete support and willingness of the management at Sharman Networks.

Thank you, Mr. Chairman, for the opportunity to have participated in this most important hearing. We invite any questions that your committee may have.

Sincerely,

Derek S. Broes
Executive Vice President of Worldwide Operations
Brilliant Digital Entertainment & Altnet, Inc.

Testimony of Congressman Tom Davis (VA)
Chairman, Committee on Government Reform
U.S. House of Representatives
Before the Senate Committee on the Judiciary
"The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-Peer File-Sharing Networks?"
June 17, 2003

Senator Hatch, Ranking Member Leahy, and other members of the Committee, thank you for inviting me to discuss the issue of peer-to-peer file sharing. As you know, the Committee on Government Reform, which I Chair, has been investigating some of the risks associated with the use of these programs.

File sharing programs are Internet applications that allow users to download and directly share electronic files from other users on the same network. These programs are easily installed and permit the sharing of files containing documents, music, or videos, free of charge.

File sharing is surging in popularity. The most popular file sharing program, Kazaa, has been downloaded almost 240 million times, making it also the most popular software program downloaded from the Internet. File sharing programs are increasingly popular with children. Research has shown that more than 40 percent of those who download files from peer to peer networks are under the age of 18.

The technology underlying file sharing programs is not inherently bad, and it may turn out to have a variety of beneficial applications. However, as our Committee has learned, this technology can create serious risks for users.

Most of the news coverage on file sharing focuses on one issue: the ability of users to trade copyrighted music, movies, and videos. Our Committee is investigating other aspects of file sharing. In March, we began our investigation by holding a hearing to examine the extent to which pornography, including child pornography, is traded on these networks. Last month, we held a second hearing to review the personal privacy and computer security risks posed by the use of these programs.

At our first hearing, we learned that peer-to-peer networks have become an increasingly popular mechanism for trafficking in pornography, including child pornography. In fact, it seems as if many of these programs have become digital pornographic libraries where all sorts of pornographic materials can be easily accessed for free. At the Committee's request, the General Accounting Office searched file sharing programs and found hundreds of pornographic images, more than half of which was child pornography and graphic adult pornography. Research performed by another witness at our hearing found that nearly six million pornographic files were available for downloading on one popular peer-to-peer network over a two day period.

These findings are very disturbing. Many of these pornographic images are appearing on our children's computer screens whether they ask for it or not. Innocent searches for files using the names of popular cartoon characters, singers, and actors produce thousands of graphic pornographic images, including child pornography.

At the hearing, we issued a report detailing our findings, and I would urge parents to review it in order to become familiar with these issues. We also developed a list of non-technical actions parents can take to reduce or eliminate their children's exposure to pornography on these networks. This list is available on the Committee's website.

Last month we held a second hearing to examine threats to personal privacy and computer security posed by the use of file sharing programs. Despite the surging popularity of these programs, few people recognize the risks that this technology presents. For example, through a couple of simple searches on one file sharing program, Committee staff easily obtained:

- Completed tax returns with social security numbers, including the names and social security numbers of spouses and dependents;
- Medical records;
- Confidential legal documents such as attorney-client communications regarding divorce proceedings and custody disputes;
- Business files, including contracts and personnel evaluations;

- Political records, including campaign documents and private correspondence with constituents; and
- Resumes with addresses, contact information, job histories, salary requirements and references.

There are several possible causes for the sharing of personal information over these networks. Users may accidentally share this information because of incorrect program configuration. We learned at our hearing that the installation and set-up process can be confusing and can cause users to unwittingly expose their entire hard drive.

Unintentional sharing of personal information can also result from the sharing of one computer among several users. For example, a teenager sharing a computer with his or her parents may elect to make all the contents on the computer available for sharing without thinking about the types of files stored on the computer.

Users may also intentionally share these files because increased file sharing earns the user higher priority status, resulting in faster downloads of popular files.

Either way, the public should be aware that use of these programs could result in the sharing of personal information, which can open the door to identity theft, consumer fraud, or other unwanted uses of their personal data. Parents, businesses, and government agencies also need to be aware of these risks if file-sharing programs are installed on their home or office computers.

Another privacy concern raised by the use of peer-to-peer file sharing is the bundling of these programs with software known as "spyware" and "adware." These programs monitor Internet usage primarily for marketing purposes often without the user's knowledge. They also give rise to pop-up advertisements and spam e-mail.

Finally, computer viruses can easily spread through file sharing programs, since files are shared anonymously.

I commend this Committee for looking into these important issues. Computer users at all levels of expertise must understand and appreciate the risks associated with the use of this technology. Because of the privacy and security risks, users must fully understand which files are being shared. File sharing companies must also play a role in helping to protect personal privacy and to make the programs safe for use by children. At a minimum, instructions for installing and configuring these programs should be easy to understand and should be designed with the least technologically savvy user in mind.

Once again thank you for inviting me to testify today.

News from . . .

Senator Dianne Feinstein

of California

FOR IMMEDIATE RELEASE:
Tuesday, June 17, 2003

Contact: Howard Gantman
or Scott Gerber 202/224-9629
http://feinstein.senate.gov/

Statement of Senator Dianne Feinstein on the Risks Posed by Peer-to-Peer Networks

***Washington, DC** – The Senate Judiciary Committee today convened a hearing to examine how peer-to-peer file-sharing networks could compromise sensitive government information.*

Peer-to-peer (P2P) file sharing allows users to transfer files between computers over the internet. While this technology has many legitimate uses, it is frequently used to facilitate the illegal distribution of copyrighted music and movies, in addition to the sharing of pornography of all kinds. Peer-to-peer file sharing, however, poses an even greater danger. Because this practice opens a computer to another user, it puts at risk all files on that particular computer, including sensitive information. The following is the prepared text of Senator Feinstein's committee statement:

"Peer-to-peer software allows Internet users around the globe to share files with each other fairly easily – all you need is some free software and an Internet connection, and your files are instantly made available to the Internet. This technology can be used to help researchers share information or files seamlessly across borders, or to help business people share documents – in other words, there are legitimate uses for this software.

But as with many new technologies, there are also risks. One such risk is the recent explosion of illegally shared, copyrighted files over the Internet, most of it occurring through these relatively anonymous, peer-to-peer networks. Using this free software, one Internet user can simply put his or her entire music collection onto a computer, and then open that computer up to the rest of the world, allowing anyone else with an Internet connection and similar software to find the music, download it to their own computers, and listen to it at will - without compensating the copyright holders.

Meanwhile, these peer-to-peer networks are also facilitating a new era of easily obtainable pornographic material, including child pornography. 'Media Defender' a company that will testify today, has estimated that more than 800 universities are hosting child pornography on their own networks.

Of most concern, however, is the use of peer-to-peer file sharing by government employees. According to recent studies, the vast majority of peer-to-peer users have no idea of the breadth of data they are sharing with other users – a federal employee intending to simply download and share music files, therefore, could easily make available every file on his computer, without intending to do so or even realizing it after the fact. This could include personal correspondence, private financial information, and even proprietary and sensitive government documents.

- more -

For normal users, this lack of security presents the real threat of identity theft. Stored credit card information, financial documents of all kinds, personal information like birthdays, mother's maiden names, you name it - all of this is often stored on an individual's computer, and all of it can thus be compromised if the user is not careful when setting up peer-to-peer software.

For government users, the situation is far worse. Not only personally sensitive information can be stolen, but information vital to the functioning of government as well – confidential memos, defense department information, law enforcement records...all could be available to any Internet user with some free software and the desire to go looking.

The scope of this problem is unclear - nobody really knows how many government employees are using this software, and what level of risk there truly is. But one thing seems clear – the risk is not worth it. According to recent reports, it appears that many government employees are indeed using their time at work to set up peer-to-peer software on government computers, search for and obtain pornography of all kinds, and illegally download and distribute copyrighted material. Each of these activities reduces work productivity, many of these activities violate the law, and, most importantly, the entire process opens those computers and computer systems up to invasion by outside entities.

The House and Senate have already prohibited the use of this technology on Congressional computers, as I understand it, for these reasons. And I am preparing letters to the heads of each Cabinet agency asking them to look into this problem and work towards addressing it within each of their organizations. There can be no doubt that the widespread use of these new technologies represents a grave security risk to this nation, and should be treated as such."

###

Written Testimony of Nathaniel Good, Graduate Student
University of California, Berkeley
School of Information Management Systems
And
Aaron Krekelberg, University of Minnesota
Office of Information Technology
Before the
Senate Committee on the Judiciary

Hearing: "The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of P2P File Sharing Networks?"

June 17, 2003

Good afternoon Chairman Hatch, Ranking Member Leahy, and Members of the Committee. Thank you for the opportunity to appear before you today. My name is Nathaniel Good. I am a graduate student at the University of California, Berkeley in the School of Information Management and Systems. My colleague, Aaron Krekelberg, is the Lead Web Developer at the University of Minnesota's Office of Information Technology. It is an honor to be here today to testify before the Committee and to discuss the results of a study we performed on usability and privacy of the KaZaA peer-to-peer file sharing network.

Goals of the Study

The primary goal of our study[1] was to demonstrate that good user interface design is an essential part of designing an application that is secure and preserves users' privacy. By exploring how private information could be exposed by miscommunication between the user and the application, we hoped to illustrate how important it is to develop and incorporate human-computer design principles into the process of creating applications that could potentially leave users' data exposed. We also hoped to draw attention to the larger, more general problem of creating safe user interfaces for all types of continuously connected, networked systems that store and share users' personal and private information.

The Problem

We discovered that users of the popular file-sharing program KaZaA, were misconfiguring the application and allowing other users on the network access to their private and personal information. In our study we determined that these errors were due to a confusing user interface and users' misunderstandings about the programs actions and capabilities. Programs that allow people to share files over P2P assume that the users understand concepts about networking, their file system and the intricacies of being connected to a P2P network. A recent study quoted in the New York Times by the NPD Group states that half of all people in the United States connected to the internet (43

[1] Good, Nataniel S., and Aaron Krekelberg, "Usability and Privacy: A study of Kazaa P2P file-sharing." June 2002. Available at: http://www.hpl.hp.com/shl/papers/kazaa/index.html.

million Americans) have used P2P file sharing applications. While the assumptions that P2P programs make about the users' knowledge and understanding may have held for the initial population of users, this is not the case now that the user base has expanded to millions of people with widely different conceptions of what these programs actually do. We discovered that in some cases even experienced computer users who had used P2P applications did not fully understand the assumptions that the application was making about the file types being shared, as well as which folders and files were designated for sharing with others on the P2P network.

We decided to explore this issue within the context of the larger problem in the field of Human Computer Interaction of creating informative and easy to use interfaces that do not sacrifice security and privacy for convenience. In addition, we also hoped to draw attention to the larger, more general problem of creating safe user interfaces for all types of continuously connected, networked systems that store and share users personal and private information.

Summary of Study Results

In this study, we determined through both user studies and analysis that the KaZaA application's interface had several critical flaws that may contribute to participants misconfiguring the application and thus inadvertently sharing their private and personal information. All of our study participants used networked computers daily at home and/or in the office for at least 20 hours a week. In the user study we conducted, only 2 of the 12 participants were able to correctly determine that the installation they were given was sharing all files on their hard drive. We conducted a survey with 12 participants and asked them to identify the types of files that could be shared using a P2P network (such as word documents, financial information, spreadsheets, music files, etc.). From the survey, we discovered that 9 out of the 12 assumed incorrectly that only certain types of files could be shared, rather than all files and file types on their hard drive.

We also conducted a study to determine how many other users' unique inboxes we could find from a single KaZaA installation. By using this approach, we hoped to examine how a person on KaZaA could possibly search for others' private information on the network without having to have any sophisticated tools or knowledge. Using this approach we were able to find 150 unique users' inboxes in 12 hours, and almost 1000 users' inboxes in a week.

In addition, we ran a dummy client sharing files that were disguised as personal files such as "credit cards.xls" and the email file "inbox.dbx" to determine if other KaZaA users were searching for and downloading these files from other users. Over 24 hours, we discovered that four unique users had downloaded "credit cards.xls" and two unique users had downloaded "inbox.dbx".

Summary of Conclusion and Findings

The problems we discovered with KaZaA are not intrinsic to P2P architecture in general, nor are they a reflection of an underlying security weakness in P2P systems that causes users to share files without their knowledge. The problems we describe in our report can

be adequately addressed by educating users about P2P and networking in general, and more importantly, improving the user interface for the KaZaA application following the guidelines described in our report. The default settings should recognize that all files are not created equal, and some file types shouldn't be available for sharing by default, such as email, excel spreadsheets, tax returns etc. To provide the maximum protection for users sharing files, the default settings should be configured to prevent sharing of potentially harmful files and file types. Also, the application should make explicit the types of files that it is sharing, and try not to use confusing terminology that may create misunderstands. In addition, any modifications to these settings should be easily recognizable for others who may not have configured the application, but share the computer on which it is installed.

Background of the KaZaA study

Several months prior to our initial study, we became increasingly aware of personal files such as email, spreadsheets and financial documents appearing in search results on KaZaA. We initially assumed that the results were limited to isolated cases, but after several months were convinced that the problem was larger than we initially suspected. An investigation of the user interface of KaZaA, along with anecdotal accounts from several KaZaA users, led us to believe that confusion around the user interface could account for users inadvertently sharing more information than they intended, including the personal and private information we were seeing on the network. We decided to run a study to test our hypothesis.

KaZaA was interesting from a research perspective because it is widely used, has user interface issues that could compromise users' privacy, and has grown rapidly from a small knowledgeable user base to a large user base with many users of very different backgrounds and levels of computer experience. Unlike previous P2P file sharing services such as Napster, KaZaA allowed users to not only share music files in the popular mp3 format, but any other kind of file as well. Also, despite a relatively safe default installation, there were many people sharing personal information without their knowledge. This suggested that a significant number of people had been misconfiguring the application after the installation had occurred. For this reason, we saw this as a problem with the application's usability, and chose to use techniques from human computer interaction to analyze it.

What is Usability and Human Computer Interaction?

Human Computer Interaction is an interdisciplinary field that merges fields such as computer science, cognitive science and design. Its primary goal is to reduce the friction between humans and machines and create a means for people to use machines as intuitively as possible.

One can think of Human Computer Interaction in terms of a highway system. A highway is designed to take people where they need to go, quickly, safely and efficiently. If there are confusing road signs, people may miss exits and have trouble getting where they need to go. If there are ill-designed roads that require people to jump across many lanes to exit, or have sudden curves or blind corners, the effects can be more than just irritating; they

can be deadly. One can imagine several approaches to fixing poorly designed roads. One can put up signs alerting drivers to the dangers or changes, and hope that they read them. This approach could be considered one of education. The other approach is to try to redesign the road altogether, which can be quite costly. Human Computer Interaction is a discipline dedicated to ensuring that users have "smooth" rides when working with applications, improving existing applications that may currently be "bumpy" or frustrating for users, and assisting in redesigning interfaces and interactions that could have serious negative consequences.

It is important to explain the difference between this view and views traditionally discussed on security and privacy. When security breaches are typically described in the common press, they are described as errors or vulnerabilities in the program's code, which allow attackers to take advantage of these mistakes and compromise the system. Typically, these kinds of errors can be corrected or "patched" by writing new code that fixes the problem, and then having the users download and install the "patch", thus plugging the security hole.

For problems that exist with the user interface, however, it is not as simple as writing a patch. Adding more security in the form of data encryption or other technical measures will not help with misconfiguration problems or address problems with miscommunication. Eventually, the data being protected by such measures has to be unencrypted and handled by a user, and it is at this point that the system must help guide the user into making the correct choices and help prevent them from "shooting themselves in the foot" and making fatal mistakes. To fix these kinds of issues, the software creators need to rethink, test and redesign the user interface to properly address the problems.

Details of the KaZaA Study

For our study we decided to look at whether (to the extent that we could measure) sharing personal files was a problem on the KaZaA network, whether other users knew this and were taking advantage of this a problem, and whether confusion with the user interface and assumptions about file sharing could be a cause of this problem.

Can I find other users' private information?

For this question, we wanted to search for unique users who were sharing files that were personal in nature. A very personal file is ones email file. People generally do not want strangers to read their email, so if people were sharing this file then we could assume that they might also be sharing other files that were private. We chose to search for the file "inbox.dbx" because it is common on all Windows machines, which is currently the only operating system that KaZaA supports. It also was a good choice because it typically resides in a folder that contains other private files, which people would not want to share. We ran test queries, and for each test query used the KaZaA function to "search for more files from this user" to see the other files that the user was sharing to confirm that they were sharing more than just the inbox.dbx file. In 19/20 cases, this assumption was correct. In the one case it wasn't, the user was sharing a suspicious collection of many inboxes.

Results

For our initial study, in a 12 hour period we were able to find 156 distinct email inboxes. In a later study performed this year, over a 7 day period we were able to find approximately 1000 distinct email inboxes. In the first study, we looked more closely at a subset of 20 users and found that in addition to exposing files other than "inbox.dbx", 9 users had exposed their web browser's cache and cookies, 5 had exposed word processing documents, 2 had exposed data from financial software and 1 user had files that belonged in the system folder for Microsoft Windows.

Are other users' downloading KaZaA users' personal files?

For this question, we were interested in determining if other users on KaZaA were aware of some users sharing private information, and were taking advantage of this by downloading these files. To test this, we setup a KaZaA client to share personal and private files such a spreadsheet called "credit cards", and the email file described earlier, "inbox.dbx". We let our "honeypot" run for 24 hours and looked at the files downloaded over that period of time.

Results

From our dummy server, we received a total of four downloads from four unique users for an Excel spreadsheets named "Credit Cards.xls" and four downloads from two unique users of an Inbox.dbx file for our initial study. The second follow up study we performed this year had similar results for both file types.

Is the interface confusing users and does it match their assumptions?

For this question, we created a user study to test if users could determine what files were being shared on a KaZaA installation, and if the problems we found in the initial interface analysis contributed to this confusion. In addition, we wanted to learn about the assumptions our users had about the types of files that could be shared on P2P file sharing systems, and how much experience they had with P2P. We had 12 users run through our task and answer a short survey on their computer experience, P2P experience and assumptions on the types of files that could be shared on P2P networks.

Results

10 of the 12 users had used file-sharing programs, and all were considered "experienced" computer users by the standard QUIS metric of greater than 10 hours of computer time a week. Of the 12 users, only 2 correctly identified that KaZaA installation had been set to share all files on the hard drive. In addition, only 2 users correctly indicated that all types of files could be shared over a P2P network. 9 of the 12 users believed that only multimedia files such as music, video and pictures could be shared.

Limitations of the KaZaA study

It is important to note what we did not study. We did not do a study of what percentage of files on the KaZaA network were personal files. The KaZaA P2P network is encrypted, and although reverse engineering the protocol is feasible, this is not currently allowed

under the existing DMCA regulations, and also in the KaZaA user agreement. In addition, even if we were allowed to reverse engineer the protocol, the distributed decentralized nature of the network would make it difficult to look at it in its entirety. However, if we were allowed to reverse engineer the protocol we would be capable of examining the network contents and traffic in greater detail.

Because of these imposed limitations on our ability to conduct a more thorough probe of the KaZaA network, we were limited to automating the KaZaA user interface to perform out searches. A disadvantage of this approach is that it prevented us from knowing how much of the network we are searching at any given time. In addition, KaZaA's distributed "super-node" architecture is such that there is no guarantee that computers will connect to the same part of the network at any given time. For example, two computers may be physically next to each other, but would see completely different search results because they would be connected to different supernodes.

In addition, we did not perform a full scientific study on why users were sharing personal information. We could not speculate on all of the various reasons users would want to change their default settings, although we knew from our data that they were indeed modifying the settings and were not aware of the implications. Our initial goal was to describe how this could happen, given the anecdotal evidence we had from KaZaA users and the types of files we saw being shared. By analyzing this information, we determined that the types of files being shared were similar to files that one would find in system folders, document folders, program folders and in some cases, indicative of users sharing an entire hard drives' contents. Conversations with KaZaA users who were sharing this information and who responded to our requests confirmed that they were sharing these without their knowledge. For this reason, we hypothesized that configuration issues could account for users inadvertently sharing personal files, and we chose to concentrate on the user interface issues.

Also during the course of the study, we did not download any files from users. Although it may have been legal, we felt it was not ethical to take this information from users. The types of files being shared, as well as comments from others who did download these files convinced us that some users were indeed sharing their private and personal information.

Conclusions

Since the publication of our first study, KaZaA has responded by providing an explanation of how to configure the program on their website, although they have yet to modify the user interface. We are hopeful that by providing the information in our report and offering suggestions for improvement, KaZaA will take measures in the near future to redesign the most serious user interface problems we discovered.

The problems we describe are very much part of a larger, more general problem that applies to all networked systems and peer-to-peer systems that store and share users' personal and private information. The problems we described in the report could also exist in email application, knowledge sharing applications and other types of applications

that have sensitive information managed by users on continuously connected networks. We see our work in the context of a new and emerging interest in the field of Human Computer Interaction on providing secure and usable user interfaces to help users manage the complexities of access control for private, semi-private and public information.[2] As the world becomes more networked, and devices and means for sharing and gathering personal information proliferate, work in this area is central to the design of applications that support peoples' privacy and security in a networked world.

Thank you very much for allowing us to present here today.

[2] Yee, Ka-Ping, ICSIS 2002 "User Interaction Design For Secure Systems"

Statement of Senator Patrick Leahy
Hearing Before the U.S. Senate Committee on the Judiciary
"The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-peer File Sharing Networks?"
June 17, 2003

Today's hearing will, I hope, mark the beginning of the Judiciary Committee's serious investigation of the enormous potential of peer-to-peer networks, as well as some of the risks posed when this technology, like so many others, is misused. I cannot overstate my interest in the topic of this hearing, nor my conviction that the Committee has a critical role to play in promoting the potential, and policing the problems, associated with peer-to-peer technologies.

I must note at the outset, however, my concern about the process by which we arrived here this morning. It is critically important that we ensure that we are well-prepared to make good use of the expertise and time generously contributed today by the witnesses seated before us. A careful selection of those witnesses, and a thorough study of their written testimony, are absolutely vital to a useful evaluation of the problems associated with peer-to-peer file sharing. The last-minute rush to put this hearing together has meant that, despite the fact that this hearing is supposed to shed light on the important national security issues raised by peer-to-peer networks, there is no witness here from FBI or the Defense Department or the Department of Homeland Security, who can speak to those issues. In the short time leading up to this hearing, I understand that the Committee majority was simply not able to find anyone who was available. As we move forward to explore this important new technology, I am hopeful that we can work in a bipartisan manner and make real progress.

Peer-to-peer file sharing allows people around the world to share information with one another faster and more efficiently than ever before. Individuals with common interests can easily search each others' shared files, and find a wealth of information that they may not even have known existed. They can then download those files directly from each other with remarkable speed and accuracy. Whether you are in rural Vermont or downtown Los Angeles, you – and everyone else with access to the network -- can have all the information you need. And because there is little centralization of the networking process, minimal infrastructure is needed. Thus, peer-to-peer networks can operate in hostile places, without fear that the network will be shut down. In Iraq, for example, peer-to-peer has been used, and is still being used, by humanitarian groups who need to share critical information needed to carry out their missions.

Peer-to-peer has the potential dramatically to change the way we share information, but it is not new to the Internet. In fact, peer-to-peer merely refers to any network that allows users to share information directly with each other, with little or no centralized control. We should not forget that email, and even the world wide web itself, are both types of peer-to-peer networks. When these

networks first developed, they also presented serious concerns, and this Committee, both under my leadership and that of Chairman Hatch, correctly took the lead in responding to those concerns. With the expertise and the mandate needed to address these important issues, this Committee has focused on such issues as online privacy, the availability of pornographic materials on the web, computer piracy, and the dangers of computer viruses. By and large, we have responded appropriately to these challenges, by allowing the communities that use these technologies to find the most efficient and effective ways to deal with their concerns. Only where absolutely necessary have we stepped in to regulate in cyberspace. As a result of this careful work, new technologies have developed, with new uses and more powerful abilities -- and they have developed largely without hindrance.

Like email and the world wide web, peer-to-peer file sharing holds simultaneously enormous promise and the danger of harmful misuse. At its core, it has two components. First, it allows a user to search any of millions of computers for a particular file or kind of file. Next, it allows the user to download those files extremely quickly, directly from others on the network. Despite the promise of these networks, there are problems with some of the ways peer-to-peer is used. Peer-to-peer makes it quite easy to share copyrighted materials. It has also become clear that peer-to-peer networks offer an easy way for people to share pornographic materials, often child pornography, and may allow sexual predators a way to lure their victims into an instant messaging conversation. These are very serious concerns, and I look forward to working with Chairman Hatch and the rest of the Committee to address them. Today's hearing, however, was apparently designed to focus on another important aspect of peer-to-peer networking, the personal and national security problems it may raise.

First, peer-to-peer file sharing can render a user's entire hard drive vulnerable to download by anyone else using the network. This is because the default setting on some of the programs will search your hard drive for any video or audio files, and then make *everything* in that folder available for download by *anyone* on the network. Thus, if there is one picture in your "My Documents" folder, the software will recognize it and make all of the "My Documents" folder available for download. You can commonly find personal information like tax returns, credit card information and medical documents on peer-to-peer networks, and many of the users have no idea that they are sharing this information with everyone else on the network. If the user is a government employee and the computer is a government computer, sensitive government information could be made available to those unfriendly to the United States. Here in the Senate, of course, the firewalls installed by the Sergeant at Arms are intended to keep us safe from these dangers by effectively eliminating the possibility of file sharing using Senate computers. But I also understand that not all government offices have such protections in place, which presents the ominous possibility of genuine risks to national security interests.

Second, some peer-to-peer software is designed to circumvent firewalls and other security protections intended to keep peer-to-peer off a computer or network. This prevents parents from protecting their children from adult content, and also prevents network administrators such as universities from keeping unlawful uses of peer-to-peer off their networks. Many networks would choose to preclude peer-to-peer because the software tends to use up a lot of bandwidth. Parents and those who run computer networks should be able to keep peer-to-peer off if they choose to.

Third, certain peer-to-peer programs include "spyware" and "adware." These two types of software track an individual's Internet browsing, and can record any information sent via the Internet, like credit card numbers. They then send that information to marketers, allowing targeted "pop-up" ads and spam. Because they collect personal information, spyware and adware may contribute to identity theft. Spyware and adware often get installed on the user's computer with little or no notice to the user.

These problems are serious ones, but they are not new. In my Privacy Report Card for the 106th Congress, I noted: "Increasingly, personal information such as diaries, finances, and schedules, will not be stored on hard drives, but instead on Internet-based files. Combined with the reality that a substantial amount of our information is being carried over the 'Wireless Web' access to our personal information–by private and by public snoopers–is also growing exponentially." What is new is the public awareness of the risks posed by peer-to-peer, and the urgency we in Congress are feeling about the best ways to address those risks.

And while these problems are serious, they are not insurmountable. The inadvertent sharing of files may well be remedied by improving the instructions and warnings that users are given when they install peer-to-peer software. The software also need not have the ability to circumvent firewalls to work effectively. Finally, peer-to-peer need not insert spyware or adware on a user's computer to work. None of these programs are necessary elements of peer-to-peer technologies. And the problems they raise can be solved, or better yet avoided, if good corporate citizens and good cyber citizens take the responsibility to do the right thing.

I look forward to hearing from our witnesses and to working with all members of the Committee and with the many online communities to help people to solve these problems. We will hear from Senator Feinstein, who has worked so hard to address the problem of identity theft, and Representatives Waxman and Davis, who, as usual, held a very informative hearing on this subject in the House of Representatives last month. I am disappointed that appropriate witnesses from the Administration are not here to discuss the national security aspects of the peer-to-peer problem. We will hear from Chris Murray, the Telecommunications Counsel of Consumer's Union. Mr. Murray has been invaluable in the protection

of consumers' interests in the online and telecommunications world. We will also hear from Randy Saaf, the CEO of Media Defender; Alan Morris, the CEO of Kazaa Networks, the most popular peer-to-peer file sharing program; and Nathaniel Good and Aaron Krekelberg, who have researched the problem of inadvertent sharing of personal information on peer-to-peer networks.

# # # #

Statement of Mr. Alan Morris, Executive Vice President,
Sharman Networks Limited
Before the
Senate Judiciary Committee
Regarding
Security Considerations for Peer-to-Peer Networks
Washington, DC
June 17, 2003

Chairman Hatch and members of the Committee, I want to thank you for this opportunity to share the views of Sharman Networks Limited (SNL) regarding security considerations for peer-to-peer (P2P) technology. I am Sharman's Executive Vice President and, as it is a global business, I am responsible for supervising the enterprise whilst Sydney is off-line at night. I also have specific responsibility for developing the promotion and distribution of licensed content in conjunction with Altnet. I am accompanied at the witness table today by Mr. Derek Broes, Executive Vice President of Worldwide Operations for Los Angeles-based Brilliant Digital Entertainment (BDE). BDE's Altnet service is available to all users of the Kazaa Media Desktop (KMD) software. Altnet is the largest distributor in the world of licensed and protected media files, as well as the leading purveyor of files utilizing Microsoft Windows Media digital rights management (DRM) technology. Mr. Broes is a recognized expert on Internet security, and Altnet is now in the process of rolling out a new high-security file-sharing network for users of KMD. He has submitted a formal statement to the Committee that I would ask to be made part of today's official hearing record.

We commend the Committee for scheduling this important hearing. P2P is a natural step in the evolution of the Internet. It is seen by many as a powerful and beneficial technology for maximizing the efficiency of computing and network resources, as well as a medium for making information and media available to a worldwide audience at the lowest conceivable cost. But P2P is hardly the end point of the Internet evolution – it is a way station toward fully distributed computing applications commonly referred to as

"grid computing". As described in the article "The Grid: Computing Without Bounds" which appeared in the April 2003 issue of Scientific American, *"Grid computing refers to the large-scale integration of computer systems (via high-speed networks) to provide on-demand access to data-crunching capabilities and functions not available to one individual or group of machines...[It] enables large-scale scientific and business collaboration among members of virtual organizations, remote experimentation, and high-performance distributed computing and data analysis."*

That same Scientific American article recognized Kazaa's legitimate place among new distributed computing technologies: *"The concept of globally virtualized grid computing is a natural extension of today's Internet. The Internet virtualizes communications, permitting any person to connect with any other person or device, regardless of location or the means used to do so. The result has been an explosion of innovative functions: e-mail, the World Wide Web,* ***peer-to-peer applications, including file-sharing systems such as Kazaa****, and simple distributed-computing schemes such as SETI@home and the Smallpox Research Grid."* (Emphasis added)

SNL's Commitment to User Privacy and Security

From inception, Sharman Networks Limited, owner and operator of the Kazaa Media Desktop (KMD), has taken great care to protect users' privacy and security. As the most popular peer-to-peer application, KMD has consistently lead the field with security enhancements developed specifically for the challenges of this new industry, including peer-to-peer's first anti-virus tool.

Kazaa Media Desktop is the only P2P application that includes specifically designed and fully integrated third party virus protection software. 'BullGuard', one of the most advanced proprietary virus protection technologies available, has been installed free to users of KMD since late 2002 and provides an additional layer of protection over and above any antivirus software users have already installed on their computers.

Sharman Networks takes every opportunity to encourage responsible and safe peer-to-peer usage through user education as well as via the default configuration of the software. The nature of decentralized peer-to-peer technology means that users control the material they choose to share with others. Our goal is to provide users with the tools they need for safe and responsible use, though the decision to share material is always at the users' discretion.

The Kazaa.com website provides users of KMD with extensive information to enable them to achieve desired levels of security. Our Privacy Statement provides clear and extensive disclosure of our consumer-friendly policies regarding information collection, use of "cookies", and opt-out mechanisms. Kazaa has a firm "No Spyware" policy to protect users against software that is either surreptitiously installed or which covertly gathers user information. Our Security and Privacy guide is constantly scrutinized and upgraded in the light of usability trials and third party reports and instructs users on how to engage in safe sharing and protect themselves against computer viruses. Our Setup guide provides detailed information as to how users may disable file sharing and activate our password-protected Family Filter to block the inadvertent download of offensive and adult material, as well as to activate additional filter options that can block file types known to transmit viruses, files that would not be blocked by a firewall, and bogus files. We believe that we have the most extensive and effective protection policies and capabilities of any P2P software available today. But we are not resting, and are continuously testing further improvements consistent with our role as the P2P technology leader.

The availability of offensive materials, in particular any involving children, on every search engine including Yahoo and Google is a great concern of ours. Like those companies mentioned, we are making great efforts to educate and when possible, work with authorities in their efforts to mitigate the problem. We aggressively encourage the use of our built in family filter and believe it should always be used in households where children may have access to the PC. We also believe filters can never take the place of active and involved parenting.

Sharman Networks is committed to the security of its software and has proven that it will take the proactive steps necessary to defend the integrity of Kazaa Media Desktop, including addressing any new malicious viruses that 'freeze', 'silence' or otherwise compromise a user's experience. Sharman continues to maintain its role as market leader and will continue to set best practices and high standards for the burgeoning growth of P2P in general.

Inadvertent Sharing and Identity Theft

Mr. Chairman, identity theft as a byproduct of using P2P software remains a hypothetical threat. Last month James Farnan, the Deputy Assistant Director of the FBI's Cyber Division, told the House Government Reform Committee that *"no instances of identity theft have been reported to be associated with P2P networks"*. Despite the assurance this gives in the short term with regard to the competency of our existing systems, we are never complacent – Sharman will continue to do everything possible to make use of the KMD completely secure by default; with a design so intuitive that users cannot inadvertently share personal files, and so clear in its operation that users can easily ascertain exactly what files they are sharing.

We take responsible critiques of our software very seriously, and we respond to them quickly. We welcome intelligent research such as "Usability and privacy: a study of Kazaa P2P file-sharing" (the "HP study") first published by Nathaniel Good and Aaron Krekelberg last year and updated in April 2003, and we integrate such thinking into our product development plans. As soon as we received that study we compared its findings with the focus group user sessions we have conducted by independent third parties. Version 2.5 of KMD, now in beta release and soon to go public, incorporates a variety of security changes to prevent inadvertent file sharing during KMD installation, prevent a change in the location of the "My Shared Folder" that might lead to accidental sharing of preexisting folders, and make it far easier for users to determine what they are sharing. In particular, any user who attempts to share an entire drive, including their hard drive, now receives a very strong warning against doing so. Users are more definitively encouraged

to maintain the KMD default settings, which designate the My Shared Folder as the only shareable location. The "Participation Level" portion of our online guide makes clear that preferential queuing for a requested file depends on the ratio of uploaded to downloaded megabytes and not upon the total megabytes available for sharing. In other words, making lots of files available, that others are not likely to be interested in, provides no benefit. Users are likewise rewarded for rating the integrity of files. The goal of our participation level policy is to maximize the functionality and integrity of the Kazaa P2P experience.

We would note that, in testimony before the Government Reform Committee last month, the authors of the HP study stated, *"The problems we discovered with the Kazaa interface are not intrinsic to P2P in general, nor are they a reflection of an underlying security weakness in P2P systems... [They] can be adequately addressed by educating users about P2P and networking in general, and more importantly, improving the user interface."* As noted, we took their study seriously and have made the recommended upgrades.

P2P in Perspective - User Education Needs

Mr. Chairman, while some entertainment industry executives have embarked upon a campaign to demonize P2P, the risks associated with this digital technology are neither unique nor exceptional. Jeffrey Schiller, Network Manager and Security Architect for MIT, testified before the House Government Reform Committee last month that, *"In some ways they [P2P programs] are more secure than E-mail...File-sharing programs, as viewed by the end-user are no more or less secure than other common Internet applications such as web browsing or reading E-mail...* ***The risks are slightly different, but the magnitude of danger is about the same."*** (Emphasis added)

Indeed, Congress could keep itself very busy holding hearings on the security flaws of all sorts of well known, branded digital software. In just the past few weeks, the press has carried reports that:

- Vulnerability in the Microsoft Windows Media Player could enable an attacker to execute an attack on the computer of a user who downloads a new "skin" for the player.
- The latest version of America Online's ICQ instant messaging software contains a flaw that could allow an online attacker to take control of a user's computer.
- Microsoft acknowledged a security flaw in its popular Internet Passport service that left 200 million users vulnerable to hackers and thieves, and that may have been in violation of an FTC consent order regarding the veracity of its claims for Passport's security and privacy protections.

These are just a few of many possible examples. Certainly, any software flaw that has the potential to let a third party take over one's computer is the ultimate security risk and the most egregious form of digital identity theft. What is required in response to such reports is not accusation and vilification, but immediate remedial actions combined with a long-term commitment to improving basic education on security risks for all computer users. We cannot overemphasize the need for improved user education, especially as we move into an "always on" world of broadband connectivity through both wired and wireless access. While one must undergo extensive training and obtain a driver's license to cruise the interstate highways, absolutely no such prerequisites apply to surfing the information highway. We are hardly about to suggest that government impose a licensing requirement for Internet use, but government should promote the need for a greater level of public understanding of the risks of all forms of public Internet activity and the ways that they can be effectively managed.

The pressing need for such education was brought home by last week's release of "Fast and Present Danger: In-Home Study on Broadband Security Among American Consumers", a study conducted by America Online for the National Cyber Security Alliance. That study revealed that for broadband users in general:

- 97% of broadband parents do not use parental controls
- 67% of users do not have properly and securely configured firewalls
- 62% do not regularly update anti-virus software

- Despite vulnerabilities, 86% keep sensitive information on their home computer

The adoption of broadband is both inevitable and desirable. For years policymakers in Washington and other capitals have debated how to best encourage more rapid adoption of broadband to create the infrastructure for the long promised wide range of innovative new products and services. Commentators, telecommunications companies and service providers all agree that P2P is the "killer app" that has finally given the public the incentive to acquire broadband and so drive the development of the many societal and commercial opportunities created by a high speed wired world. But the public and private sectors must do far more to help educate users about the inherent risks of fast connectivity, as well as the available and effective means for ameliorating them.

External Threats to P2P Security

Mr. Chairman, Sharman Networks is committed to continually improving security and privacy safeguards for the tens of millions of users of Kazaa Media Desktop worldwide. Indeed, much like companies such as Microsoft and AOL in other Internet sectors, Sharman has set standards for security in P2P. However, real threats to the security of the computers of millions of P2P users around the world arise from the activities of those who seek to portray themselves as being impacted negatively by P2Ps existence. From its inception, Sharman Networks has been dedicated to legitimate and licensed uses of P2P technology that compensate copyright owners and reward creators. But content industries have yet to fully understand and embrace the commercial benefits available to them through P2P. As Michael J. Wolf, Managing Partner of McKinsey & Company's Media and Entertainment Practice wrote in a May 1, 2003 Wall Street Journal opinion piece on digital music services: *"But what's missing from the equation are the file-sharing services themselves, sites like Morpheus, Kazaa and Grokster, which attract 30 million consumers every month. These are the killer apps of the broadband computing world, and one presumes they'd rather attract revenues than lawsuits."*

Indeed, we would much prefer to enter into mutually beneficial agreements that serve artists and the public. But the entertainment sector does not seem to be ready to admit that P2P can be their path to prosperity. Until they realize that, some of their current tactics constitute a clear and present danger to the privacy and security of P2P users

In this regard, we recommend that this Committee should overview the "software bullet" technology initiatives being funded by the entertainment industry. A front page story in the May 4, 2003 New York Times reported that, *"Some of the world's biggest record companies, facing rampant online piracy, are quietly financing the development and testing of software programs that would sabotage the computers and Internet connections of people who download pirated music, according to industry executives...The covert campaign, parts of which may never be carried out because they could be illegal under state and federal wiretap laws, is being developed and tested by a cadre of small technology companies, the executives said."* Among the technologies reportedly being tested and developed are those that lock up computers for hours, delete files from hard drives, and disrupt Internet connections. Such technologies pose a grave threat to both individual users and to ISPs. As Stanford Law School Professor Lawrence Lessig noted, *"Freezing people's computers is not within the scope of copyright laws."* Hard questions need to be asked about why public companies are investing in the development of technologies that are illegal to implement. Congress also has a right to know what precautions are being taken to make sure that these malicious viruses do not "escape from the lab", and what steps the financers and developers of these dangerous technologies will take to admit responsibility and advise the public of effective countermeasures in such a situation. Otherwise, there is a distinct possibility of extreme disruption of computer networks and substantial economic loss to their users occurring without public awareness of the source of the infestation.

Further, the activities of the Entertainment industry in pursuing their ends are seen by many observers to constitute a real threat to public privacy: As former Clinton Administration chief privacy officer Peter Swire commented; *"The RIAA's position* (on

gaining subscriber identities from ISPs..) *would make it trivially easy to learn the name, address and phone number of anyone who sends e-mail or visits a website".*

Conclusion

Mr. Chairman, thank you again for providing this opportunity to discuss privacy and security considerations related to P2P software. While P2P is not without risks neither is any Internet experience, and its present and potential benefits far outweigh them. We at Sharman Networks will continue to make improvements that reduce the chances of inadvertent sharing of sensitive files, and to educate our users regarding the basics of online protection. And we stand ready to work with this Committee, other agencies of government, enterprise and public interest organizations toward shared goals of educating and protecting consumers.

I would be pleased to answer any questions you may have.

Consumers Union
Publisher of Consumer Reports

Testimony of Chris Murray, Legislative Counsel, Consumers Union

Before the

United States Senate Committee on the Judiciary

Regarding

The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-peer File Sharing Networks?

June 17, 2003

Washington Office
1666 Connecticut Avenue, Suite 310 • Washington, D.C. 20009-1039 • (202) 462-6262

Chairman Hatch, Ranking Member Leahy, and other distinguished members of the Committee, I am grateful for your invitation to testify today.

Consumers Union,[1] as publisher of Consumer Reports magazine, is an organization that makes its living based on the trust of readers and compensation for our intellectual property. Since the first issue of Consumer Reports arrived in mailboxes in the 1930s, we have built our reputation on a love for technology and a desire to make technology safer and better for consumers. Today's hearing presents us another opportunity to scrutinize a technology with enormous promise and enormous problems.

Before we dive into the "Dark Side" of peer-to-peer, what does peer-to-peer distribution (P2P) mean exactly? Peer-to-peer technologies allow the sharing of resources between computers, whether sharing content, storage, computing cycles, or bandwidth. One of the most popular P2P application today is the Kazaa Media desktop, which has been downloaded over 200 million times and claims over 60 million users worldwide. Other popular P2P content-sharing tools like Morpheus and Grokster have millions of users as well.

But other applications, like email, instant messaging and the Internet itself, would likely fall into anyone's definition of what is P2P. If you'll permit me to jump ahead of myself, here is the punchline of my testimony: when we begin to explore solutions to the problems presented by P2P, such as serious security and privacy issues, not to mention the tremendous volume of piracy facilitated by P2P, we will find that as we try to define what exactly P2P is with precision, our definitions start folding back on themselves, blurring attempts to draw boundaries between what is P2P and what is the Internet. The fundamental architecture of the Internet is that of P2P. Any attempt to regulate P2P as such may entail a regulation or even redesign of the Internet as a whole.

This is by no means to belittle the security and privacy concerns implicated by P2P technologies—in fact I hope I will be heard to be saying the exact opposite. It is precisely because the security and privacy of consumers are so critically important that Congress should beware anything that appears to be a magic bullet. There is no broad, easy legislative fix as far as we can see.

Congress's near term role should be narrower, to avoid the risks of unintended consequences. Congress would do well to spur an investigation of the practices alleged here today, regardless of whether they involve, strictly speaking, peer-to-peer

---

[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.

technologies—the fact is that there is an epidemic of spyware and adware in P2P applications, and the epidemic is not limited to P2P. Many mainstream applications such as media players and Web browsers seem to contain or at least enable similar spyware and adware and should be included in any such investigation. Companies who use spyware must provide consumers with notice that they are doing so and should be held accountable by policymakers and in the marketplace.

There is something I believe everyone in the room can agree upon: innovation is the root of what makes this country strong. It is instructive that this is one of the few things that the Framers of the Constitution were explicit about. It is the business of Congress and the Courts to promote the progress of the arts and sciences.[2] Today's hearing title clearly indicates that the committee understands the power and potential of peer-to-peer networking, and is seeking to ensure that P2P is on the right track. As with any new technology, P2P has its risks along with its benefits.

Let's remember as we go forward to keep our eyes on the benefits. Peer-to-peer network architecture could once again revolutionize the way our citizens create, communicate, and collaborate—assuming that misuses of the technology do not overtake legitimate uses. The promise of peer-to-peer is almost as significant as the Internet itself. As of 2001, the computers connected to the Internet represented at least 10 billion megahertz of power and 10,000 terabytes of storage.[3] Peer-to-peer brings with it the potential for dramatic cost savings, including the ability to do massive parallel processing.

Intel, Novartis, the University of California and NASA have saved money and time by developing P2P programs that combine unused computer processing power instead of using expensive supercomputers. GlaxoSmithKlein, Hewlett-Packard and the Naval Post-Graduate School are using peer-to-peer applications that support and encourage collaboration, by virtue of shared documents and information,from students and employees worldwide.

Yet the peer-to-peer applications used by most consumers today come saddled with troubling design that compromises users' security—intentionally or unintentionally—and while outside the scope of today's hearing, we must keep in focus the fact that certain P2P systems are widely used as a tool to illegally share copyrighted works.

One may ask, given the costs to copyright holders that such peer-to-peer applications pose, why is peer-to-peer worth protecting? Assuming we could squash it, why not just do so if it's mostly used for piracy and pornography, and as we're learning today, if it's rife with security problems, crawling with spyware and adware?

---

[2] United States Constitution, Article 1, Section 8: "The Congress shall have power . . . [t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries;"

[3] http://www.guardian.co.uk/Archive/Article/ 0,4273,4139668,00.html

The answer is that we dare not throw the baby out with the bathwater. To show you what we might lose if we mis-regulate peer-to-peer, let me give you a few examples of the real power of peer-to-peer, examples why this is a technology worth setting on course so that it can blossom into its full potential.

Beneficial Uses of Peer-to-peer

Through peer-to-peer distributed computing, normal users like you and I can cooperate with scientists by donating our computers' idle processing power to help researchers simulate protein folding. When our computers are doing nothing other than running our screensavers, we can cooperate with a project such as Stanford's "Folding@Home,"[4] and help researchers to discover the causes of Parkinson's disease and Mad Cow disease.

Oxford's Centre for Drug Discovery[5] uses peer-to-peer distributed computing in the search for new drugs in the treatment of cancer, and is now looking for a cure to Smallpox.

Intel's "Philanthropic Peer-to-peer Program"[6] was created to demonstrate the power of peer-to-peer distributed computing and increase the acceptance of such applications by the general public, in order to enhance scientific research.

Others, like the SETI@Home project,[7] are using P2P distributed computing to discover our universe and listen for hints of life beyond our planet.

And beyond research, some consumers are using peer-to-peer to fight back against spam by participating in a collaborative spam filtering system called "SpamWatch."[8] Each user on the SpamWatch system tags unsolicited commercial emails he or she receives as spam. When multiple users tag something as spam, SpamWatch will filter out similar emails to other users.

BitTorrent is a P2P tool for copying files from one machine to another, and is different from the Internet's common file distribution methods. Typically, the more popular a software program or independent movie is, the harder it is to download. BitTorrent changes that. As more users download a program or independent movie or a large scientific database, BitTorrent makes that file available to other people from users that have already downloaded the file, rather than clogging up bandwidth by continually getting the file from a central server. Bandwidth is expensive, and independent moviemakers and software developers often cannot afford to distribute their content once it becomes popular. BitTorrent, and other similar P2P technologies take advantage of

---

[4] *See* www.stanford.edu/group/pandegroup/folding.
[5] *See* www.chem.ox.ac.uk
[6] *See* www.intel.com/cure.
[7] *See* http://setiathome.ssl.berkeley.edu.
[8] *See* www.cs.berkeley.edu/~zf/spamwatch.

that popularity, which means more efficient downloads for everyone who wants to use that software or watch that new movie. BitTorrent doesn't solve the "last mile" problem facing commercial broadband users in this country, but it does ease the burden a bit, allowing users to make maximum use of the bandwidth they have purchased from a broadband provider.

P2P is also being used for national defense. DARPA has funded the Terrorism Information Awareness program to look at ways peer-to-peer applications can be used for intelligence gathering.

These applications and many others make it clear that peer-to-peer is more than just a means to illegally share multimedia files. But as we develop new models of cooperation and communication like peer-to-peer systems, we are of course confronted with new challenges along with these opportunities for new business models. As our other witnesses here today have detailed, users of peer-to-peer systems must guard against some substantial privacy and security risks.

Security and Privacy Risks for P2P Users

When a peer-to-peer user first installs file-sharing software such as Kazaa on his or her computer, the program looks for files to share. This becomes a particular problem when the software's code aggressively searches the computer's drive, grabbing files that the user might not imagine would potentially be shared. As the authors of the Kazaa usability study[9] found, dozens of users were unwittingly sharing sensitive documents like their tax returns, email inboxes, and check registers. By using Kazaa, these users were leaving sensitive personal data and personal communications exposed to millions of users around the world.

It seems certain that much of this sharing of personal information is not intended by users and due in part to faulty interface design. Many people have no idea that any files they download will automatically be shared, nor do they realize that they may accidentally open up entire file folders for sharing if they save a shared file to one of those folders.

A more troubling privacy and security issue facing P2P networks, however, is the invasive, nonconsensual use of "spyware" and "adware" programs. Spyware is a generic term that describes software whose purpose is to collect demographic and usage information from a person's computer, typically for advertising purposes. Not all adware is spyware. Spyware programs target advertisements based on a user's location, browsing habits, search engine queries and other criteria, while adware programs display advertising, but do not track or report a computer user's behavior.

---

[9] Good, Nathaniel S., and Aaron Krekelberg, *"Usability and Privacy: A Study of Kazaa P2P File-Sharing."* June 2002. Available at www.hpl.hp.com/shl/papers/kazaa/index.html.

Advertising-supported software, if implemented properly and with user consent, can be beneficial for both developers and consumers. Software developers can make money off their creation and the user gets the software for free. But some freeware and shareware authors bundle spyware programs as a hidden component, suggesting they know users dislike such software and figure that the best or only way to ensure its widespread use is to prevent the end-user from discovering it.

Documented examples of spyware include:

> "W32.Dlder.Trojan," a "Trojan Horse" program capable of tracking the Web sites users visit and relaying that information to a third party. This has been found in past versions of popular file-sharing programs such as BearShare, LimeWire, and Kazaa.[10]
>
> "vx2.dll," a spyware program file packaged with certain versions of Audio Galaxy, capable of capturing lists of Web sites visited, creating pop-up ads, and even capturing users' input into Web forms and comment boxes—potentially even sensitive information like credit card numbers or Social Security numbers.[11]

Kazaa has a long-standing "no spyware" policy. This is a great idea, and a step in the right direction. But when Kazaa is installed, the default option apparently installs three adware applications, from Cydoor, DoubleClick and SaveNow.

Technically, a user agrees to this when they install Kazaa or any other software application that bundles adware. But not many users read the End User Licensing Agreement when they install software, nor would it be easy to find the relevant information even if did.

And while peer-to-peer programs commonly bundle spyware and adware with their products, alarmingly, so do more mainstream software companies such as Microsoft, AOL, and RealNetworks.

AOL Time Warner/Netscape's "SmartDownload"[12] and RealNetwork's "RealDownload" assigns users a unique ID number and keeps track of every file downloaded. Worse, for anyone who had ever purchased a RealNetworks product in the past, RealDownload sent users' names and e-mail addresses back to Real's servers during every download.

---

[10] Delio, Michelle, *"What They Know Could Hurt You."* Wired News, Jan. 3, 2002.
[11] Benner, Jeffrey, *"Spyware, In a Galaxy Near You."* Wired News, Jan. 24, 2002.
[12] Hansen, Evan. *"Netscape Settles NY Privacy Suit," ZDNet. June 16, 2003. See* http://zdnet.com.com/2100-1105_2-1017275.html *"The New York Attorney General's office said on Friday Netscape would pay $100,000 as part of a settlement of complaints about a feature used by the unit of America Online to track what users downloaded online. Netscape would also delete all URLs and related data it has obtained through its SmartDownload browser software and undergo privacy audits, the Attorney General's office said. The settlement comes after a two-year probe, begun in 2002, into Netscape's collection and retention of information that identified files downloaded by users, which contradicted its statement to consumers that none of the information was saved."*

Microsoft's Windows Media Player 8 was reported to be collecting information on what movies and music consumers were listening to and watching, and sending that information back to Microsoft. The European Union launched an investigation of the spyware alleged to be lurking within Microsoft's software last year.[13] While Microsoft was clear that it was not selling that information to third parties, nor was it associating users' identities with the playlists, consumers were understandably concerned about their media habits being tracked.

I believe it is important to separate what is a peer-to-peer specific issue and what is not. In the case of Kazaa's spyware, I see this to be an issue of public domain software that is advertising supported. When a business has no income stream other whatever data it can sell and whatever advertising it can serve, we have a recipe for egregious violations of users' security and privacy. But this recipe exists in many business models beyond P2P.

Due to design of the software, and especially because of the prevalence of spyware and adware on peer-to-peer systems, we must consider the real threat that misuses of peer-to-peer technology could potentially overtake good ones yet to emerge.

Solutions

So what is to be done? Inevitably, every new technology requires a period of social adaptation and transition. Most mistakes are made in that transition period. When we first developed the telephone network, it became possible for people to give away information to strangers in new ways, and many consumers were taken advantage of as a result. Over time, people learned to maintain a certain degree of skepticism with phone solicitors. The advent of email also came with its own learning curve—people did not realize how easy it is to forward something and often got burned by writing something that was passed on.

Peer-to-peer sharing of resources is part of the fundamental design of the Internet and it simply cannot be turned off in any categorical way. There is simply no way to define what is peer-to-peer and wall it off from the rest of Internet traffic without redesigning the Internet. But we can reduce risks to acceptable levels. In the national security environment, we can do that through policy—we can instruct workers and employees not to engage in certain kinds of risky behaviors. I think we can safely say that if you work at the NSA, CIA, or DIA, for example, you have absolutely no business running filesharing services for the purpose of sharing or obtaining unlicensed commercial content.

To protect normal consumers using P2P, first and foremost, we need to educate people about how the software works, and how improper configuration can expose one's

[13] Muriel, Diana. *"Microsoft, Real Face 'Spyware' Probe,"* CNN.com June 17, 2002. http://edition.cnn.com/2002/WORLD/europe/06/17/eu.cookies.

entire computer to the public. Education needs to extend to parents, since often a young person will download a peer-to-peer product without the knowledge of their parents. Parents need to know to look for software such as Kazaa that may expose their personal files to undue risk.

However, it may be that there is no educating around a design problem. If spyware and adware are inherent in the design of certain kinds of software, there may be little that educating consumers can accomplish. The most efficient solution I can offer today is that users should reject bad software design, but they first need to know what is "good" and "bad" software. Any company that uses spyware and adware should notify their consumers they employ such practices and should be held accountable for doing so. Our publication, Consumer Reports, is based on the fundamental belief that properly informed consumers will make better decisions. We believe better information about the risks of "bad" software will lead consumers to reject such software in the marketplace.

But how can we determine what the "bad" software is? Policymakers could help fill the gap by investigating the most prevalent uses of adware and spyware currently being employed. I encourage the Committee to urge the Federal Trade Commission to open an investigation regarding spyware and adware in the market. Given what we are learning today about peer-to-peer, it seems critical that peer-to-peer be included in that investigation—however, it also seems essential that any investigation include within its purview use of spyware by vendors of media players and how Web browsers may facilitate use of spyware and adware by individual Web sites.

The globally interconnected nature of the Internet creates the same threat to users as leaving one's house unlocked. The best locks and security system available won't do any good if one leaves keys in the door. Regardless of whether users are using peer-to-peer applications, there are many other "front doors" that can be left unlocked, many ways security and privacy can be compromised.

Our magazine, Consumer Reports, recommends that all Internet users run a virus checker and have it scan the computer at least one time every week, especially if users have broadband connections. Additional protection can be had by installing a firewall, or even better, by using a router with a built in firewall. Consumers also need to be very careful about downloading programs where they do not know and trust the source—email attachments are the source of many viruses and spyware.

Users have several means available to determine if the programs they download contains spyware or adware. First, consumers should download programs from downloading portals—sites that offer a large selection of programs for almost every purpose. The best of these portals make clear which programs bundle spyware or adware and which programs do not. Second, when installing software, computer users should always select the "Custom" option. This option often gives the user an opportunity to deselect third-party software.

As I said before, Congress would do well to spur an investigation of the practices alleged here today, regardless of whether they involve, strictly speaking, peer-to-peer technologies—the fact is that there is an epidemic of spyware and adware in P2P applications, and the epidemic is not limited to P2P. Many mainstream applications such as media players and Web browsers seem to contain or at least enable similar spyware and adware and should be included in any such investigation. Companies who use spyware must provide consumers with notice that they are doing so and should be held accountable by policymakers, which will allow consumers to hold them accountable in the marketplace.

In sum, because the technologies that underlie P2P are so deeply intermingled with the underlying design of the Internet itself, and because the Internet has proved itself to be an amazing engine of commerce and economic growth, the best that Congress can do now is to identify and bring sunshine to particular problems. Once those problems have been identified, it may be appropriate for Congress to suggest or develop narrowly crafted, rifle-bullet solutions to those problems. Any attempt to demonize P2P or even existing P2P applications is likely to reach too far and have unintended consequences. What we most want as we step into this new era is that all of our regulatory consequences be intended ones.

Written Testimony for the U.S. Senate Hearing on "Security Concerns Associated With Peer-to-Peer Networks"

By: Randy Saaf, President of MediaDefender, Inc.

June 17th, 2003

My Name is Randy Saaf, and I am the President of MediaDefender. MediaDefender is one of the largest P2P anti-piracy software companies in the world, and has some of the most sophisticated tools for understanding P2P networks. I want to make it clear from the outset that there are security risks associated with all types of computer software, not just P2P. That being said, there are some very specific security concerns associated with P2P networking that the public should be aware of. Usually, only very sophisticated, trained computer users get involved with networking software. The numbers of users on P2P would suggest that most are not sophisticated and most do not know the ramifications associated with pushing buttons and altering settings in the program. The two main security concerns I would like to address in my testimony are private individual data being unintentionally shared and P2P software allowing content to be shared at government institutions. Lastly, I will discuss measures that can be taken to prevent some of the security problems associated with P2P.

In the summer of 2000 Napster was hitting its stride as the hottest Internet software application since the web browser. As we all know, the primary use of Napster was for the illegal trading of copyrighted music over the Internet. This was the birth of the P2P movement that continues to build momentum even today. At its peak Napster had roughly 40,000,000 users. Today, P2P networks, such as KaZaA, Gnutella, and WinMX, have roughly 80,000,000 users and are used to trade all sorts of rich media including pictures, music, pornography, television shows, and movies. Additionally, most modern P2P networks allow the trading of documents and executables (software programs). The trading of documents and executables raise a host of security concerns. These same security concerns were not present with Napster, because it only allowed trading of audio files (MP3s). Generally, sensitive information is not present in MP3s, and it is near impossible to embed viruses or create security holes using an MP3.

MediaDefender was founded in the summer of 2000 with the company calling to "Fight Crime on the Internet." MediaDefender's primary business is to prevent the illegal distribution of copyrighted material over P2P networks. However, lately many companies and schools have been hiring MediaDefender to advise them on the security holes associated with P2P software running on their networks. MediaDefender is able to use the same tools is has for fighting piracy to find and prevent some of the security problems created by P2P networking software. These very sophisticated tools give MediaDefender some clear insight into the security risks associated with P2P networking, and I intend to share some of that insight in this hearing.

I want to make it clear that MediaDefender is not anti-P2P networking or anti-technology. Everybody at MediaDefender believes that advances in technology are beneficial to society as a whole. P2P networking is a huge evolution in the Internet and will have countless legitimate applications. However, as with many advances in technology, several problems have arisen that should be addressed now before irreparable damage is done.

All security concerns associated with P2P networking arise out the file sharing aspect common to every program. A user of P2P software can share any or all of their hard drive with a few mindless key strokes. By default, most P2P software programs create a common directory for downloading and sharing. A P2P user likely will never encounter security problems if they never change the default download directory. The problem is that there are over 4.5 million users of P2P software at any one time, most of whom do not know very much about their computers. Most P2P networks have sharing turned on by default. Many of these users probably do not realize that content is automatically shared from their downloading directory as soon as they install the program. A typical scenario might be a child on his parents' computer who wants to download all his music to their family's "My Documents" folder. The "My Documents" folder likely contains sensitive, personal family information. Everything from their tax returns to their love letters will be available to the world if they do not have sharing turned off. You can see the clear extension of this security risk to companies, schools, and government organizations who have employees who want to download content from P2P networks at work.

MediaDefender was invited to participate in this hearing on the 5th of this month, after which we collected.data from the 6th to the 9th. All of the data was collected from the Fast Track based Kazaa network, which is the largest P2P network with over 4 million simultaneous users at any point in time..

We started by seeking to locate files that were sensitive in nature and may expose a large security hole in individual computers. An obvious pick was any file generated from a Microsoft program. We chose Microsoft Money because it is a private file, one that almost no person would wish to share on P2P. These files are easily identifiable because they have a unique .mny extension. Additionally, people sharing those files are likely sharing their entire "My Documents" folder because that is where it saves by default.

We found 8034 unique files on 6052 unique IP addresses. Microsoft Money is personal tax and financial management software. All sorts of dangerous information can be pulled out of these files and used for any number of illicit purposes, including identity theft. Downloading these files is basically anonymous. P2P users are certainly not tracking who is connecting to their computer and downloading content. The larger implication is these individuals are sharing their entire "My Documents" folder, which likely contains every one of their personal documents. The rest of the files being shared on that person's computer can be accessed by simply right clicking on the Microsoft

Money file and hitting "Find More From Same User". Any document that person has on their computer can be downloaded in a matter of minutes.

Keep in mind that these results cover only individuals found to be sharing a Microsoft Money file. Many more people are sharing their "My Documents" folder who do not use Microsoft Money. It is tough to speculate as to the exact number, but I would wager that only a small percentage of P2P users run Microsoft Money. Therefore, many more than the 6052 individuals sharing Microsoft Money files on P2P are sharing their entire "My Documents" folders.

We next did a search for "Inbox.dbx" which is the file generated by Microsoft Outlook to store all incoming e-mail. Again, we considered this to be a good test file because most people would not want their private e-mail to be accessible. We only found 220 copies of Inbox.dbx. However, the Inbox.dbx file gets stored deep in the Windows directory structure by default, in a place that most people will never access. The implication is that these people had their entire hard drive shared on the P2P network. Finding only 220 copies of Inbox.dbx means that it is very uncommon for people to share their entire hard drive on P2P networks. However, 220 copies also mean that there will always be a certain segment of users who do accidentally share their entire hard drive. Clearly, the major individual security risk lies with people accidentally sharing their personal documents in the same folder they are sharing their music and movie files.

MediaDefender has very sophisticated tools for finding P2P related security problems in government organizations and businesses. However, individual security problems are so prevalent that anyone can find them. I searched for Microsoft Money files using the "mny" extension as the search term in a normal version of Kazaa. I got a large selection of returns. I picked one that looked interesting because it was titled "blank's money.mny" **[fig 1]**. I figured that had to be personal. I right clicked on the file, hit "Find More From Same User", and up came every file he had in his "My Documents" folder **[fig 2]**.

Just from the first screen I could tell his name. (I am concealing that information for his privacy). He is a sophomore at Auburn University. Naturally, his Microsoft Money file had all of his personal financial information in it, including bank and credit card information. I went on to download all the files he had. I found pictures of him and his friends. I found his friends' phone numbers and addresses. I found tons of personal information on him, including his Social Security number. I found his dietary meal plan. I found letters he had written to his family and girlfriend. I found tons of papers he had written for school. I found out he is a Christian. I found out what type of pornography and music he likes. I found out his copy of Microsoft Money is pirated. This was all a five minute exercise. You can easily see how a malicious individual could do this all day and never run out of victims.

We approached our study of P2P security problems in government institutions differently. There is no common proprietary file that would be commonly shared by different government organizations on a P2P network that a hacker could look for.

Instead, a hacker would look for any government computer sharing **anything** and poke around on that computer hoping to stumble over something interesting. This is how we structured our study.

We looked over the entire Fast Track (Kazaa) network for any individual sharing files using the search words Madonna, The Matrix, Porn, and Sex. We arbitrarily chose these key words because the files they produced would likely have no legitimate work-related purpose, but would give us a large sampling of IPs from which to find government organizations. We do not have a list of every government IP range, so we had to eyeball most of the results.

There were well over 2000 government computers sharing content on P2P networks. For the purposes of this brief study, we focused on Los Alamos National Laboratory, NASA, and Naval Warfare Systems Command. We chose those organizations because of the sensitive nature of the work they perform. We found 155 computers at Los Alamos National Laboratory sharing content on P2P. We found 138 computers at NASA sharing content on P2P. We found 236 computers at Naval Warfare Systems Command sharing content on P2P.

Given our time and resource constraints, MediaDefender did not sift through all the data to see if there are actually any important secret documents shared. The point is simply that these people at these government institutions are unknowingly opening their computers up to the world. It is unlikely that they intended to share pornography and music from their government work computers, so it stands to reason they might accidentally share other sorts of files as well. A more comprehensive study should probably be run over a longer period of time to get a completely accurate view of the extent P2P has created a security problem on our government networks. Our findings simply show that a problem exists.

Plugging up the security holes created by P2P networks is not a trivial issue. There is no universal program or system to deploy that will solve the problem. The solutions for individual security and corporate network security are very different. Individuals who use P2P should be very careful about what directories they have shared up. I would suggest that most individuals concerned with security actually turn off the sharing capabilities on their P2P program. Every download should be scanned with anti-virus software before double clicking on it. Individuals should always look at the file extension of what they download. If someone is trying to download an MP3, they should make sure the extension of the file is .mp3 as opposed to something that could be malicious like .exe or .vbs.

Individuals should never download documents or programs from P2P. All sorts of nasty things from viruses to trojans can be hidden in documents and executables. Someone could erase your entire hard drive or create a backdoor for spying or stealing resources. When these attacks happen, they are not always immediately obvious because time-delay mechanisms are often built in to disguise the malicious file. Often these malicious files are hidden in real working files. You may download a copy of Adobe

Acrobat, run it, use it, and think that nothing is wrong. Unbeknownst to you, a hacker embedded a trojan horse on your computer with the intention of hacking your system later. The point is that files downloaded from P2P may be maliciously planting things on your computer even if they appear to work when you double click them. The same security problems that plague individuals on P2P can jeopardize the integrity of an entire network.

The first and most obvious solution to corporate P2P security is to proxy the whole network so that employees cannot use any Internet software except their web browser and e-mail. Many companies do this for other security reasons. The problem with this approach is that you give up all the wonderful productivity and research tools the Internet has to offer such as Instant Messaging. This solution is fine for some companies, but would never work for a school or Internet company that is reliant on open, unhindered Internet connections for their development. You cannot block uploading without blocking downloading on a P2P network. So, you either have to block the whole program or run the risk that sensitive data may be accidentally shared up.

There are tools on the market for blocking specific programs from working on a network. The problem with this approach is that there is a plethora of P2P software programs, and you will never block them all. Many institutions target the big P2P networks only. However, an academic institution may not want to block P2P software from their students for a variety of reasons. In that case, they should make sure the dorm networks are buffered from the other university networks that may contain sensitive information. The most comprehensive security measure is to have a consulting company like MediaDefender look at the P2P network on a macro-scale from the outside and see what we can find being shared from within your corporate network. Viewing your network from the outside could also be important because your employees may be sharing illegal content such as pirated music or child pornography.

There is no magic technology bullet for solving the problems associated with P2P networking. Problems will always proliferate when there are free, unregulated channels of information traveling between millions of computers. Developers of P2P software have a duty to safeguard less informed individuals from opening their computers to invasions of privacy, viruses, and hackers. Simple measures can and should be added to all P2P software to prevent unintentional directory sharing and downloading of dangerous files. Information technology specialists at government institutions, schools, and businesses have a duty to safeguard their networks against security holes associated with P2P networks. Overall, every organization that does not completely block P2P should have a policy toward P2P that includes security, preventing piracy, and preventing child pornography. Unfortunately, few IT organizations are doing a good job controlling the problems associated with P2P networking, and this will eventually cause irreparable damage.

Testimony of Rep. Henry A. Waxman
Hearing before the United States Senate Committee on the Judiciary
The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of P2P File-Sharing Networks?

Mr. Chairman, Senator Leahy, I thank for you for the opportunity to testify today on the important issue of peer-to-peer networks and file-sharing programs. Chairman Davis and I have worked together closely to bring attention to this technology and the questions it raises.

Peer-to-peer technology is in many ways a "bright idea," as you indicate in the title of the hearing. It is a unique and innovative use of Internet technology. But we have found that it also carries significant risks that most people don't know about.

These programs are incredibly popular, especially with youth. They have been downloaded literally hundreds of millions of times. For teenagers and people in their twenties, peer-to-peer file-sharing programs are as common a computer application as e-mail and word-processing programs are for the rest of us.

My concern is that there is a digital generation gap when it comes to understanding these programs. Parents simply don't have the knowledge about these programs that their children do. As a result, many parents are unaware of the special risks posed by these programs.

How many parents realize that these programs, if carelessly installed, can make every single bit of electronic information on a family computer available to millions of strangers? Very few.

The Committee's first investigation into peer-to-peer technology looked at one of the risks posed by file-sharing programs: the prevalence of pornography.

We learned that these peer-to-peer networks operate like a vast library of free pornographic content. Any child that has access to a broadband connection can easily find and download the most hardcore, triple-x videos imaginable in just a matter of minutes at absolutely no cost.

A GAO report released at our hearing found that kids are bombarded with pornography even if they aren't looking for it. GAO searched for popular entertainment figures like Britney Spears and the Olson Twins and for cartoon characters like Pokemon. They found that more than half of the files they retrieved were pornographic, including files that contained illegal child pornography.

We have also done some investigation into the topic of today's hearing: privacy and security risks from file-sharing programs.

Peer-to-peer programs connect users from anywhere in the world into a vast open free trade network. With the click of a mouse, users can share files back and forth with other users across the globe. It is impressive technology with enormous potential.

But our investigation found that many people are inadvertently sharing incredibly personal files with millions of strangers through these peer-to-peer networks.

Our staffs installed Kazaa, the most popular file-sharing program, and ran test searches to see what kind of information people were sharing unintentionally. What we found was amazing. We found completed

tax returns, medical records, and even entire e-mail inboxes through simple searches using file-sharing programs.

We also found other incredibly private documents, such as attorney-client correspondence relating to divorce proceedings and living wills.

We prepared a report on our findings, which I would like to make part of this hearing record.

No one would want to share this kind of personal information, but in many cases that is exactly what's happening. Due to the way some users configure their computers, their personal files can be accessed by millions of strangers through peer-to-peer networks.

And you don't have to be a hacker who illegally breaks into a computer to get access to these files. These private files are in effect being put on public display, allowing millions of other users to access them perfectly legally.

These security risks take on a new level of concern for government computers. Clearly, we need to assure that national security is not compromised by improper use of file-sharing programs. For that reason, we are working with GAO to assess our government's vulnerability.

I welcome the interest of your Committee in exploring this new technology. There is much this hearing and future ones can add to our understanding of file-sharing programs. And I look forward to working with you.

Thank you.