AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OVEREXPOSED: THE THREATS TO PRIVACY AND SECURITY ON FILESHARING NETWORKS

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MAY 15, 2003

Serial No. 108–26

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

88–016 PDF 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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on May 15, 2003	1
Statement of:	
Broes, Derek S., executive vice president of Worldwide Operations, Brilliant Digital Entertainment	59
Davidson, Alan B., associate director, Center for Democracy and Technology	39
Farnan, James E., Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, accompanied by Dan Larkin, Supervisory Special Agent, Federal Bureau of Investigation	89
Frank, Mari J., esquire, Mari J. Frank, Esquire & Associates	66
Good, Nathaniel S., University of California, Berkeley, School of Information Management Systems	13
Hale, Dr. John, assistant professor of computer science and director, Center for Information Security, the University of Tulsa	31
Schiller, Jeffrey I., network manager/security architect, Massachusetts Institute of Technology	25
Letters, statements, etc., submitted for the record by:	
Broes, Derek S., executive vice president of Worldwide Operations, Brilliant Digital Entertainment, prepared statement of	62
Davidson, Alan B., associate director, Center for Democracy and Technology, prepared statement of	41
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	3
Farnan, James E., Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, prepared statement of	91
Frank, Mari J., esquire, Mari J. Frank, Esquire & Associates, prepared statement of	69
Good, Nathaniel S., University of California, Berkeley, School of Information Management Systems, prepared statement of	16
Hale, Dr. John, assistant professor of computer science and director, Center for Information Security, the University of Tulsa, prepared statement of	34
Schiller, Jeffrey I., network manager/security architect, Massachusetts Institute of Technology, prepared statement of	27
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	7

OVEREXPOSED: THE THREATS TO PRIVACY AND SECURITY ON FILESHARING NETWORKS

THURSDAY, MAY 15, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:09 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis of Virginia (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Shays, Putnam, Duncan, Murphy, Waxman, Maloney, Cummings, Tierney, Clay, Sanchez, and Ruppersberger.

Staff present: Peter Sirh, staff director; Melissa Wojciak, deputy staff director; Keith Ausbrook, chief counsel; Anne Marie Turner and Randall Kaplan, counsels; David Marin, director of communications; Scott Kopple, deputy director of communications; Ken Feng, investigator/GAO detailee; Teresa Austin, chief clerk; Joshua E. Gillespie, deputy clerk; Corinne Zaccagnini, chief information officer; Brien Beattie, staff assistant; Phil Barnett, minority chief counsel; Karen Lightfoot, minority communications director/senior policy advisor; Josh Sharfstein and Nancy Scola, minority professional staff members; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Chairman TOM DAVIS. Good morning. A quorum being present, the Committee on Government Reform will come to order.

Let me say a special thank you to our visiting students from Woodson High School, out in the 11th Congressional District of Virginia. We are happy to have you with us, and I hope you will find some of this hearing interesting.

We are here today to continue our examination into peer-to-peer file-sharing programs. This is the committee's second hearing on this topic.

At our first hearing held in March, we examined the growing problem of the availability of pornography, including child pornography, on these networks. The committee found that pornography is, in fact, being traded on peer-to-peer networks, and children are at great risk of inadvertent exposure to pornography while using these programs.

File-sharing programs or Internet applications allow users to download and directly share electronic files from other users on the same network. Users of these programs can share files that contain documents, as well as music or videos. These programs are surging in popularity.

KaZaA, the most popular file-sharing program has been downloaded almost 225 million times, making it the most popular software downloaded on the Internet.

File-sharing technology can be beneficial. However, as we learned from our first hearing on this topic, use of this technology also presents certain risks. Today, the committee will examine the risks to personal privacy and computer security posed by the use of peer-to-peer file-sharing programs.

Specifically, we are going to look at three issues: first, the reason why highly personal information is available over these networks; second, the potential effects of software known as "spyware" or "adware" that is being bundled or included with file-sharing programs; and third, the growing risk of downloading computer viruses from files shared on these programs.

The committee will release a staff report today that highlights these issues. Through a simple search on one file-sharing program, committee staff easily obtained tax returns, medical records, attorney-client communications, resumes, and personal correspondence.

Users of these programs may accidentally share this information because of incorrect program configuration. They also could be intentionally sharing these files because increased file-sharing earns the user higher priority status on popular downloads.

Either way, users of these programs need to be aware that sharing personal information 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 their home or office computers contain file-sharing programs.

Another concern raised by the use of peer-to-peer file-sharing is the bundling of these programs with software known as "spyware" or "adware." These programs monitor Internet usage primarily for marketing purposes, without the users' 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. In fact, just this week, a new computer virus called "Fizzer" spread rapidly across the Internet, affecting computers worldwide through e-mails and the file-sharing program, KaZaA.

We have assembled an excellent panel of witnesses who will discuss these important issues. I would like to thank each of our witnesses for appearing today. I would now like to yield to Mr. Waxman for his opening statement.

[The prepared statement of Chairman Tom Davis follows:]

Statement of Chairman Tom Davis
Government Reform Committee Hearing
"Overexposed: The Threats to Privacy and Security on File Sharing Networks"
May 15, 2003

Good morning, a quorum being present, the Committee on Government Reform will come to order. We are here today to continue our examination into peer-to-peer file-sharing programs. This is the Committee's second hearing on this topic. At our first hearing held in March, we examined the growing problem of the availability of pornography, including child pornography, on these networks. The Committee found that pornography is, in fact, being traded on peer-to-peer networks, and children are at great risk of inadvertent exposure to pornography while using 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. Users of these programs can share files that contain documents as well as music or videos. These programs are surging in popularity.

Kazaa, the most popular file-sharing program, has been downloaded almost 225 million times, making it the most popular software downloaded on the Internet.

File sharing technology can be beneficial. However, as we learned from our first hearing on this topic, use of this technology also presents certain risks. Today, the Committee will examine the risks to personal privacy and computer security posed by the use of peer-to-peer file-sharing programs.

Specifically, we will look at three issues: first, the reason why highly personal information is available over these networks; second, the potential effects of software known as "spyware" or "adware" that is being bundled or included with file sharing

programs; and third, the growing risk of downloading computer viruses from files shared on these programs.

The Committee will release a staff report today that highlights these issues. Through a simple search on one file-sharing program, Committee staff easily obtained tax returns, medical records, attorney-client communications, resumes, and personal correspondence.

Users of these programs may accidentally share this information because of incorrect program configuration. They also could be intentionally sharing these files because increased file sharing earns the user higher priority status on popular downloads.

Either way, users of these programs need to be aware that sharing personal information 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 their home or office computers contain file-sharing programs.

Another 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, without the users 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. In fact, just this week, a new computer virus called "Fizzer" spread rapidly across the Internet, infecting computers worldwide through emails and the file sharing program Kazaa.

We have assembled an excellent panel of witness who will discuss these important issues. I would like to thank each of our witnesses for appearing today.

###

Mr. WAXMAN. Thank you very much, Mr. Chairman. I am pleased to join with you in this hearing. I want to commend our staff for developing this report that we issued today, "File-Sharing Programs and Peer-to-Peer Networks, Privacy and Security Risks."

This is the second of a series of hearings that this committee has been holding to highlight and educate the public about not just the great opportunities with these new file-sharing efforts on the computers, but the risks involved, as well.

At our last hearing, we talked about the fact that if young people, who are, for the most part, the ones who are using these peer-to-peer file-sharing programs, try to get music from the programs, more often than not, they are having very vile pornography pushed upon them.

Most parents were not aware of that fact; and most people, I think, are not aware of the facts that we are going to examine at our hearing today.

We live in a world that is increasingly more connected. New computer innovations can open us up to new experiences and offer more choices than ever before. As we experiment with new technologies, however, we must recognize their risks. In the real world, we know how to guard our privacy and security carefully. It is just as important to do so in the on-line world.

So in this hearing, we are going to look at these very incredibly popular programs. In fact, the most popular of these file-sharing programs, KaZaA, has been downloaded more than 220 million times. That is really incredible, 22 million times in the last 2 months alone.

Despite their soaring popularity, few people understand the risks that these new file-sharing programs can pose. In large part, this is due to what I call the on-line generation gap. The users of file-sharing programs are predominantly teenagers. The parents, however, and grandparents are too often left struggling just to keep up.

In our report that we are releasing today, I think we have an opportunity to inform the parents and grandparents that when their kids use these file-sharing programs, they may find that inadvertently they are sharing incredibly personal files through these peer-to-peer networks.

Our investigators found that they could find completed tax returns, medical records, and even entire e-mail in-boxes through simple searches using file-sharing programs. No one would want to share this kind of personal information, but in many cases, that is exactly what is 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. This invasion of privacy is not the only risk families face. Our report finds that when users download free file-sharing programs, they are also exposing their computers to hidden software called "spyware" or "adware."

These programs track what you do online, the Web sites you look at, how long you stay on those Web sites, even your e-mail address. This zombie-like ware, which takes over the spare computing power of personal computers can be bundled with file-sharing programs.

So not only can they get access to what is in your personal files, they can make your computer server a zombie for their own purposes. Besides tracking your computer habits, these programs can also cause software conflicts and computer crashes. In fact, in committee testing, these programs ruined a committee computer twice. Even the House's most experienced computer technicians could not restore the computers.

The chairman mentioned that we are putting computers at risk for viruses and other damaging computer files, and we will have more testimony about that in our hearing.

While technical innovation on the Internet is tremendously important, our purpose in holding these hearings and releasing these investigative reports is not to say that peer-to-peer technology is inherently bad. In fact, it may ultimately prove to have important and valuable uses.

But there can be no question that this new technology, at least in its current incarnation, can create serious risks for users. Our purpose in holding these hearings is to help the public understand what these risks are. Without this knowledge, families and businesses simply will not be able to make intelligent decisions about the technology.

[The prepared statement of Hon. Henry A. Waxman follows:]

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
The Threats to Privacy and Security from File Sharing Networks

May 15, 2003

I join with Chairman Davis today to bring attention to an Internet technology that is in many of our homes and may be risking our personal privacy and security without us even knowing it.

We live in a world that is increasingly more connected. New computer innovations can open us up to a new experiences and offer more choices than ever before. As we experiment with new technologies, however, we must also recognize their risks. In the real world, we know to guard our privacy and security carefully. It's just as important to do so in the online world.

Today's hearing is the second in a series of hearings in the Committee about peer-to-peer file-sharing programs. These programs are incredibly popular. In fact, the most popular of these file-sharing programs, Kazaa, has been downloaded more than 220 million times – 22 million times in the last two months alone.

But despite their soaring popularity, few people understand the risks that these new file-sharing programs can pose. In large part, this is due to what I call the online generation gap. The users of file-sharing programs are predominantly teenagers. We parents and grandparents are too often left struggling to keep up.

Two months ago, at our Committee's first hearing, we focused on one key issue raised by file-sharing programs: how they can inundate our children with pornography. We learned that even when kids are searching for music by Britney Spears or videos of the Olson Twins, what they encounter is often the most hard-core, triple-x pornography imaginable.

Today, we will focus on another key issue: the ways that these programs can jeopardize personal privacy and security.

Chairman Davis and I are releasing a new report by our investigative staff that examines these issues. Its findings should concern every family that's using one of these new file-sharing programs.

Our Committee investigation found that many people are inadvertently sharing incredibly personal files through these peer-to-peer networks. Our investigators found that they could find completed tax returns, medical records, and even entire e-mail inboxes through simple searches using file-sharing programs.

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 this invasion of privacy is not the only risk families face. Our report finds that when users download free file-sharing programs, they are also exposing their computers to hidden software called "spyware" or

"adware." These programs track what you do online – the websites you look at, how long you stay on them, even your e-mail address. Even "zombie-ware," which takes over the spare computing power of personal computers, can be bundled with file-sharing programs.

Besides tracking your personal computer habits, these programs can also cause software conflicts and computer crashes. In fact, in Committee testing, these programs ruined a Committee computer twice. Even the House's most experienced computer technicians could not restore the computer.

And there are still other risks. Our staff also contacted some of the leading experts from universities and the private sector to find out whether file-sharing programs can put computers at risk for viruses and other damaging computer files. You will hear what they have to say about this serious threat later today.

Technical innovation on the Internet is tremendously important. Our purpose in holding these hearings and releasing these investigative reports is not to say that peer-to-peer technology is inherently bad. In fact, it may ultimately prove to have important and valuable uses.

But there can be no question that this new technology – at least in its current incarnation – can create serious risks for users. Our purpose in holding these hearings is to help the public understand what these risks are. Without this knowledge, families and businesses simply won't be able to make intelligent decisions about the technology.

Chairman TOM DAVIS. Thank you very much, and let me also commend the staff, and Mr. Waxman, your leadership in helping put these hearings together.

Are there any other opening statements; the gentleman from Maryland?

Mr. RUPPERSBERGER. The information superhighway has opened many doors and opportunities, both in terms of communication and in terms of commerce. It gave us a .com boom in the mid-and late 1990's and helped us to make a more technologically advanced country.

Now privacy on the Internet has been discussed in Congress since 1998. We have discussed what information needs to be protected. Is a disclosure policy a privacy policy? How do we protect it and how do we enforce it? Does Congress need to set standards, or do we let the industry decide what is best?

As technology advances, we have to ask ourselves, if Government does promulgate regulations, will those regulations be able to keep up with the pace of technology?

Now today we are discussing file-sharing networks like KaZaA and Morpheus. These networks allow subscribers to download and share music, photo and video clips with other subscribers. The question is, how safe are these networks?

Can a hacker or an individual use networks to get around any firewalls and protections and invade persons' more personal files? Can they look at people's Quicken statements? Can they view saved e-mails and documents?

Privacy is not just about personal information. The most important part is, we have to be able to be concerned about how those companies track and use what you download to market your items.

Do these networks sell your information to retailers? Do they share them with spammers, companies that flood our e-mail with product information?

At this time, I think we need legislation, but I am fearful whatever we write up in Congress will be obsolete within 1 year.

Can we legislate privacy? Yes, we can. Congress has done that. We have cable and video store privacy. We have financial privacy and we have medical privacy. Why not person-to-person network privacy? How about a strong Federal enforcement mechanism, based on violations of industry-based best practice standards?

Now obviously, no one wants to harm the continued advancement of technology. But eventually there will be the need for a balance. There will be the need to assure people that your information is safe as you connect to the Internet as it travels through cyberspace.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

Does anyone else wish to make an opening statement?

[No response.]

Chairman TOM DAVIS. We will now move to our witnesses. We have Nathaniel Good from the University of California, Berkeley, who will be demonstrating for the committee how personal documents can easily be accessed from peer-to-peer file-sharing networks.

Next, we have Jeffrey Schiller, who is network manager for the Massachusetts Institute of Technology. Following Mr. Schiller is Dr. John Hale, the director of the Center for Information Security at the University of Tulsa.

We will then hear from Alan Davidson from the Center for Democracy and Technology; and then from Derek Broes, the executive vice president of Brilliant Digital Entertainment.

Next is Mari Frank, who is an identity theft expert. Rounding out the panel is James Farnan, Deputy Assistant Director of the Federal Bureau of Investigations Cyber Division.

It is the policy of this committee that all witnesses be sworn before they testify, so if you will rise with me and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much; please be seated. We have a light in front. We have your total statements in the record that we have read. Your green light will be on for the first 4 minutes. In the 5th minute, an orange light will go with the red light, so at 5 minutes, we would appreciate your summing up.

Your total testimony is in the committee record, and we will go from there. I think for our first witness, you are going to do a demonstration. We will cut a little slack on the time, but if we can get it down, then we can get to questions; thank you very much, Mr. Good.

STATEMENT OF NATHANIEL S. GOOD, UNIVERSITY OF CALIFORNIA, BERKELEY, SCHOOL OF INFORMATION MANAGEMENT SYSTEMS

Mr. GOOD. Thank you very much; good morning, Mr. Chairman and committee members. Thank you for the opportunity to appear before you today.

In the brief amount of time that we have to talk to you about our study, we would like to give you a video demonstration of the problem that we found with KaZaA; describe how this problem can occur; and then talk about the possible solutions to this problem.

On the screen in front of you is KaZaA. KaZaA is the most popular peer-to-peer file-sharing program on the Internet today. With KaZaA, you can look for any type of file, such as music, documents, videos. Any file that can be stored on your hard drive can be shared through the KaZaA network.

To do this, one would download the application, type the key words that one is looking for into the search box, hit the return, and the results would pop up to the right to your search box.

In this example, we will show how a user could get ahold of someone else's personal information through KaZaA by typing key words and looking for information from the search results.

So in the first example that we have, we have a user who is looking for a file called "inbox.dbx." Inbox.dbx is someone's e-mail file. As you can see, there have been a couple different results that we have returned.

If we wanted to see what other files these people were sharing, we could go to that person's file. We could find more from that user, and we would see all the files that this person is sharing.

So we can see there are other e-mail files that this person has. There is the "sent" files that this person has. There are a whole bunch of deleted items that we could download and restore and look at, and there is also the in-box and other personal pieces of information.

So for the next search, we will be doing a slightly more sophisticated search, where we will be looking for an Excel spreadsheet that has possibly credit card information.

In this demonstration, we will show how, if you know a little about what Excel is, that you know an Excel document has the extension "XLS," and you think that someone would call their Excel document credit card, or something that begins with credit. You could type in these key words here, run a search, and this is what you would probably see, something very similar to this.

So here we have a list similar to the list that we had earlier, where we had a bunch of files that were returned from various users. If we wanted to see some more files from an end user, we could click on a file there, type in find more from same user. Again, we would see all the fields that that person has shared.

In this case, it looks like the person has pretty much shared most of their hard drive. There is again, the in-box file. This is the e-mail file we were talking about before. There are a whole bunch of system files. There are cookie files. If we scan over, we can see a little bit more detailed file information.

We can sort by media type, so we can browse around and look for other types of information. So we can see that this person has certain spread sheets that pertain to salary structures. They have a PDF on tax returns. They have letters that they have written to people. They have an address book.

If we keep browsing through, we will find that they have bonus agreements that they have sharing. There is a lot of stuff here that this person probably does not want the rest of the world to download.

We also have the credit card activity, the spreadsheet that we talked about earlier. There is quite a bit, as you can see; office documents and there is the credit card file, again. There is another one.

Here, we also have a password list which, unfortunately, probably contains all the passwords that this person has to get into various Web sites or corporate sites. People typically keep their passwords in a document, because they have to remember so many of them.

So if we downloaded this, we probably would be able to hop around to various Web sites and jump into this person's accounts and such.

So this is pretty much the problem that we discovered on KaZaA. We determined that through a series of user studies and analyzing the interface, that this problem could occur because parts of the KaZaA application could be very confusing to users, and it relied very heavily on some 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 if you were able to go over the research report that we have and our written testimony, you should be able to get more details about how this problem could possibly occur.

As for solutions, we see two possible paths that we could take. The first is education. It is important for people to understand that what peer-to-peer can share, and more generally, what it means to be connected to a network in terms of privacy and security.

We would also like to see stronger default settings and better explanations of what is going on in the program. It is important that applications should be safest right out of the box.

Security and convenience are typically seen as tradeoffs of one another. As the world becomes more networked and more devices are able to store, collect, and share private information, it is crucial that we find ways for applications to be secure without sacrificing convenience and vice versa.

Thank you very much for your time.

[The prepared statement of Mr. Good follows:]

Testimony by Nathaniel Good and Aaron Krekelberg
University of California, Berkeley
School of Information Management Systems
And
University of Minnesota
Office of Information Technology
Before the
House Committee on Government Reform

Good morning Mr. Chairman and Committee members. 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 Chief Web Architect at the University of Minnesota's Office of Information Technology. It is an honor to be here today to present to the committee and 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 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.

Summary of Study Results

In this study, we determined through both user studies and analysis that the KaZaA applications interface had several critical flaws that may contribute to participants' misconfiguring the application and thus inadvertently sharing their private and personal information. 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 our 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

It is our opinion that 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 that "causes" users to share files without their knowledge. We feel that 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. 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 initial 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 applications 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, 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 only 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, our understanding is that it 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 examine 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.

We would also like to state that 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 users interface problems we discovered.

The problems we describe are very much part of a larger, more general problem that applies to all networked systems that store and share users' personal and private information. The problems we described in the report could also exist in email applications (as reported in a related paper on usability and security by Whitten and Tygar), 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. 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.

Handouts on KaZaA File Sharing

Nathaniel Good
School of Information Management Systems
University of California, Berkeley

Aaron Krekelberg
Office of Information Management Technologies
University of Minnesota

Types of Files Found on Kazaa

Docume...	CSC Information.xls
Docume...	Credit Card Activity.xls
Docume...	Formulas.doc
Docume...	Classificationedit.xls
Docume...	CF_Ultra_brochure.pdf
Docume...	CF16mb.pdf
Docume...	Business Solutioins.doc
Docume...	Budget1.xls
Docume...	Budget_Christmas.xls
Docume...	Book4.xls
Docume...	Bonus Agreement.doc
Docume...	Bens'.xls
Docume...	Automating Office.doc
Docume...	Auto Makes.xls
Docume...	April[1].pdf
Docume...	humanresources[1].pdf
Docume...	compbenefits[1].pdf
Docume...	ADT Safewatch Owners's Manual.
Docume...	Address book.xls
Docume...	addr'.xls
Docume...	aa_apfa_letter_of_agreement[1].
Docume...	2176[1].pdf
Docume...	2001 Tax Return.pdf
Docume...	2001 Salary Structures.xls
Docume...	802%20Termination%20All[1].pdf
Docume...	801%20Reduction%20in%20For
Docume...	802_termchecklist[1].pdf
Docume...	take the 1996 tan chevy tahoe it
Docume...	take the 1999 black bmw 323 last

These are actual file listings acquired from a KaZaA user. They include, spreadsheets, documents containing password information, business documents, and other private information

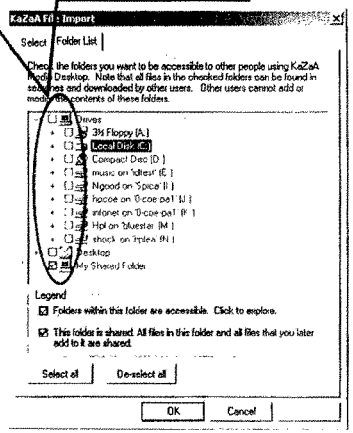
Docume...	WAREHOUSE.doc
Docume...	WAREHOUSE2.doc
Docume...	VPN Installation Instructions for 3.
Docume...	VoiceMail[2].pdf
Docume...	VoiceMail[1].pdf
Docume...	veo_claimform[1].pdf
Docume...	Password List.doc
Docume...	OLJOURN.DOC
Docume...	Time Envelope---2.xls
Docume...	Time Envelope---1.xls
Docume	SYMAD Fax.doc
Docume	Sunglasses.doc
Docume	Signature1.rtf
Docume	shiftschedule.xls
Docume	Vehicle List 1.xls
Docume	Vehicle list2.xls
Docume	SampleSalespersonReports.xls
Docume	SampleProductReports.xls
Docume	SampleOrderReports.xls
Docume	SampleCustomerReports.xls

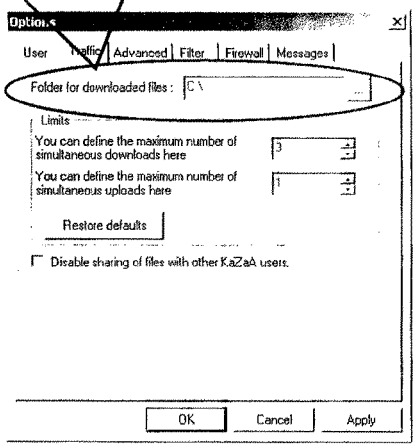
1024	Docume...	Employee List.xls
1024	Docume...	etman.pdf
1024	Docume...	eEHumanResources.doc
1024	Docume...	Dyann Adair.res.doc
1024	Docume...	Dukie Birthday.ppt
1024	Docume...	Dukie.ppt
1024	Docume...	Draft.xls
1024	Docume...	Distributed Spreadsheet Data Sh..
1024	Docume...	Dealership List.xls
738	Docume...	daa 4-30.doc
738	Docume...	DAA LIST.doc
738	Docume...	DEALERS AA LIST.doc
1024	Docume...	David.rtf
1024	Docume...	DAILY PRODUCTION PLANNING...
738	Docume...	DAA RUN LIST.doc
1024	Docume...	CSC Information.xls
1024	Docume...	Credit Card Activity.xls
1024	Docume...	Formulas.doc
1024	Docume...	Classificationedit.xls
1024	Docume...	CF_Ultra_brochure.pdf
1024	Docume...	CF16mb.pdf
1024	Docume...	Business Solutions.doc
1024	Docume	Budget1.xls
1024	Docume	Budget_Christmas.xls
1024	Docume	Book4.xls
1024	Docume	Bonus Agreement.doc

Confusing Terminology: One example of how KaZaA could confuse users

What you think you are sharing is nothing, or only files in the "My Shared Folder". There are no checkmarks to indicate otherwise.

What you are actually sharing are all the files in the "folder for downloaded files." The folder in which one chooses to save files to and all files and folders in it are shared. In this case, it is all the files on C:, which are all the files on the hardrive.





Chairman TOM DAVIS. Thank you very much.

Mr. Schiller.

STATEMENT OF JEFFREY I. SCHILLER, NETWORK MANAGER/SECURITY ARCHITECT, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Mr. SCHILLER. Good morning and thank you for inviting me.

Chairman TOM DAVIS. Thank you.

Mr. SCHILLER. I am actually not going to read my statement, but I will tell you essentially what is in there. I have been involved in the Internet since the day it was born which was, we say, January 1, 1983, and there is a story behind that.

It is funny, I remember, e-mail was the application that everybody said was the forbidden application, because it was a waste of network bandwidth. So here we are today with e-mail being one of the killer applications, and we are looking at another application that causes us a bit of concern.

From my view as a security expert, I can tell you that my professional assessment is that these programs, peer-to-peer file-sharing, particularly once they are perfected, are not significantly more dangerous, from an end users perspective, than any other technology they use.

Just as we have seen here today, KaZaA can be used to reveal private information. I have certainly received in my e-mail inbox private information that was sent via e-mail, due to various viruses and worms that people have caught. Because of who I am, I net a lot of that sort of stuff, and it is pretty amazing what you can get.

So I try to say, what is the difference between a file-sharing program that we have today and some of the traditional technology that we have on the Internet, such as e-mail and Web browsing?

One of the key differences is that file-sharing is still under active development. The e-mail technology we use today was standardized many years ago, and it does not change.

As a manager of a network, if I wish to control e-mail, if I wish to set up a firewall that examines incoming e-mail messages to make sure they do not contain viruses or worms, I can do that, but I can be pretty assured that my e-mail scanning will, in fact, happen as it is supposed to.

However, file-sharing programs are programs that are currently under active development. As some of us who run networks try to put in ways of controlling them, the authors of these programs in their newest versions put in ways to get around those controls.

So one of the ways that peer-to-peer file-sharing significantly differs from the more traditional applications is the intent to subvert third party controls. That is inherent in them. That is not inherent in other technologies.

So as a network manager, one of my concerns with peer-to-peer file-sharing is its use of our precious bandwidth, which we pay dearly for; and there are various tactics that we can do to try to limit the use of that bandwidth. What happens next, of course, is the next version of these programs, those various techniques to avoid that rate limiting.

Without going into a lot of technical detail, one of the things we have been seeing is what I call "port hopping." Most Internet applications use a well known port. E-mail travels over port 25, for example; file transfer over port 21, Web browsing over port 80.

Well, in their early days, most file-sharing programs had well known ports. I use port 1214, for example, and by controlling access to that port, we could control its use.

What we are seeing more and more of are programs that hop around. They might use port 1214 for a few minutes, and then a few minutes later, we see a lot of traffic on some other literally randomly chosen port. With applications that do this, it becomes very difficult to actually know what is going on and control it.

We have also seen applications that appear to be encrypting their content; not to hide it from any eavesdropper, but to make it difficult again for us to figure out, oh, this is file-sharing programs. There are many such programs that do this. KaZaA is not the only one.

So my point today is that one of the things that makes these things just a bit more dangerous than other things is the attempt to subvert third parties.

Particularly in an environment where you have end users who are not necessarily experts, who leave themselves exposed, we have many places where we try to use firewalls at the corporate level to protect people, and that is being subverted.

Now like everything, many things are a two-edged sword. Sometimes, the third parties trying to control access to the network are not necessarily what we could consider good guys.

The same technology that a corporation can use to control access can be used by governments that wish to suppress their people, and peer-to-peer file-sharing programs can often be used as a way of spreading the work, without it being controlled. But like all things, it is a two-way street, thank you.

[The prepared statement of Mr. Schiller follows:]

Testimony by Jeffrey I. Schiller,
Network Manager/Security Architect,
Massachusetts Institute of Technology,
before the
House Committee on Government Reform
(as prepared for delivery)

May 15, 2003

My name is Jeff Schiller and I am the Network Manager at the Massachusetts Institute of Technology. I have had this position since 1984. I have been involved in the development and operation of the Internet from its very early history. I am also a security expert, an author of the MIT Kerberos Authentication System, which is used as the basis for authentication in Windows 2000 and Windows XP, among other systems. I have also deployed a Public Key Infrastructure at MIT that has been operating since 1996. This infrastructure provides for secure web authentication and authorization at MIT.

From 1994 through 2003 I served as one of the two Area Directors for Security for the Internet Engineering Task Force, the Standards body of the Internet. In this role I was responsible for the groups working on security protocols for the Internet as well as for reviewing all Internet Standards documents for correctness. I am therefore very familiar with the protocol workings of the Internet as well.

I am here today to help you look at what are called "Peer to Peer" file sharing programs, through the lens of security.

It is funny how we refer to these programs as "Peer to Peer" when the architecture of the Internet itself is peer to peer. E-mail is peer to peer, even web browsing is peer to peer. Most people don't run a web server, however the Internet would work just fine if they did. The innovative nature of the Internet itself is dependent on this peer to peer nature. If it were not that way, E-mail may have never arisen as the important application that it is. In fact I remember the days when E-mail was considered a waste of network resources and quasi forbidden, yet today it is one of the killer applications of the Internet. If it were not for the peer to peer nature of the Internet, a programmer at CERN in Switzerland could not have modernized the CERN telephone directory, and invented the World Wide Web as a side effect!

So what are we really talking about here today. What makes the programs we are concerned about different from those that preceded them?

The key attributes of what we call peer to peer programs are:

- Storage of files on "client" computers, desktops and laptops. Typically not computers that we view as "servers" more traditionally used to store data.
- The organization of networks of computers all which use the same file sharing network. When you start up a peer to peer file sharing program, it "joins" the network of other people already running the program. This "joining" takes the form of

making a direct Internet connection to one or more other computers running the same program.

- The ability of one computer user to request a file by name or attribute and have a listing of available copies downloaded to that computer. The user can then select and download the data file itself.

So are these programs secure? Well, we have to ask: "Compared to What?"

In some ways they are more secure then E-mail. Whereas E-mail tends to be "pushed" to you, file sharing is more like web browsing, you have to go looking for information, it doesn't show up on your computer unbidden.

So what are the risks to the end-user of a file sharing program?

A malicious person might place a file in the network with the name of a popular download, but instead of providing the information advertised, the file contains a virus or other active content that when opened results in compromise or damage to the end-user's computer. One might argue that this risk is present in web browsing as well. We have heard of plenty of cases of security weaknesses in web browsers that start with the phrase "A malicious user could put content on their webpage that..."

However when web browsing, people have some sense of where they are going (at least some people do!). File sharing programs tend to hide this level of detail. Instead they will show you a menu of several places where the file you request is located, listing each by Internet address, which isn't particularly meaningful to someone.

My conclusion is simply this: File sharing programs, as viewed by the end-user are no more or less secure then other common Internet applications such as web browsing or reading E-mail. The exact technical details are slightly different. The risks are slightly different, but the magnitude of danger is about the same.

So where do these program really deviate, if not now, in the future?

To go further we need to stop for a second and talk about the various actors involved in the use of a computer. Up until now I have discussed the world from the view of an end-user, the user of a client computer either at home or in an office.

However there are four different "actors" potentially involved. The end-user is one obvious actor. The provider of the file being requested is another actor. The owner of the computer or enterprise the computer is located in, is an actor with a stake in the security properties and risks of a file sharing program. Finally, there is the author of the file sharing program and the "operator" of the peer to peer file sharing network.

Unlike E-mail and Web Browsing, the peer to peer file sharing networks are still evolving. This means that the "author" of the programs are still active "actors" continuing to modify their programs to address both new features and to adapt to the operating environment of the Internet. It is this adaption that is cause for concern.

The administrator of an enterprise network, or the parent of a child who uses a computer. Can install programs and/or technology to attempt to control traditional Internet applications such as E-mail and Web Browsing and even newer applications such as on-line chat rooms. The authors of these more traditional applications do not evolve their programs with the goal of subverting these controls. Not so the peer to peer file sharing networks.

The authors of the peer to peer file sharing networks continue to modify and adapt their programs with the apparent goal, among others, of subverting attempts to control them. I cannot authoritatively speak as to why they wish to do this, you will have to ask them. However I know from my role as a network manager that many institutions wish to block or throttle[1] these programs either because of copyright concerns or because of the cost of providing the Internet bandwidth these applications consume.

Presumably this blocking or throttling is unpopular with the users of the file sharing programs and the authors are merely reacting to the demands of their customers!

It is worth noting that the institutions that have the most difficulty with controlling peer to peer file sharing programs are those that are completely open, or quasi open, such as universities. It is possible to completely firewall an enterprise so that file sharing programs cannot make connection across the firewall. This is accomplished by blocking all access between the internal "Intranet" and the Internet at large, and only allowing limited applications, through application level proxy programs, to cross the firewall.

However many institutions cannot enforce such a harsh policy. Research universities as a community need to permit their researchers more or less unfettered access to the Internet. It is through this access that innovation is fostered and new Internet applications are developed. In such organizations some protocols, such as E-mail or web browsing are controlled either in order to control costs, or to filter out junk E-mail. However most other protocols are permitted unimpeded. If we establish controls on the protocol ports[2] used by the peer to peer file sharing programs, the authors of those programs simply have the next version use a different port. It is also possible for them to switch ports continuously, making it difficult to track and to control.

So in conclusion, peer to peer file sharing technology is not fundamentally more or less secure then the common Internet applications that people use everyday. However the goals of the authors of these programs are, among others, to subvert controls placed on them by enterprises. As such they may permit inadvertent, or malicious compromise of those systems that an enterprise wishes to protect.

One final comment. I have been saying today that a major risk of peer to peer file sharing is that it attempts to subvert legitimate controls placed on its use. Considering the case where the controlling party is an institution or parent. However we do have to realize that sometimes the "controlling" party may be a government whose goal is to control their

1 Limit the Internet bandwidth consumed by.

2 Internet applications typically communicate over "ports" which are number assigned to the different protocols. These numbers are used by two computers communicating to label data as to what application it is for. For example E-mail travels over port 25 and most web browsing happens over port 80.

citizens access to the Internet at large. In such an environment peer to peer file sharing may well be an important way to bring freedom of expression to an otherwise oppressed population. It all depends on your point of view.

Thank you for inviting me here today and I hope I have provided information that you will find useful. I am available for any questions.

Chairman TOM DAVIS. Thank you very much.

Dr. Hale.

STATEMENT OF DR. JOHN HALE, ASSISTANT PROFESSOR OF COMPUTER SCIENCE AND DIRECTOR, CENTER FOR INFORMATION SECURITY, THE UNIVERSITY OF TULSA

Mr. HALE. Mr. Chairman, Ranking Minority Member Waxman, and members of the committee, thank you for giving me the opportunity to testify today on a topic that is of growing concern to the network security community, to American businesses and schools and, in fact, anyone that uses the Internet.

I am an Assistant Professor of Computer Science at the University of Tulsa, and serve there as the Director of its Center for Information Security.

Over the past 5 years, I have watched peer-to-peer technology make a startling transition from the backwaters of computer science to mainstream society. This March, Sharman Networks hit the 200 million mark for downloads of its popular KaZaA Media Desktop.

File-sharing softwares are in homes, businesses, and schools across the world, connecting users in a peer-wise architecture that is both resilient and efficient. Peer-to-peer networking has grown faster than the Internet itself, reaching a much broader audience at this stage of its development.

But there is a downside to placing such a potent technology in the hands of novice users. A peer-to-peer client exposes a computer to new threats, and some of the practices of its developers magnify the risk.

The prevalence of spyware in peer-to-peer clients is but one example. Developers bundle spyware in their clients to generate revenue. One company maintains that it is "intrigral" to the operation of their product.

Of course, there is no inherent functional dependency between advertising and file-sharing. Intrigral then means that the peer-to-peer software has been deliberately engineered so that it will not function without the spyware active.

To avoid detection, spyware often hides in system folders or runs in the background. Amazingly, some spyware components remain on a system long after the original application is removed and will even imbed themselves in a host, despite an aborted installation of a carrier program.

Spyware imbedded in clients sometimes downloads executable code without user knowledge. Even if the code is not malicious, it may contain flaws that render a system vulnerable to attack. More importantly, the clandestine nature of the software makes detection and remediation extremely challenging.

Peer-to-peer is also commonly designed to circumvent network security services. Techniques such as tunneling, port hopping, and push request messages make it difficult to detect and filter peer-to-peer traffic.

HTTP tunneling, in which peer-to-peer communications are disguised as Web traffic, is popular because such traffic often travels freely across networks. To this end, tunneling not only helps violate a network security policy by enabling forbidden applications, but

also expands the network perimeter in ways unknown to system administrators.

Another trick used by some of the most popular peer-to-peer clients is to vary communication ports, a technique called port hopping. This thwarts blocking and scanning software that identifies network services, based on well-known port assignments, as described previously.

Push request messages in the Gnutella protocol are used to circumvent firewalls. Instead of a client pulling a file to it, it asks the host behind the firewall to push the file out. This is all transparent to the user, but it constitutes a subtle collusion between the two clients to violate a security policy.

Another concern is how flaws in clients can increase exposures in a network, leaving it vulnerable to hackers. Exploitable weaknesses in peer-to-peer software have been identified, and in some cases, the media files themselves can enable an attack.

There is nothing special about peer-to-peer clients that makes them any more flawed than other software. However, several factors conspire to amplify the risks they induce.

They engender massive ad hoc connectivity across network domains. Hosts are exposed to every user on a peer-to-peer network. More than that, they allow users to share files pseudo-anonymously. Often, clients, themselves, are installed from peers on a network.

In short, peer-to-peer file-sharing exposes systems to untrusted hosts and software, and offers little in the way of protection.

Worms and viruses are also very real threats. The most recent example is the Fizzer virus, a blended attack that propagates via e-mail and KaZaA.

Another is the Duload worm, which hides in a system folder, and alters the registry so that runs it startup. But it then copies itself to several provocatively named files within a folder that it exposes to the peer-to-peer network. Since Duload relies on human interaction, it is more of a virus than a worm.

So Internet worms that target Web and data base servers actually provide better insight of the real potential. Code Red infected almost 400,000 Internet hosts within 14 hours, causing an estimated $2.6 billion in damage. Nimda infected 2.2 million hosts. The Slammer worm, by comparison, only affected 200,000 hosts, but set new speed records, infecting 90 percent of its victims in under 10 minutes.

A true peer-to-peer worm can infect an entire network with similar speed. More importantly, the obstacles for remediation indicate that it would have tremendous staying power, re-infected unpatched hosts and infecting new ones as they came on-line.

There is a role for technology to play in addressing these problems, but it is only a small piece of the solution. Users have to be made aware of the risks of file-sharing. Developers must live up to higher standards of integrity and transparency for the software they develop.

We cannot predict the next Code Red or Nimda. But if and when it strikes peer-to-peer networks, I hope we do not look back and see a missed opportunity to lead a promising technology out a turbulent period in its development; thank you.

[The prepared statement of Mr. Hale follows:]

Statement of John Hale
Assistant Professor of Computer Science and
Director, Center for Information Security,
The University of Tulsa
Before the Committee on Government Reform
U.S. House of Representatives

Oversight Hearing on Security and Privacy in Peer-to-Peer Networks

May 15, 2003

Mr. Chairman, Ranking Minority Member Waxman, and Members of the Committee, thank you for giving me the opportunity to testify before you today on a topic that is of growing concern to the computer security community, to American businesses and schools, and, in fact, to anyone that uses the Internet.

I am an Assistant Professor of Computer Science at the University of Tulsa, and serve there as the Director of its Center for Information Security. As an information security researcher and an educator, I have watched P2P technology make a startling transition from the backwaters of computer science to pop culture in mainstream society.

This March, Sharman Networks hit the 200 million mark for downloads of its popular Kazaa Media Desktop. Over the past two years, the active host count at any given time in the Gnutella network has ranged from 100,000 to 500,000. P2P software is installed on computers in homes, businesses and schools across the world. P2P networking has grown faster than the Internet itself, and has reached a much broader audience at this stage of its development.

Part of the attraction of P2P networks is their dynamic nature. P2P technology creates flexible *ad hoc* networks that span the globe, connecting end users in a peer-wise architecture that is both resilient and efficient. Search engines built into P2P clients are powerful and intuitive. They put a staggering volume and variety of digital content at a user's fingertips.

But there is a downside to placing such a potent technology in the hands of novice users. A P2P client can turn a computer into a server, exposing it to a new range of threats. Installation and operation is so easy that most do not fully appreciate the risks. And deceptive practices of the purveyors of P2P file sharing software who are trying to stay one step ahead of copyright owners and network administrators have made the situation much worse.

Spyware and Adware

The prevalence of embedded spyware and adware in P2P clients is but one example. Spyware monitors user behavior and tracks web browsing habits. The information collected by spyware is typically sold to companies and/or used by adware to conduct targeted web marketing. Based on an individual's browsing patterns, adware opens web pages promoting a particular product or service.

P2P developers bundle spyware and adware in their clients to generate revenue. One P2P company maintains that its embedded spyware is "integral" to the operation of their product. Of course, there is no inherent functional dependency between advertising and file sharing. In fact, lightweight implementations of P2P software have been developed that leave the spyware out. "Integral" means that the P2P software has been deliberately engineered so it will not function without the spyware active.

Spyware and adware are, by construction, difficult to detect and may be impossible to disable or remove from a client. Common tactics include hiding in system folders and running in the background from system startup. Amazingly, some spyware components remain on a system long after the original application is removed, and will even embed themselves in a host despite an aborted installation of the carrier application.

Spyware not only poses a threat to user privacy, it can also create additional vulnerabilities on a user's system. Spyware products embedded in the most popular P2P clients download executable code without user knowledge. Even if the code is not malicious, it may contain flaws that render a system open to attack. The clandestine nature of the software makes detection and remediation extremely difficult.

Circumventing Security

P2P software is commonly designed to circumvent network security services. Enterprises and institutions wishing to stem the tide of media piracy on their networks often find that P2P file sharing traffic is disguised as or hidden amongst normal network activity. Techniques such as tunneling, port hopping and push requests make it difficult to detect and filter P2P traffic. That is their intent; to foment user participation in spite of an enterprise's security policy. One consequence (intended or not) is that these techniques dramatically weaken an organization's security posture.

Tunneling embeds P2P messages within another protocol so that they blend in with other traffic, making them more difficult for firewalls and filters to detect. A common scheme is HTTP tunneling, in which P2P communications are disguised as web browsing traffic. This variation is popular because web traffic is so common and typically travels freely across enterprise networks. To this end, tunneling not only helps violate a network security policy by enabling forbidden applications but also expands the network security perimeter in ways unknown and unpredictable to system administrators.

Another commonly used trick is for P2P clients to vary their communication ports – a technique called port hopping. This thwarts blocking and scanning software that identifies network services based on well-known port assignments. Port hopping is built into the latest versions of the most popular P2P clients – and there is no reason for it other than to allow network software clients to avoid detection.

Developers of the Gnutella protocol devised a special solution that permits clients to circumvent firewalls configured to block its file request messages. In this scheme, a 'push-request' message is sent through the Gnutella network to the system behind the firewall, which then knows to initiate a file upload to the requesting host. So instead of a client 'pulling a file to it,' it asks the serving system to 'push the file out.' To the user, the net effect is the same – they get the file – but to the firewall, which usually has looser restrictions on out-bound traffic, it makes all the difference in the world. And once again, an enterprise's network security policy is violated.

Software Vulnerabilities

Another major concern is how software flaws in P2P networking clients can greatly increase the exposure in a network, leaving it vulnerable to intruders and hackers. All software has flaws, and some flaws create exposures that can be exploited to violate the security of a system.

Exploitable weaknesses in P2P software have been identified. Buffer overflow and cross-site scripting vulnerabilities were reported in early iMesh and Gnutella clients, respectively. P2P clients that use the Fasttrack protocol are known to be susceptible to Denial of Service attacks due to its client-to-client messaging architecture. Sometimes the shared files themselves enable an attack. MP3s contain special meta-data that in the past has been used to exploit buffer overflow vulnerabilities in media players. In this particular attack, a P2P network is simply a distribution mechanism for the malicious payload, but it is an incredibly effective one.

There is nothing special about P2P software that makes it inherently more flawed than other software. It is built for the same platforms and developed in the same programming languages as other computer and network applications. However, several factors conspire to make the risks induced by security vulnerabilities in P2P file sharing clients much more serious.

The first factor is that P2P clients engender massive *ad hoc* connectivity across organizational and enterprise domains. P2P file sharing networks are well beyond the administrative control of any one company or organization. A system running a P2P client may be behind a firewall, but it is exposed through the client to every user on that P2P network, regardless of their location. Simply put, P2P clients can dramatically amplify exposures to external threats.

A related factor deals with trust. P2P file trading networks are open environments that allow anyone to share files pseudo-anonymously. Trust in this circumstance is hard to

come by. Users are connected to and download files from hosts they know very little about. In many cases, the P2P client itself is installed in a bootstrap process that downloads it from a peer on the network. P2P file sharing networks expose systems to untrusted hosts and software, and offer little in the way of protection.

Enterprise security management in the presence of contraband P2P file sharing software is a supreme challenge. The dynamic nature of P2P networks, the stealth tactics employed by the software and the tendency of individuals to hide its use makes a complete inventory of P2P clients on a large network virtually impossible. This again magnifies any security vulnerabilities because inventories are essential for security remediation processes. It is very difficult to address problems on a network if you cannot find the software that is causing them.

Worms and Viruses

No discussion of security threats to P2P networks is complete without covering the potential for viruses and worms. Viruses and worms are self-replicating code that may or may not contain a malicious payload. The difference between the two is that a virus typically requires some form of human participation to propagate while a worm can spread across a network without human intervention. Both are viable modes of attack in P2P networks.

A P2P virus needs a carrier file to contain its payload. The obvious choices are audio, video and executable files traded over the network. Buffer overflow vulnerabilities have already been exploited in media players by maliciously crafted MP3 files. A virus can leverage such a weakness to execute code that replicates itself in the shared folder directory of a user. The act of downloading an infected file spreads the virus to a new host.

The recent integration of executable content in media formats creates a richer entertainment experience, but also offers a limitless palette for viral code. I am reminded that e-mail attachments became the preferred mode of virus transmission after the introduction of active content in word processing documents and web pages. Scripting means you no longer have to break an application with a buffer overflow attack. Instead, you can exploit weak security policies and input validation processes to achieve the same effect.

Several so-called P2P worms have been documented. The Duload P2P worm may be the most sophisticated of these. This piece of malicious code copies itself into the system folder and alters the registry so that it always runs at startup. It then copies itself to several provocatively named files within a media folder which it exposes to the P2P network as a shared folder. Since Duload relies on a human to download, it really acts as a virus. A true P2P worm would have to exploit a flaw in a P2P client to propagate itself across a network.

The P2P viruses uncovered to date barely hint at the real potential of self-replicating code in P2P environments. Code Red, Nimda and Slammer – worms that targeted Internet web and database servers – provide much better insight. The Code Red Internet worm infected 359,000 Internet hosts within 14 hours, causing an estimated $2.6 billion in damage. The Nimda worm caused an estimated $590 million in damage and infected 2.2 million hosts. Comparatively, the Slammer worm only infected 200,000 hosts, but set new speed records, infecting 90% of the hosts vulnerable to it on the Internet in an astonishing 10 minutes.

Likewise, a self-propagating P2P worm could infect almost every host on the P2P network, crossing enterprise network boundaries with blazing speed. More importantly, the previously discussed obstacles to efficient remediation indicate that a P2P worm would have tremendous staying power, re-infecting unpatched hosts and infecting new ones as they came online.

There is a role for technology to play in addressing these problems. Tools and systems can be developed to better monitor and secure hosts running P2P clients. Of course technology is only one piece of the solution. Users must be made aware of the risks of participating in open P2P file sharing networks. Developers must be held accountable and live up to higher standards of integrity and transparency for the P2P software they build. Ultimately, P2P technology must shed its reputation as a tool for media piracy.

In a very real sense, peer-to-peer file trading software exposes individuals and enterprises to risks above and beyond those of other software. The technology itself is beautiful in its design, but developer and user practices conspire to create a dangerous operational environment. On its current evolutionary track, threats to security and privacy posed by P2P file sharing technology will get worse, not better. We cannot predict the next Code Red or Nimda. But if and when it strikes peer-to-peer networks, I hope we do not look back to this moment in time and see a missed opportunity to lead a promising technology out of a turbulent period in its development.

Chairman TOM DAVIS. Thank you very much.
Mr. Davidson.

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

Mr. DAVIDSON. Mr. Chairman, Mr. Waxman, members of the committee, I am Alan Davidson, associate director of the Center for Democracy and Technology. CDT is a non-profit public interest group, based here in Washington, dedicated to promoting civil liberties and human rights on the Internet.

Since its creation, CDT has been heavily involved in issues of online privacy and security, and we welcome the opportunity to testify today on a timely issue of privacy and security, the question of privacy on popular peer-to-peer file-sharing systems.

We commend the committee for its thoughtful efforts on this and other topics related to peer-to-peer over the last few months and few years.

Our top line is this. The use of file-sharing software certainly raises serious privacy issues for consumers and computer users, often through mistakes that the users make in sharing very sensitive personal information.

At the same time, file-sharing technology can be very beneficial. It is new and changing, and it is largely in the control of the people who use it. So the most important thing that we can do is to inform people about the potential risks of sharing, and teach them how to use peer-to-peer safely. There are other things, as well, and I will go into that.

As we have heard, peer-to-peer file-sharing systems are a computing phenomenon. They are among the most popular and downloaded computer programs today. Much of the concern that we have comes from the fact that these are systems that just a few years ago were used by a relatively small and savvy group of people. Today, they are being embraced by millions of users, many of whom do not have a lot of expertise.

People who install these powerful tools need to be aware of the potential privacy and security risks that come from their use or their misuse. Among our top concern, first and foremost, and potentially most serious, is this issue of inadvertent sharing of sensitive personal information.

I cannot do much better than the demo that you saw in trying to make it clear how it is possible, in some cases, probably too easy, for people to share personal files. Certainly, there is a lot of evidence that some people, at least, are doing this.

A cautionary note, we need to keep this in perspective. We do not have a good set of data right now about how big a problem this is. There is not very much research in terms of quantifying how large a percentage of people are doing this. But certainly, for some people, this is a very real problem.

Second, many file-sharing programs, as we have heard, contain spyware that communicates information for advertising or for other reasons, often without a user's knowledge.

This is not a problem that peer-to-peer file-sharing networks have alone. This is a problem in many software programs for users. But whether in peer-to-peer or in other software, consumers de-

serve real notice and real choices about how their computers are going to communicate with third parties.

A third issue for us are the legal risks that people face when using these systems and the privacy issues that can come with that.

First of all, file traders who violate copyright laws face obvious legal risks. At the same time, we are concerned that at least one provision of the current law, which is the broad subpoena power that is granted to any copyright holder under Section 512(h) of the DMCA, too easily allows the identity of a peer-to-peer participant, or for that matter, any Internet user, to be unmarked wrongly or by mistake without their knowledge. That is something that we think Congress should address.

So what do we do about all of these problems? First and foremost, and I think you have already heard some of this, the public and particularly the families of file trading minors need greater awareness of the potential risks of file-sharing.

One example of how to do this is something that we have been working on, in collaboration with a number of other companies and public interest groups, which is the GetNetWise. It is a collaborative collection of tools for families seeking to protect their kids on-line. It is a Web site, GetNetWise.org, that is linked to by over 80,000 sites, including many major Internet providers, other public interest groups, Members of Congress including, I believe this committee, for which we are always grateful, and your tips on how to protect kids in peer-to-peer networks from adult content.

First of all, there is a major new initiative in this project. I have attached to the back of my testimony some of the materials from that, to try to educate parents about how to keep their kids safe when using peer-to-peer networks.

There are lots of tips. There are tips in some of the other sets of testimony that were put together. Those are the kinds of things that we need to do to really make parents and families aware of the risks that they may be facing.

There are other things that can be done, as well. Another is that we must insist that fair information practices be obeyed in file-sharing software. Much more could be done to design these systems with better transparency and better control. Software producers should reject invasive spyware, unless they find ways to give people more notice and control.

Finally, we do think that Congress should be looking at finding ways to add privacy protections to these DMCA subpoenas so that mistakes are not made.

I think our bottom line is, we do not need to throw the baby out with the bath water. There are many benefits to some of these technologies. They are also facing their own moments of dislocation and concern.

We look forward to working with Congress to find a way to make sure that privacy is protected without damaging what can be a very good source of innovation.

[The prepared statement of Mr. Davidson follows:]

Peer-to-Peer File Sharing Privacy and Security

Testimony before the House Committee on Government Reform
Alan Davidson
Associate Director
Center for Democracy and Technology
May 15, 2003

Summary

Mr. Chairman, Mr. Waxman, and Members of the Committee, the Center for Democracy and Technology welcomes this opportunity to testify on the timely issue of privacy and security on popular peer-to-peer file-sharing systems. The use of file-sharing software can raise serious privacy problems, often through mistakes by users that result in the sharing of very sensitive personal information. At the same time file-sharing technology is largely user controlled, oftentimes beneficial, and decidedly hard to regulate. A broad public education effort and better software practices are needed in order to inform people about the risks of file sharing while preserving the benefits of this valuable technology.

CDT is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values on the Internet. Since its creation in 1994, CDT has been heavily involved in the policy debates concerning privacy and computer security online. More recently, in partnership with other consumer groups, CDT has undertaken a project to articulate balanced consumer perspectives on digital copyright issues.[1]

So-called "peer-to-peer file-sharing" systems – like the popular Kazaa, Morpheus, or Grokster applications – are among the most downloaded computer programs today. People who install these powerful tools need to be aware of the potentially serious privacy and security risks that may come from their use or misuse. Key concerns facing file-sharing users include:

> Inadvertent sharing of sensitive personal information – Peer-to-peer systems make it possible, and in some cases too easy, for people to share personal files. There is evidence on major peer-to-peer networks of users sharing very sensitive documents like their tax returns, inboxes, or check registers, certainly in most cases by mistake.
> Spyware and adware – Many file-sharing programs contain "spyware" that communicates information for advertising or other reasons, often without the user's knowledge. Whether in peer-to-peer or other software, consumers deserve notice and real choices about how their computers communicate with third parties.
> Security concerns – File trading introduces risks similar to those faced by Internet users generally. People should take care to only execute files whose source they trust, and they should safeguard their computers when online.

[1] CDT is working in partnership with Public Knowledge and Consumers Union on P2P and related copyright issues, made possible in part by the support of the MacArthur Foundation and the Robert J. Glushko and Pamela Samuelson Foundation.

Legal risks – File traders who violate copyright laws face obvious legal risks. At the same time, CDT is concerned that at least one provision of current law – the broad subpoena power granted any copyright holder under Section 512(h) of the Digital Millennium Copyright Act – too easily allows the identity of a peer-to-peer participant or any Internet user to be unmasked wrongly or by mistake without their knowledge.

These concerns are exacerbated by the growing use of file-sharing programs by millions of individuals and families, often with little or no training or experience.

With these risks come benefits. Peer-to-peer file sharing can be used for legitimate, non-infringing file distribution. Its underlying technology, not so different from peer-to-peer networks like the World Wide Web, is rapidly evolving and being adopted for many new uses. Regulating this technology without broader ramifications would be difficult, and could have many unintended consequences.

How then do we address these real privacy and security concerns? CDT believes that an active program of education and better software practices is needed. Such a program would:

Inform people about the risks in file sharing – The public, and particularly the families of file-trading minors, need greater awareness of the potential risks of file sharing. Educational efforts—like the Internet community GetNetWise website—are already including tips for safe peer-to-peer use that should be widely disseminated.
Seek fair information practices in file-sharing software – Much more should be done to design peer-to-peer software with transparency and better control over shared files. Software producers should reject invasive spyware, adopt fair information practices, and must provide better notice when information is transmitted to third parties.
Add privacy protections for DMCA subpoenas – Privacy and safety protections for end users should be included in the broad DMCA Section 512(h) subpoena provision in order to require more due process – including notice to the user and other protections– before ISPs are compelled to reveal sensitive personal identity information.
Prevent invasive "self-help" tactics- In no circumstances should it be legal to damage another person's computer or files based on allegations of wrong-doing, including copyright infringement.

All of this should take place against the broader backdrop of action regarding Internet privacy generally, where the continued growth of privacy technologies and industry self-regulatory efforts along with baseline privacy legislation are necessary to ensure public trust and democratic values.

Congress has a valuable role to play in educating the public about the potential risks of file-sharing systems, in encouraging companies to design more user-friendly systems, and in modifying current legal provisions that create privacy risks. CDT looks forward to working with this Committee and others to further these efforts.

1. The Growing Use of Peer-to-Peer File Sharing Networks

Peer-to-peer (P2P) file sharing networks are an important and rapidly growing new channel for Internet communication. Millions of people are using P2P networks today to share text, software, audio, and video files stored on their computers. By helping users communicate directly with minimal (in some cases no) central coordination, peer-to-peer networks can allow people to share data with far greater freedom and flexibility.

While the P2P file-sharing phenomenon is relatively new, "peer-to-peer" technology underlies the Internet communications model. In many ways, the Internet is the world's largest peer-to-peer network. E-mail, the World Wide Web, and instant messaging are all "peer-to-peer" applications.

The kinds of peer-to-peer networks that are the topic of today's hearing are the new, highly decentralized systems for sharing information stored on many distributed computers. Napster first brought P2P into the public eye; now largely defunct, its progeny like Kazaa, Morpheus, or Grokster are used by millions today.

Peer-to-peer file sharing networks differ from other Internet applications in that they tend to share data from a large number of end user computers rather than from the more central computers we generally think of as Web servers. A key innovation of peer-to-peer file sharing networks is their sophisticated mechanisms for searching millions of "shared" files to find data among many connected systems. Information on P2P networks tends to be less centrally controlled and more reflective of what end user participants believe is valuable or worth sharing.

File-sharing networks have become remarkably popular in a very short time. The leading peer-to-peer file sharing software, Kazaa Media Desktop, has been downloaded over 200 million times and claims over 60 million users worldwide, and continues to grow in popularity.[2] At any given moment, as many as 4 million users might be participating in the Kazaa network, sharing thousands of terabytes of information. Millions of others regularly use Gnutella, a related open source sharing system.

Peer-to-peer networks have become notorious for fostering piracy of copyrighted materials. A tremendous number of copyrighted songs, video programs, and games have made their way onto file-sharing networks without authorization. While outside of the scope of this hearing, CDT does not condone the widespread infringement of copyright online.

---

[2] "200m - Hooray!" Sharman Networks press release. March 11, 2003. Available at <http://www.kazaa.com/us/news/201.htm>. Woody, Todd. "The Race to Kill Kazaa." Wired. February 2003. Available at <http://www.wired.com/wired/archive/11.02/kazaa.html>.

Less visibly, peer-to-peer file-sharing technology can support valuable new applications.[3] Some examples include:

> **Data coordination and collaboration**. Peer-to-peer technology is being used by organizations to give workers up-to-the minute data and to facilitate group coordination on large-scale projects. For example, humanitarian groups in Iraq are using peer-to-peer technology to synchronize distribution of aid to the Iraqi people.[4] The fact that peer-to-peer systems require no central servers and minimal centralized coordination makes them ideal for use in environments with little infrastructure.
>
> **Lawful music sharing.** Peer-to-peer file sharing networks can help users share music lawfully. For example, Furthur Network is a non-commercial, open-source peer-to-peer file-sharing network of live music from bands such as the Grateful Dead, the Allman Brothers, and the Dave Matthews Band.[5] The network is designed so that bands who explicitly authorize the taping and redistribution of their shows can help their fans share recordings of performances from around the globe.
>
> **Public domain material.** Project Gutenberg seeks to distribute via the Internet thousands of works available in the public domain and other freely available works such as the King James Bible, the works of Shakespeare, and the CIA World Fact Book.[6] Peer-to-peer technology will allow Project Gutenberg and other content publishers to significant diminish the costs associated with making content available to millions of people.

These applications thrive as a result of the flexibility of peer-to-peer architectures. At the same time, with this flexibility has come new risks: infringement of copyrighted works, availability of explicit content, and questions about privacy and security.

Even as new uses are found for P2P file sharing, the underlying technology itself is rapidly evolving. New generations of file-sharing systems will be even more decentralized, support greater anonymity among users, split files among different computers, and rapidly change protocol settings to defy attempts at interdiction.[7] These changes are likely to ease some

---

[3] Additional details about the importance of peer-to-peer networks are available in Sohn, Gigi B. "Statement of Gigi B. Sohn, President, Public Knowledge. 'Piracy of Intellectual Property on Peer-to-Peer Networks.'" Testimony before the House Judiciary Committee, Subcommittee on Courts, the Internet, and Intellectual Property. September 26, 2002. Available at <http://www.house.gov/judiciary/sohn092602.htm>.

[4] Jones, Mark. "Taking Collaboration to the Masses." *InfoWorld.* April 11, 2003. Available at <http://www.infoworld.com/article/03/04/11/15noise_1.html>.

[5] More information about Furthur Network is available at <http://www.furthurnet.com/>.

[6] More information about Project Gutenberg is available at <http://www.promo.net/pg/>.

[7] Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman. "The Darknet and the Future of Content Distribution." *2002 ACM Workshop on Digital Rights Management.* Available at <http://crypto.stanford.edu/DRM2002/darknet5.doc>.

concerns (by enhancing privacy and security, for example) and exacerbate others (by defying efforts to regulate P2P use.) As a whole they underscore the difficulty of policy-level efforts to deal with a changing and complex technology.

2. Privacy and Security on Peer-to-Peer File-Sharing Networks

Peer-to-peer file-sharing systems are powerful tools for sharing information with millions of other people around the world. People who install these tools need to be aware of the potentially serious privacy risks that may come from their use or misuse.

In many respects the problems facing peer-to-peer users are akin to the problems facing any speaker on the Internet. For example, someone who creates a website to share family pictures could inadvertently place sensitive files or pictures they don't wish to share on their site.[8] Many of us have a favorite story about someone who sent an embarrassing email message to a mailing list by mistake.

Several factors heighten privacy concerns for peer-to-peer networks. They are used by millions of consumers, typically with far less expertise than the average web publisher. Their powerful search capabilities can make files more widely accessible than other publishing tools. The sharing activities of these systems can be less transparent to users, especially for those unfamiliar with their workings.

Privacy risks

Peer-to-peer systems make it possible, and in some cases too easy, for people to share personal files. Two academic studies as well as CDT's own qualitative research indicates that as least some file-sharing users are sharing highly sensitive personal documents on major peer-to-peer networks.

For example, a recent study by Good and Krekelberg[9] found dozens of examples of Kazaa users who were sharing sensitive documents like their tax returns, email inboxes, or check registers, certainly in most cases by mistake. In doing so, these people are making financial information, personal files, and even intimate correspondence easily available to millions of users around the world.

It appears that much sharing of personal information is inadvertent and the result of misconfiguration or popular misconceptions about how file sharing works. For example, many file-sharing systems come with a default that files in a "shared" directory will be available to others. Some users may not realize that any files in that shared directory, often

---

[8] Even professional corporate web site operators have been known to inadvertently share sensitive corporate data on the web. And new web authoring tools, like Apple Computer's .mac initiative, make it even easier for consumers to share files and publish web sites.

[9] Good, Nathaniel 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>.

including any files they download, will automatically be shared unless they take steps to avoid sharing.

Some systems have been designed to maximize sharing. For example, many systems default at installation to allow sharing of the shared folder. They may also suggest that users find other directories to share and will assist users in doing so. Many of the most popular file-sharing systems are upgrading their systems to make misconfiguration harder. For example, while early versions of Kazaa appeared to encourage greater sharing a more recent version creates a pop-up screen demanding confirmation before sharing a whole drive (and the software appropriately suggests *not* sharing the drive, though it's default setting remains "Yes".)

Diaries, personal letters, email, and financial records are commonly found on personal computers today and could be shared inadvertently if someone were, for example, to share their whole hard drive. Once available, these sensitive files could be used to commit fraud, invade privacy, or even commit identity theft.

Though such consequences are sobering, it is important to keep the size of the problem in perspective. GAO and FTC studies on identity theft indicate that, in cases where the source of an identity theft is known, Internet or e-commerce sources constitute a very small percentage of identity theft cases.[10] To date CDT knows of no identity theft case that has been attributed to peer-to-peer file sharing problems.

CDT is also not aware of any study of the scope of file sharing privacy problems. Available data seems to indicate that the percentage of peer-to-peer users who inadvertently share sensitive files is very small.[11] This is an important area for future research.

"Spyware" Risks

A troubling privacy and security issue facing peer-to-peer file sharing networks is the use of so-called "spyware" programs."Spyware" is software that, without the user's knowledge, gathers information about an Internet user and sends that information to a third party. A number of popular peer-to-peer file sharing software programs have been found to install spyware onto user's computers, often without the user's knowledge.[12] Once installed, the programs may transmit sensitive information and are often hard to remove.

---

[10] U.S. General Accounting Office. "Identity Theft: Prevalence and Cost Seem to be Growing." GAO-02-363, March 2002. Available at <http://www.consumer.gov/idtheft/reports/geo-d02363.pdf>. Federal Trade Commission. "Information on Identity Theft for Consumers and Victims From January 2002 Through December 2002." Available at <http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf>.

[11] Most estimates of the number of users sharing sensitive files number in the dozens or hundreds. While this is significant, the total number of users connected to a given P2P file-sharing network may number in the millions. This seems to indicate that the number of people accidentally sharing sensitive files may be considerably less than 1% of all users.

[12] Metz, Cade. "Spyware: It's Lurking On Your Machine." *PC Magazine.* April 22, 2003. Page 85. Available at <http://www.pcmag.com/article2/0,4149,977889,00.asp>.

There are many forms of spyware, and not all are alike. 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. "W32.Dlder.Trojan" has been found in past versions of popular file-sharing programs such as BearShare, LimeWire, and Kazaa.[13]
>
> "vx2.dll," a spyware program file packaged with certain versions of Audio Galaxy, capable of capturing lists of Web site visited, creating pop-up ads, and even capturing user's input into Web forms and comment boxes -- potentially even sensitive information like credit card numbers or Social Security numbers.[14]

The Fair Information Practices provide a baseline for protection of personal information -- a baseline with which spyware does not comply. The surreptitious manner in which spyware operates denies users any opportunities for notice, consent, access, or other critical abilities. As such, spyware constitutes a significant threat to the privacy of the users of peer-to-peer file sharing networks, and of all Internet users.

Moreover, some spyware conceals itself from users and may even obstruct users' attempts to disable it. This can prevent users from even knowing what software is running on their computer, let alone take corrective action.

CDT believes that the spyware problem demands greater transparency. Users need to be notified whenever a piece of software is installed on their computer, especially one that could diminish the security and stability of their computer and the sensitive information on it. Increased transparency would permit users to make informed decisions about the software they use, and would incentivize software makers to address known flaws in their software. The fair information practices that describe how best to handle personal information can and should be applied as well to the technologies that collect personal information.

Security Risks

Users of P2P file-sharing systems face many of the same security risks as other Internet users. Just as in other applications, P2P users must take care to only run programs from sources that they trust, and should be careful to check for viruses. They should safeguard their computer from attack when online. File sharing adds an extra dimension to these concerns due to the quantity and frequency of files traded, the relatively unsophisticated user base, and the rise of self-help systems to prevent copyright infringement. At this time, P2P

---

[13] Delio, Michelle. "What They Know Could Hurt You." *Wired News.* January 3, 2002. Available at <http://www.wired.com/news/privacy/0,1848,49430,00.html>.

[14] Benner, Jeffrey. "Spyware, In A Galaxy Near You." *Wired News.* January 24, 2002. Available at <http://www.wired.com/news/technology/0,1282,49960,00.html>.

file-sharing applications are not known to be any less -- or any more -- secure than Internet applications on the market in other areas.

Viruses - Because peer-to-peer file sharing networks enable files to be transferred among millions of computers -- most of which are owned and operated by total strangers -- there is an ever-present risk that files downloaded from a peer-to-peer file sharing network could carry various kinds of malicious software like viruses and "worms."

It is, of course, possible to receive a dangerous file in numerous ways, such as over the Web or by e-mail. The best protection against viruses continues to be the use of up-to-date anti-virus software. 100% protection can never be achieved, but users should be aware that to download files without adequate protection opens them up to substantial risks.

Online Attacks - When peer-to-peer networks identify shared files to millions of users, they also identify the location of a user's computer, and could even target that computer's IP address (Internet Protocol address) with attempts to gain access. This is not a risk unique to peer-to-peer file sharing networks; all Internet communications involve an exchange of IP addresses. But because peer-to-peer file sharing networks search millions of computers, they can provide access to millions of IP addresses.

"Self-Help" Attacks – A new form of security threat may be growing for peer-to-peer users in the rise of "self-help" techniques by copyright holders concerned about infringement on file-trading networks. More benign versions flood P2P networks with bogus copies of copyrighted works in order to fool people into downloading or storing them. Such practices are considered legal because they do not disrupt the technical operation of a person's computer or networks.

Some companies are reportedly pursuing more invasive forms of self-help. The *New York Times* recently reported that companies were investigating systems that invade the computer of a suspected copyright infringer and delete files, slow network access, or even do more permanent damage.[15] Such practices are most likely illegal today, but amendments to our computer crime statutes have been proposed to allow some of them in the future.

CDT is concerned that invasive self-help measures create privacy and security risks for users. Innocent users might find their computers attacked by mistake, perhaps due to a confusingly named files. A person's computer might stop working without them ever know why. Even infringers might not warrant the costly effects of damaging self-help measures.

More generally, the overall security of these networks and of the Internet itself would be harmed by the sanctioned development of attack tools that might be used for inappropriate purposes. Instead, we strongly believe that copyright infringement should be punished in accordance with current law, with due process afforded.

---

[15] Sorkin, Andrew Ross. "Software Bullet is Sought to Kill Music Piracy." *The New York Times*. May 4, 2003. Available at <http://www.nytimes.com/2003/05/04/business/04MUSI.html?ex=1053001791&ei=1&en=8d9f2b1d372d373>.

Legal risks

File traders who violate copyright laws risk lawsuits, civil penalties, and even criminal prosecution. These actions typically begin with efforts to identify individuals and can result in the disclosure of personal information. Peer to peer users should always be aware of the legal penalties for copyright infringement and should share legally, and responsibly.

At the same time, CDT is concerned that at least one provision of current law– the broad subpoena power granted any copyright holder under Section 512(h) of the Digital Millennium Copyright Act–too easily allows the identity of a peer-to-peer participant or any Internet user to be unmasked wrongly or by mistake, without their knowledge.

CDT strongly sympathizes with the need of copyright holders to identify potential infringers in order to enforce their legal rights online and curb the increasing piracy of digital content. At the same time, the unique subpoena provision in DMCA Section 512(h) and the interpretation of that provision in the recent Federal court rulings in *RIAA v. Verizon* raises important privacy concerns. In that case, Verizon, a prominent ISP, challenged the recording industry's attempt to gain identifying information about Verizon customers through a 512(h) subpoena. The court permitted the subpoena, and its broad interpretation of section 512(h) has raised serious concerns about the privacy of Internet users who are thought -- even mistakenly -- to be sharing copyrighted content.

Section 512(h) would permit any copyright holder – possibly millions of organizations and individuals – to compel an ISP to disclose the identity of an Internet user based on an allegation of copyright infringement. This disclosure of personally identifying information would take place without requiring any notice to the end user that his or her identity had been unmasked, and without extensive legal review or judicial oversight as to the likely truth of the allegations. An ISP could now be compelled to disclose the identity of any user of its networks – such as someone downloading a web page – who is alleged to be a copyright infringer, not just those who host materials at an ISP. Although we recognize the importance of fighting massive copyright infringement online, we are concerned that personal identifying data about users will be revealed without their knowledge due to misuse, abuse, or mistake, casting a chill on their privacy and security.

Recent events illustrate the extent to which mistakes can be made in seeking action against alleged infringers. This week the RIAA formally apologized for a letter sent to Penn State University threatening legal action over a music file created by PSU Professor Emeritus Peter Usher that was apparently confused with the copyrighted work of the recording artist Usher.[16] Had such a mistake been made in the context of a 512(h) subpoena, the end user

[16] McCullagh, Declan. "RIAA apologizes for threatening letter." *CNet News.com*, May 12, 2003. Available at <http://news.com.com/2100-1025_3-1001095.html>. Recent reports have shown that the Usher incident is just one of a number of mistaken notices sent by content companies. See McCullagh, Declan. "RIAA apologizes for erroneous letters." *CNet News.com*, May 13, 2003. Available at <http://news.com.com/2100-1025-1001319.html>. Also, in a submission before the court in *RIAA v. Verizon*, ISP UUNET assembled a list of notices it had received since January 2001. Among those notices were numerous files mistakenly associated with recording artist George Harrison, including pictures such as "Portrait of mrs harrison williams 1943.jpg"

could easily have had sensitive identity information released without his or her knowledge.

Effective copyright enforcement need not come at the expense of individual privacy. CDT believes that a better balance can and should be struck. For example, providing end users with notice when their identity is revealed would go a long way toward preventing abuse by giving those with the greatest interest in correcting mistakes an opportunity to contest release of their information. Courts could be required to exercise greater oversight. Sanctions could be put in place for misuse. Reporting requirements could be established to ensure that provisions were not being used in ways beyond what Congress intended. ISPs could be compensated for the efforts required to identify users, in part to provide a check against repeated and inappropriate use.

Many of these suggestions -- particularly a notice requirement -- could simultaneously protect user privacy while advancing intellectual property protection online. We believe that resolving this issue will ultimately be a policy question for Congress to decide if the courts continue to uphold a broad interpretation of the provision.

3. Suggested Approaches for Dealing with Peer-to-Peer Privacy and Security

Regulating peer-to-peer file-sharing technologies directly is likely to be difficult and undesirable. The systems we tend to think of as "peer-to-peer" share many characteristics with other Internet technologies like instant messaging, network file transfer protocols, and even email or web browsing. The rapid evolution of these systems—from central control towards decentralized systems with encrypted data, anonymous clients, rotating ports, and split files – will continue to make it hard to isolate peer-to-peer traffic. The technology itself is oftentimes beneficial and the source of innovation.

In many ways file sharing is inherently user-controlled. Users decide which directories to share and what files to download. For that reason the most critical privacy protections for peer-to-peer are best addressed through user education about how to protect themselves and how to choose applications that respect their privacy. In only a few key areas – where developers fail to obey fair information practices, or where the law already has created privacy risks – might legal changes be needed.

We believe several key steps should be taken to protect privacy and security without jeopardizing the benefits of this important new technology.

Inform Users About Privacy and Security Concerns in Peer-to-Peer File Sharing - Users need to better understand the basic operation and potential risks of peer-to-peer systems. Based on these and other concerns, CDT has developed a set of Tips for Safe Sharing attached at Appendix I. These and sets of tips like it are among the types of resources that should be shared widely with peer-to-peer users.

---

and with the movie *Harry Potter and the Sorcerer's Stone*, including a text file entitled "harry potter book report.rtf."

Raising public awareness is a critical first step. CDT, along with over forty-five other Internet industry companies and public interest groups, has helped create a family information portal called GetNetWise (see *http://www.getnetwise.org*). Established in 1999, GNW is a comprehensive collection of tools for families seeking to protect their children online. Its web site is linked to by over 80,000 other sites, including major Web companies like Yahoo!, MSN, and AOL, public interest organizations like CDT and the National Center for Missing and Exploited Children schools, individual Internet users, and the offices of numerous members of Congress. Now there is an effort underway to expand GetNetWise's offerings into other areas of Internet privacy and security. New resources are currently being developed describing how families can protect themselves when using peer-to-peer file sharing networks. (A copy of GetNetWise's peer-to-peer resource pages is attached as Appendix II.)

With such a broad base of support, GetNetWise's offerings can help catalyze discussion among the industry, public interest, and lawmakers about privacy and security throughout the Internet. CDT hopes that members of Congress will continue to view GetNetWise as a valuable tool to educate American Internet users about the risks that exist online, and how to protect oneself against them.

Expect fair information practices in file-sharing software - The developers of file-sharing software could do much more to make it easier to use, with greater transparency and better control over shared files. The Kazaa usability study, for example, notes how difficult it can be to determine what files are shared. Pop-up warnings about sharing drives, default settings that favor privacy, limits on tools that assist in sharing more files, and simpler user interfaces generally should be standard features for powerful file-sharing software.

More importantly, like others who might collect personal information peer-to-peer software producers should adopt fair information practices,[17] particularly regarding any use of adware or spyware. Better notice at a minimum should be provided – including privacy policies and machine-readable notices like P3P, the Platform for Privacy Preferences[18]. Meaningful choice about collection of information, access to information stored, and other fair information practices should be followed as well.

We recognize that a diverse and young marketplace, including small companies and open source developers, may not be equipped to deal with such practices. But unless such practices are adopted through industry standard setting groups that are open to consumer participation, users will feel the need for more regulatory approaches.

Add privacy protections for DMCA subpoenas – As noted above, the broad DMCA Section 512(h) subpoena provision allows the sensitive identity of Internet users to be unmasked by any copyright holder, without the knowledge of the user, and with little oversight. Privacy

---

[17] For example, the OECD Guidelines for the privacy of personal records are generally cited as a baseline of fair information practices. Available at <http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>.

[18] More information about P3P is available at <http://www.w3.org/P3P/>.

and safety protections should be attached to this authority to prevent misuse, abuse, or mistake. In many areas of electronic surveillance and privacy Congress has struck a balance to support enforcement while protecting privacy. This example need not be different. Numerous due process tools are at our disposal – including notice to the end user when their privacy is being invaded, additional judicial scrutiny, reporting and audit requirements, cost reimbursement to ISPs (as a check on misuse), and other protections.

Such tools can and should be put to use in a way that simultaneously protects users and advances the cause of intellectual property protection. In particular, attaching a notice requirement to the 512(h) subpoena provision of DMCA would both help protect the anonymity of innocent users and serve as a warning to those who would engage in copyright infringement. Privacy need not come at the expense of enforcement.

Prevent invasive "self-help" tactics- Under no circumstances should it be made legal to damage another person's computer or files based on mere allegations of wrong-doing, including copyright infringement. Efforts to amend the computer crime, anti-hacking, or electronic privacy laws to allow for invasive self-help measures without adequate due process should be resisted.

Continue the broader push for Internet privacy protections – All of these efforts take place in the context of a broader debate about protecting privacy in a digital age where more personal information is in the hands of third parties, particularly online. The application of fair information practices remains a touchstone of privacy online, although not always a sufficient one. CDT continues to believe that a three-part package of technology protection measures (like encryption, anonymizers, or P3P), self-regulation (like the adoption of notice, choice and other practices by companies), and where needed, narrowly tailored and technology-neutral baseline privacy legislation.

4. Conclusion

History is replete with examples of technological change that sparked fear and social concern. The automobile, the telephone, email itself, were all greeted by skepticism and concern about the very real dislocations and social changes they caused. Some issues turned out to be serious; others hyperbolic; in each instance people adapted, policy responses were crafted as needed, and concerns were dealt with while preserving innovation and societal benefits.[19]

Peer-to-peer file sharing is likely facing such a moment of dislocation. The concerns it raises are very real. Preserving the potential benefits of the innovation and open, decentralized communication model that P2P is part of will be important as well.

Solving the problems of peer-to-peer privacy and security will ultimately require the cooperation of the Internet industry, lawmakers, and the public interest sector in order to be

[19] See, e.g., Standage, Tom. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers.* New York: Berkley, 1998.

effective. By fostering dialogue and promoting public awareness, Congress can help guide this process as well as raise the public profile of these important issues. Additionally, continued dialogue will help illuminate the path forward and will help users and policymakers avoid the pitfalls of premature regulation. CDT looks forward to participating in the effort to promote safe, secure use of these valuable tools.

House Rule XI, Clause 2(g)(4) Disclosure: Neither Alan Davidson nor CDT has received any federal grant, contract, or subcontract in the current or preceding two fiscal years.

Appendix I: CDT's Tips for Safe File Sharing

To aid in the education effort, CDT has assembled its own list of tips to help users keep their file sharing safe.

1. **Know what files you're sharing.** Sharing files makes them accessible to millions of people. Be sure you know what you're sharing. Many applications automatically share files you've downloaded. Others make it too easy to share parts of your hard drive that might contain personal information. Monitor what files your computer is sharing, particularly if several people use your computer.
2. **Be careful with files you download.** Downloaded files can be a source of viruses or other damaging software. As with any files you download, be sure you sufficiently trust their source before using them. Make sure that your computer is protected with up-to-date anti-virus software.
3. **Use the security tools.** Many tools to protect privacy and security on peer-to-peer networks are already available, and more are being developed. These include network firewalls, spyware-removal tools, and newer, more secure file sharing clients.
4. **Share lawfully.** Unlawful sharing of copyrighted works can result in serious legal liability. Peer-to-peer users should know whether they are infringing copyrights in their activities and should keep their file sharing legal at all times.
5. **Look out for spyware.** Some file-sharing programs collect information about your computer use and may transmit it to third parties. Try to be aware of what information your software is collecting, and avoid programs that collect more information about you than you want. If you think you may have downloaded spyware and you want to remove it, consider using one of the Net's many anti-spyware tools. An informed marketplace, cautious about using tools that collect too much personal information without obeying fair information practices, is likely to be the most powerful force to counteract bad practices.
6. **Talk to your family.** Just as they have many important benefits, peer-to-peer file sharing networks also may carry real dangers. Families should be particularly aware of the risks facing children who use these networks.

For other tips for protecting privacy and security online, see CDT's privacy resource guide at <http://www.cdt.org/privacy>.

Appendix II: GetNetWise Resources on File Sharing

GetNetWise.org, a comprehensive online resource for families seeking to keep children safe online, has recently developed a resource to help answer questions about online file sharing. (See attached).

File-sharing Risks

GetNetWiseTV: Anne Collier on File-sharing Risks

Peer-to-peer or file-sharing programs allow you to share your files with others on the Internet -- and vice versa. File-sharing is a new and interesting technology that shows promise for future applications. However, just like you shouldn't open email attachments from people you don't trust, you should be wary about downloading files from them as well. You never know what you or your kids may find on the hard drives of random strangers on the Internet. [How file-sharing works]

The best tip for file-sharing is to stop and think before downloading files through these networks. Here are more tips to keep your and your kids' file-sharing safe, secure and legal. Some of the risks associated with using file-sharing programs include:

Kids' Access to Pornography

Many file-sharing programs allow children to access inappropriate audio and video clips -- most of a sexually explicit nature. Kids searching for popular music files may sometimes inadvertently pull up sexually explicit files that use the same keywords. For older children, parents should be concerned about their access to other people's video libraries that may contain inappropriate videos. If you're concerned about these things, make sure to check your computer for file-sharing programs. See a list of some file-sharing programs. Some parental-control tools on the market do not restrict access to file-sharing technologies. Check the GetNetWise Tools for [illegible] peer-to-peer networks.

Copyright Law

Many of the files available on file-sharing networks, such as many movies, songs, and video games, are copyrighted by the owner. That means that the law protects the owner's right to copy and distribute their content. What does the copyright mean to you? It means that downloading copyrighted music, movies and software using these file-sharing programs without the copyright owner's permission could put you in serious legal trouble. Peer-to-peer users should be aware that they may not be anonymous while using these networks. Copyright holders have located peer-to-peer copyright infringers and have sued them. So, make sure that you or your family does not infringe copyright while using filesharing networks. Be smart, and keep your file-sharing legal.

Dewie

www.fbi.gov

Dewie Explains the Risks and Threats to Cyberspace

Learn more about...

Viruses

Firewalls

E-Mail Filters

Sharing

Teaching Kids about Security

Computer Security

Sharing files with people you don't trust is a matter of hygiene -- and you should keep your computer as clean as possible. Using file-sharing networks creates a risk that viruses or other malignant code could be spread to your computer over the network. Computer security experts are starting to see viruses and malignant code (spyware) spread through file-sharing services. Viruses may damage your computer or interfere with your files; spyware may track your online activities and send that information to third parties. Spyware has been spotted in many places on file-sharing networks -- including packaged with the file-sharing clients themselves.

Privacy

If mis-configured, some file-sharing programs may expose the entirety of your hard drive to all other users of the file-sharing software. If you keep sensitive information on your computer, like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.

Privacy Policy Contact GetNetWise.org Tell-a-Friend Get the GNW Newsletter
Copyright © 1999-2003 Internet Education Foundation. All Rights Reserved.

Dewie Explains the Risks and Threats to Cyberspace

Learn more about...

- Viruses
- Firewalls
- E-Mail Filters
- Sharing
- Teaching Kids about Security

File-sharing Tips

The best tip for file-sharing is to stop and think before downloading files through these networks. It's best to keep your and your kids' file-sharing safe, secure and legal. Here are more tips:

- **Don't download files from people you don't trust** -- Just like you shouldn't open e-mail attachments from people you don't trust, you should be wary about downloading files from them as well.
- **Keep your file-sharing legal** -- Downloading copyrighted music, movies and software using these file-sharing programs without the copyright owner's permission could put you in serious legal trouble. Peer-to-peer users should be aware that they may not be anonymous while using these networks. Copyright holders have located peer-to-peer copyright infringers and have sued them. There are a growing number of online music and movie services where you can stream, download or purchase digital files with the copyright owners' permission. Using these services is one way to ensure that you will avoid unwanted lawsuits.
- **Watch out for "spy-ware"** -- Some file-sharing programs embed "spy-ware" programs when you install them on your computer. These programs can run in the background and create unwanted pop-up advertisements and some even monitor your online behavior.
- **Use and update your anti-virus software** -- Computer experts are starting to see viruses being spread through file-sharing networks. Be careful what you download and always make sure your anti-virus software is running and frequently updated.
- **Secure your sensitive computer information** -- If you keep sensitive information on your computer like your tax return information and online bank account data, check to make sure that you are not inadvertently making this available to thousands of strangers on the Internet.
- **Parents, talk to your kids** -- Parents should beware that file-sharing networks contain inappropriate audio and video clips -- many of a sexually explicit nature.

Copyright © 1999-2003 Internet Education Foundation. All Rights Reserved.

Chairman TOM DAVIS. Thank you very much.

Mr. Broes.

STATEMENT OF DEREK S. BROES, EXECUTIVE VICE PRESIDENT OF WORLDWIDE OPERATIONS, BRILLIANT DIGITAL ENTERTAINMENT

Mr. BROES. Thank you for inviting me. Chairman Davis, Representative Waxman, and members of the committee, I am Derek Broes. I am the executive vice president of Worldwide Operations for Brilliant Digital Entertainment and its subsidiary, Altnet.

Altnet offers the largest secure commercial platform for distribution of digital content over peer-to-peer software-based networks.

Under an exclusive agreement with Sharman Networks Limited, publisher of KaZaA Media Desk peer-to-peer application, Altnet reaches an estimated 75 million worldwide unique users per month. That is 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. As you will hear in my testimony today, Altnet is leveraging its role as the 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 in any democracy, there are challenges that must be overcome, and moral and ethical standards to be established. As with any technology that reaches millions of people, there is a responsibility that every company must assume when creating an instant messenger, e-mail, peer-to-peer, online interactive games, chat rooms, or any technology designed to share digital words or files with anyone, any time, instantly.

My past experience in the entertainment industry, combined with experience in Internet peer-to-peer security technologies, gives me a uniquely broad perspective on the issues before the committee here 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 solvable with simply 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 and the Recording Industry Association of America, and that was from an anti-piracy point of view.

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

While there are some unique challenges to making file-sharing programs applications more secure, which I will outline, it is important that we de-mystify these technologies and realize that the

many protective security technologies that are already widely available.

By simply adopting the standards commonly used by the World Wide Web such as Secure Socket Layer, 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 works and how to be a safe and responsible user of that 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 as with e-mail and instant messenger technologies, is the spread of viruses. As you would expect, when files come from an anonymous and uncertified source, the risk of that file containing a virus is greatly increased.

In addition, many file-sharing applications provide a tool to allow users to search their hard drives for files to share. If that tool is used incorrectly, users could inadvertently give access to their confidential files and folders.

Allow me to review how Altnet meets the 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's patented technology called "TrueNames" 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.

Sharman Networks has taken great care to protect users' privacy and security. As distributors of the most popular peer-to-peer application today, Sharman Networks has consistently led the field with security enhancements developed explicitly for the challenges of this new industry, including the peer-to-peer's first built-in anti-virus tool.

KaZaA Media Desktop contains two layers of propriety virus protection technology. In addition, Bullguard, a well-known anti-virus software, is installed free with the KaZaA Media Desktop application, providing users with an additional layer of security and protection.

Sharman has shown great commitment to ensure that any new malicious viruses that freeze or silence or otherwise compromise a user's PC and its information are detected by this software, as was with Fizzer.

Altnet and Sharman Networks take every opportunity to encourage responsible and safe peer-to-peer usage through user education and via the default configuration of the software of the upcoming release.

The nature of the decentralized peer-to-peer technology means that users are in control of the material they choose to share with

others. Our goal is to provide them with the education and tools they need for safe and responsible use.

Commercialization of the World Wide Web has lead to the creation and adoption of advanced security, privacy policies and protection technologies, and the evolution of file-sharing networks will follow that same path.

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 principles 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 an 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 insure that we continue to meet the responsibilities we have assumed. Thank you, Mr. Chairman, for the opportunity to participate in this important hearing today.

[The prepared statement of Mr. Broes follows:]

Testimony of Derek S. Broes

Before The
House Government Reform Committee

Overexposed:
The Threats to Privacy and Security on File Sharing Networks

May 15, 2003

Chairman Davis, Representative Waxman, 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.

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's patented technology called "TrueNames" 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.

Sharman Networks has taken great care to protect users' privacy and security. As distributors of the most popular peer-to-peer application today, Sharman Networks has consistently lead the field with security enhancements developed explicitly for the challenges of this new industry, including peer to peer's first built-in anti-virus tool. Kazaa Media Desktop contains two layers of proprietary virus protection technology. In addition, Bullguard, a well-known anti-virus software, is installed free with the Kazaa Media Desktop application, providing users with an additional layer of

protection. Sharman has shown great commitment to ensure that any new malicious viruses that 'freeze', 'silence' or otherwise compromise a users PC and its information are detected by this software.

Altnet and Sharman Networks take 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 provide them with the education and tools they need for safe and responsible use.

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.

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 insure that we continue to meet the responsibilities we have assumed.

Thank you, Mr. Chairman, for the opportunity to have participated in this most important hearing.

Sincerely,

Derek S. Broes
Executive Vice President of Worldwide Operations
Brilliant Digital Entertainment

Chairman TOM DAVIS. Thank you very much.
Ms. Frank.

STATEMENT OF MARI J. FRANK, ESQUIRE, MARI J. FRANK, ESQUIRE & ASSOCIATES

Ms. FRANK. Good morning, Chairman Davis, Ranking Member Waxman, honorable committee members and invited guests. Thank you for the opportunity to address you today.

My name is Mari Frank, and I am attorney and the author of the "Identity Theft Survival Kit" and "Privacy Piracy" from Laguna Niguel, CA. I have brought copies of these for the committee to use.

My identity was stolen in 1996 by an imposter who paraded as an attorney, robbing me of my profession, my credit, and my piece of mind. She obtained over $50,000 using my name, after going online to obtain my credit report.

Your personal information, worth more than currency itself, can be used to apply for credit cards, mortgages, cell phones, insurance, utilities, products, and services, all without your knowledge.

A fraudster can do anything you can do, and worse than that, they can do things you would not do, like commit crimes and terrorist activities.

There are three motivations for identity theft. First is financial gain. An example: Robert is a high tech computer consultant who normally encrypts all his sensitive data on his computer.

Unfortunately, his resume was not stored in an encrypted file. He suspects that his impersonator accessed his computer through a network, copied his resume, and used it to obtain a well paying job. When Robert applied for the same job, he was shocked to find out that another person with his name and credentials was already hired.

The second reason is avoiding prosecution. Tom was laid off from a high paying job in the medical industry. He had great recommendations and felt sure that he would be re-hired. For 2 years, he was denied position after position, after each company had performed a background check.

Finally, Tom hired a private investigator that showed him that his criminal background included two DUIs and an arrest for murder, none of which belonged to him.

The third reason someone commits identity theft is revenge. The first cyber-stalking case prosecuted in Orange County, CA turned out to be identity theft. A computer expert was angry when a woman he liked shunned his advances. So he impersonated her in a chat room, stating that she had fantasies of being raped. When he gave out her phone number and address, several men appeared at her door.

There are many ways in which personal information can be obtained. According to the FTC, the Federal Trade Commission, 72 percent of victims have no idea how their information was accessed.

The new May 2003 California Public Research Study on Police and Identity Theft list the top sources of identity theft: mail theft, dumpster diving, unscrupulous employees, stolen or lost wallets, Internet fraud, burglary, friends, relations, phone scams, unethical

use of public documents, shoulder surfing, medical cards and drivers licenses, and personal information sold by financial institutions.

Since this hearing is focusing on the peer-to-peer file-sharing vulnerabilities and the potential of revealing sensitive information in our computers, I am going to give a few suggestions that are just lay person things.

No. 1, research any program before installing it. No. 2, learn how to safely stop sharing your files and how to unblock wanted files from entering your computer. Three, if possible, when using peer-to-peer file-sharing on the Internet, use a computer that does not store personal information on it.

Four, password protect and encrypt your sensitive files. Five, do not put any confidential information in your e-mail, unless they are encrypted. Next, be conscious about what information you share in your files at Web sites, in chat rooms, and in e-mail.

Read the privacy policies of the Web site you deal with and try and understand them. Make sure you have updated virus protection on your computers, and do not assume that you are anonymous.

Your confidential information is a valued commodity. Marketers, information brokers, and the financial industry, buy, transfer, and sell your aggregated profiles, including your income; credit-worthiness; buying, spending, and travel habits; health information, and much more.

Intimate facts about your life are shared legally and illegally without your knowledge or consent. The loss of control over our personal information has led to the epidemic of identity theft.

I applaud this committee for researching the perils posed by peer-to-peer file-sharing. It is important to acquire knowledge, security measures, and careful strategies to protect ourselves. Hopefully, divulging security flaws in peer-to-peer file-sharing and other technologies to the media and Congress will encourage companies to make user-friendly security a top priority.

But peer-to-peer file-sharing may pose less of a theft of identity theft than the careless display of records at your doctor's office, the negligently piled tax returns left on your accountant's desk for the cleaning crew to review, the encrypted and unlocked cabinets with personnel files at work, the non-shredded trash bins behind banks, insurance agencies, and mortgage companies, and the hack data bases of credit card companies, financial companies, and universities and the like.

To prevent identity theft, the burden should be on the credit granters who are in the unique position on the front end to take precautions and require verification of change of address, and refuse to issue to fraudsters.

Unfortunately, quick, easy credit, pre-approved offers convenience checks, mass marketing of data bases and sloppy information handling make this a simple crime.

I encourage this honorable committee to also investigate ways in which the financial industry and information brokers can better protect our security.

Since Congress passed the Financial Modernization Act in 1999, identity theft has skyrocketed. Whether on-line or offline, our sensitive information must be better protected to foster consumer trust, so that our economy and our society can flourish; thank you.

[The prepared statement of Ms. Frank follows:]

WRITTEN TESTIMONY
FOR THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
TOM DAVIS, CHAIRMAN (VIRGINIA)
HENRY WAXMAN, RANKING MINORITY MEMBER (CALIFORNIA)

INVESTIGATIVE HEARING ON PRIVACY AND SECURITY WITH REGARD TO PEER TO PEER FILE SHARING
HEARING DATE: MAY 15, 2003 10:00 A.M.
ROOM 2154
RAYBURN HOUSE OFFICE BUILDING
TESTIMONY PROVIDED BY MARI J. FRANK, ESQ.

Good morning, Chairman Davis, Ranking Member Waxman, honorable committee members, and invited guests. Thank you very much for the opportunity to address you today regarding privacy and security with reference to the possible vulnerabilities of computer users when engaged in peer to peer file sharing on the Internet. I am also very grateful that Congress is looking at the greater issue of identity theft to understand how it fits into the overall issue of privacy and security in our society.

My name is Mari Frank. I am an attorney, privacy and identity theft consultant, and author of The Identity Theft Survival Kit, (Porpoise Press) and co-author of Privacy Piracy (Office Depot) from Laguna Niguel, California. I serve as a Sheriff Reserve for the Orange County, California Sheriff Department's High Tech Crime Unit, and sit on the Advisory Committee to the Office of Privacy Protection in the State of California's Office of Consumer Affairs, which focuses on privacy and identity theft protection for California citizens. Additionally, I have served on the Los Angeles District Attorney's Office Task Force on Identity Theft, which sponsored legislation to help victims of identity theft, and assisted law enforcement in the prosecution of this crime. As an advisory board member to the non- profit consumer advocacy programs, the Privacy Rights Clearinghouse and the Identity Theft Resource Center (San Diego, Ca.), I am privileged to consult with Directors Beth Givens and Linda

Foley regarding identity theft cases, research, protection for consumers and companies, and proposals for legislation.

My own identity was stolen (in 1996) by an impostor who paraded as an attorney robbing me of my profession, my credit and my peace of mind. She obtained over $50,000 using my name, purchased a red convertible Mustang, and even caused me to be threatened with a lawsuit by a rental car company for the car that she leased and damaged in an accident. It took me almost a year to clear my records and regain my credit and my life. I later learned that while working as a secretary, my evil twin (who I never met) accessed my credit report with all my personal and financial information on-line from a subscription service. From that arduous nightmare, I gained great insight into the tribulations that victims endure. Since that time I have personally assisted myriad victims across the country. I have had the privilege of testifying before several legislative bodies and have advised many national corporations on how to protect their clients, customers, vendors, employees and their company from great challenges of identity theft.

First I am grateful to this honorable committee for focusing on the growing problem of privacy and security with regard to the Internet. Your desire to expose these issues and educate our citizens deserves commendation. I am also thankful to this esteemed panel of witnesses who will bring light on these problems and help to create solutions so that we may better protect our personal and confidential information while using file sharing and other technologies on the Internet.

You've asked that I concentrate my testimony in the following areas:

I. Provide you an overview of how your identity can be stolen through the acquisition of your personal information.

II. Document examples of identity theft cases which have occurred with the use of personal identifiers.

III. Suggest ways in which computer uses and ordinary citizens can protect themselves from the threat of identity theft, which may be posed by the vulnerabilities of peer-to-peer sharing and other Internet technologies.

I. HOW YOUR IDENTITY MAY BE STOLEN THROUGH THE ACQUISITION OF YOUR PERSONAL INFORMATION

In our data driven society your personal information is readily transferred across the nation in a nano-second through networks and on the Internet (whether or not you are a computer user). Your personal information, worth **more** than currency itself, can be used to apply for credit cards, credit lines, mortgages, cell phones, insurance, utilities, products and services etc. all without your knowledge. A fraudster can do ***anything*** you can do with your identifying information- and worse- even do things you ***wouldn't*** do such as commit crimes or engage in terrorist activities.

A. WHAT IS IDENTITY THEFT AND WHAT IS THE MOTIVATION?

\ Identity theft is the use of your personal identifying information such as your name, social security number, address, birth date, unique passwords, even biometric information, (usually the key to identity door is the social security number) to commit some type of fraud for one of the following benefits to the fraudster:

1. **Financial Gain**-This includes credit, loans, employment, health care, insurance, welfare, citizenship, other governmental and corporate benefits- and anything that has a dollar value. The fraud may take place in many jurisdictions, and purchases can be made by phone, fax, on-line or in person. Usually, the perpetrator can buy or "legally" obtain a driver's license, create checks on a computer with the victims' name, obtain or buy other identity documents including medical cards, credit cards, passports, etc.

2. **Avoiding Prosecution**- A criminal commits crimes in the real world or virtual electronic world, or terrorist acts using the name and identifying information of another person. Often the perpetrator also commits financial fraud as well to supplement her income.

3. Revenge - One can remain" invisible" by stealing an identity to hurt another person. This type of fraud may occur between ex-spouses, former business partners, ex-employees, disgruntled staff or angry customers. We also see this type of fraud committed in businesses where one business owner will want to ruin the reputation of another. This is tantamount to business identity theft.

B. HOW DOES THE FRAUD OCCUR?

Stealing your identity for financial gain is the most common motivation for a thief. The Federal Trade Commission's Report on Identity Theft (12/02) www.consumer.gov/idtheft) summarized the data received from consumers regarding identity theft complaints, They found that of all reported identity fraud complaints (279,134 in their data base as of 12/02), credit card fraud comprised 42%, utility fraud comprised 22%, bank fraud 17%, Employment fraud 9% Fraud loans 6% and government benefits 8%, Almost a quarter of the consumers complaining experienced more than one type of fraud. It's also important to note that many victims are not still not aware of the FTC's Clearinghouse. The clearinghouse was instituted as a result of the Identity Theft and Assumption Deterrence Act of 1998. I was privileged to testify at the Senate Hearing to support the bill establishing this act which also instituted identity theft as a crime against the consumer victim and set forth criminal penalties in 18 USC Section 1028 (a7) Although victims are starting to become more aware that the Federal Trade Commission provides helpful resources and takes complaints (toll free 877 ID Theft or www.consumer.gov/idtheft) through law enforcement and credit grantors referrals, many don't complete a complaint form. Some victims tell us that they know that the FTC cannot take their individual case, or personally assist them (other than to provide excellent resources like affidavits, referrals, steps to take), and they are reluctant to reveal more of their private information.

The scope and extent of the problem of identity theft and number of victims is still unclear, although the numbers are increasing. In 2002 the FTC received 162,000 complaints of actual victims. In 2001 Trans Union (one of the major credit reporting bureaus) reported 3500 calls a day to its fraud hotline (not all were victims, some had lost their wallet or were aware of a security breach and were potential victims). They also reported that they received 85,000 calls a month to their fraud hotline in 2001. The epidemic of identity theft is growing. Our experience and the research shown by the Government Accounting Office Reports (www.gao.gov) the FTC at www.consumer.gov/idtheft), the Privacy Rights Clearinghouse (www.privacyrights.org) and others is that most victims' information is acquired very easily. Most often the information is stolen **off-line**; however the data is quite often used on-line and by mail to apply for credit, services, and products. For the savvy impostor, the Internet and mail provide a safer refuge to commit fraud rather than face-to-face contact where one could be confronted and apprehended.

Because of the vast ways in which personal information can be obtained, it is critical to note that most victims (according to the Federal Trade Commissions 2002 Report-**72%**) have ***no idea*** how their information was accessed unless a wallet was stolen or lost or if a family member was the impostor. Most identity theft takes place without the knowledge and beyond the control of the victim. And many who fall prey don't find out for months or even years until they are denied credit or employment, threatened by collection companies, or arrested for a crime they didn't commit.

The newest May 2003 CALPIRG (California Pubic Interest Research Group) study "Policing Privacy: Law Enforcement's Response to Identity Theft" (see pages 10-12 www.calpirg.org/reports) lists the top common sources of identity theft:

(I have listed them for you from the study, but added my own comments explaining what they are)

1. **Mail Theft** --Pre-approved offers, convenience checks, documents from banks and financial and insurance institutions containing social security numbers, account

numbers and other critical data provide a goldmine for potential impersonators. (68% of law enforcement interviewed named mail theft as a top concern leading to identity theft)

2. **Dumpster Diving** Thieves search through garbage in offices, on the street, and at commercial locations for information. Several states including California now require commercial businesses to shred or completely destroy personal information prior to discarding it to protect customers. Consumers are advised to purchase home shredders and shredding software to protect themselves.

3. **Unscrupulous Employees** - Insiders with access to information off-line and on line have a "candy store" of opportunities to commit identity fraud. For example, we know of many instances of car salesmen, "dirty" employees working for credit reporting agencies, and realtors selling credit reports. There were instances of employees from the Social Security Administration selling social security numbers, bank employees using passwords to deplete customer funds, insiders stealing information from personnel and customer files to sell or use themselves to obtain credit and services. Pilfering can be accomplished through trash inspection, stealing hard copy documents or copying of files from a computer. A couple of years ago, in Detroit, several General Motors executives became victims of identity theft when a temporary employee obtained printouts of lists of personal information of the important staff. Another recent example is the theft by an ex-employee of a software company who used passwords previously accessible to him (and the company didn't change the passwords after he left) to obtain credit reports of customers of Ford Motor Credit. He sold the credit profiles of thousands of potential victims. Your credit profile –especially one for commercial vendors have all a fraudster needs to steal your identity.

4. **Stolen/lost wallets-** This source of information loss is one of the few ways in which consumers may trace the theft back to the source. Although not mentioned by the

Calpirg study, lost, stolen or never received credit cards, convenience checks and pre-approved offers are another great source for criminals to commit financial fraud.

5. **Internet Fraud** (and computer access fraud.) There are numerous types of fraud that can begin with the accessing of information from a computer whether or not the machine is networked or connected to the Internet. A stand-alone computer can be entered if there is no password protection and sensitive non-encrypted files can be copied or removed. Many computer users keep personal information including passwords and confidential financial documents on the computer with little protection. Of course, while on a network or internet- and especially with wireless connections, hackers can intrude and take what they find un-noticed. Also, fraudulent e-mails, fake websites copied to look like real trusted sites, can gather your information through deception. However many times information may be hacked through security holes in trusted software. The most current example is of this is the Microsoft "Passport" flaw exposed last week. The system problem allows an attacker to access vital confidential personal data passwords, credit card information, etc. Peer to Peer file sharing if used incorrectly or if corrupted can permit entry by unsavory file sharing characters to access sensitive files with personal information. We've all seen the news of entire personnel files, student profiles, and credit card customer files stolen by hackers creating privacy invasions and worse yet, identity theft. A recent example is the theft of several hundred thousand health records (including the Social Security numbers) of Veterans in Arizona. Recently VISA and MasterCard customer information was hacked from a company that processes credit card transactions and it is believed that several hundred thousand files were compromised. With these types of security breaches, computer users are powerless to do anything to protect themselves prior to the intrusion.

6. **Burglary- Theft** from houses, cars, businesses of hard copy documents, faxes, e-mails, computer files, etc. Data collected on a personal level would be billing statements, bank documents, loan applications, utility bills, investment reports, credit

card bills, insurance statements, and credit reports. Business records could be client and customer files and profiles, trade secrets, data bases, financial records, computer hard drives, etc.

7. **Friends, Relations-** Unfortunately, intimate friends and family have access to our personal information or places in which we keep that information. The elderly, ill or very young are most susceptible to caretaker abuse. The trusted individual may have access to check writing, credit cards, personal information, etc. This is especially tragic since a victim may not with to prosecute a family member, and therefore may be left with the financial burden of the fraud charges.

8. **Phone Scams:** Fraudsters induce victims to reveal personal information through pretext calling- pretending to be your bank, or a governmental agency in need of your personal information.

9. **Unethical Use of Public Documents** –Birth Certificates, Death Certificates, Marriage Licenses, etc. all are public records and easily attainable on the Internet through governmental agencies, on-line information brokers, or even in person. These documents display social security numbers and other personal identifiers including mother's maiden name. (California recently passed a law requiring that public records which contain the social security number be restricted (information redacted for public disclosure) except for use by "need to know" persons.

10. **Shoulder Surfing-** Potential imposters watch for vulnerable computer users, ATM and other machine users to ascertain passwords and other information to steal.

11. **Medical Cards** –Many insurance carriers still use the social security number as the key to the system. Other personal and confidential data is also readily available for use by prying eyes at pharmacies, doctor's offices, hospitals and clinics.

C. OTHER MEANS OF APPROPRIATION OF PERSONAL AND CONFIDENTIAL INFORMATION NOT REPORTED BY CALPIRG LAW ENFORCEMENT STUDY ABOVE:

1. **Government Data Sources Revealed-** There is still several governmental agencies both state and federal that requires the display of the social security number in plain view. This is true for military service and veteran health care. Several states still use the social security number as the Driver's license number, which must be shown for identification purposes, for travel on airplanes, when cashing checks, and in other public, matters. The social security number must be displayed on payroll checks in California and other states (a California bill is pending to eliminate this requirement). The State of California Peace Officers Standards Training for all police requires that the social security number be displayed and indicated for the peace officers to continue employment. Also many state colleges require that the social security number be the key identifier and be displayed for grades. There are pending bills in the California legislature to cure these problems.

2. **Personal Information Sold By Financial Institutions**

In GAO testimony of 4/14/02, regarding **Identity Theft: Available Data Indicate Growth in Prevalence and Cost**, the Director, and Justice Issues indicated:

"Another potential source of personal identifiers for identity thieves is the personal financial information sold by financial institutions to non- affiliate third parties" Under the Gramm-Leach-Bliley Act of 1997 (GLB), a financial institution can sell your private financial data unless you respond to their "opt out" privacy notices which must be sent annually which inform a consumer of the privacy polices of that institution. There is presently a state bill in California (and also a pending Ballot Initiative) that would require that financial institutions apply the "opt in" standard, which would allow customers to prohibit such disclosure without express prior permission.

3. **Stealing Information Regarding Internet Technologies Such As Peer File Sharing**

As you can see from the information above, your personal information can be stolen in a variety of ways-most of which are very easy, and don't even require any high tech instruments. In this data profiling society, our personal and business information is available everywhere! But this doesn't mean that we should ignore the vulnerabilities of peer-to-peer file sharing. The Internet and software programs that contain security flaws, or require a great deal of understanding to use effectively – pose a threat to non-techies who want to use the new technology. Unsophisticated users of P2P File sharing may be sharing much more than they intend to and unintentionally enable a "peer" to become an identity clone. Since most victims don't know how their information is stolen to commit identity theft, it is feasible that users of these technologies who accidentally share files that contain confidential and personal information- could be subjecting themselves to the potential identify theft. One of our witnesses today, Nathan S. Good wrote an article "Usability and Privacy: A Study of Kazaa P2P File Sharing"- This study is helpful in understanding that fatal mistakes by unaware users could allow someone to get into unencrypted files with sensitive information. If you keep passwords, credit card numbers, financial information, software programs with financial information for banking in un-encrypted files (or poorly encrypted files) and you haven't understood how to make certain that ***only*** your designated file for sharing is open to share, you are vulnerable to exposing your information. Just as in many other programs that enable you to network, bank on-line, share e-mails, purchase with "passports" or use other profiling software, there may be security flaws that invite a hacker to appropriate confidential files from your hard-drive. Hacker attacks and security breaches are well known to companies and governmental websites as well. You have little control over the security flaws, but you do have control over the steps you can take to protect yourself while using technology. Steps to minimize your risk will be addressed in the later section of the testimony.

II. DOCUMENTED EXAMPLES OF CASES OF IDENTITY THEFT USING PERSONAL INFORMATION

A. Examples of Financial Identity Theft:

1. *John is a recent widower. When his wife died of cancer at age 35,(leaving him with three young children, he began receiving collection calls from credit card companies, a computer manufacturer, and a cell phone company for the items and services allegedly purchased by his deceased wife* ***after*** *her funeral. He suspects that the imposter got the information from the death certificate which has the social security number and birth date on the document. This could have been obtained in the funeral home, from public records off line or on line, through the social security administration, from an Internet information broker, or any number of places.*

2. *Sidney, a wealthy retired executive learned that his identity was stolen many months after he and his wife purchased a new home. His loan application, with his 3 in one credit report attached, revealed his credit score, his checking, savings, and investment accounts, social security number, and all necessary information for an impostor to become Sidney. He believes his masquerader had gotten a copy of Sidney's loan application through his broker's laptop computer (which also had his downloaded credit report) and opened new credit card accounts, purchased computers, electronic equipment, furniture, rented an apartment, obtained utilities, etc, stealing almost $100,000.*

3. *Robert is a high tech computer consultant who normally encrypts all sensitive data on his computer. Unfortunately, his resume was not stored in an encrypted file. He suspects that somehow his impersonator accessed his computer through a network and copied his resume. The fraudster used the vitae as his own to obtain a well paying job with the government. When Robert applied for the same job- he was shocked to find out another person with his name and credentials was already hired- the agency thought he was the fraudster.*

B Examples of Criminal Identity Theft

1. *George, a disabled veteran living in Colorado was suddenly denied his disability payments, and hit with a large IRS bill for the income that his impostor had earned working under his name in Tennessee. Upon further investigation, we learned that George's impostor had also established a criminal record in yet another state and there was a warrant for George's arrest.*

2. *Debbie signed up for e-mail and Internet access with a reputable Internet Service Provider. She received e-mail from her provider asking her to give her personally identifying information, including her social security number, to renew her account, she later learned that she and many other people had responded to a false e-mail set up to look like her provider. Months later she received collection calls and when stopped for speeding one night she was nearly arrested for outstanding warrants issued in her name in another state.*

3. *Tom was laid off from a high paying job in the medical industry. He had great recommendations and felt sure he would be rehired. For two years he was denied*

position after position after each company had done a background check. Finally Tom hired a private investigator who showed him that his criminal background included 2 DUI's and an arrest for murder. None of which belonged to him. He learned that an on-line information broker continued selling this erroneous information even after he corrected it with the Sheriff.

C. Examples of Identity Theft for Revenge

1. *Dan was trying to get joint custody in divorce proceedings. His estranged wife somehow was able to access his e-mail accounts and passwords and send herself fraudulent e-mail messages from him threatening to harm her and kill the children.*

2. *The first cyber stalking case prosecuted in Orange County, California turned out to be identity theft. A computer expert was angry when a woman he liked shunned his advances. He proceeded to go online to a chatroom and pretend to be her- stating that she has fantasies of being raped. He gave out her telephone number and home address. The woman didn't even own a computer. When several men appeared at her door to share her fantasies, she was terrified and called the police.*

3. *The Sept 11, 2001 terrorists had opened 14 accounts at a Florida bank, using false social security numbers and other documents. They obtained credit cards, apartment units, leased cars, and fraudulently charged airline tickets. They not only did this for revenge against our country- but also they committed financial theft to avoid being caught or prosecuted.*

The above cases demonstrate how identity theft can take many forms. Often the victim can only guess how his information was obtained. The assaults against these victims caused great anguish and negatively impacted every aspect of their lives. The time spent trying to regain their lives, the damage to their reputation, and the out of pocket costs were minimal compared to the tremendous emotional turmoil these people endured. The purpose of showing you these examples is to help to understand why it is so important to educate our citizens, support law enforcement efforts, encourage best business practices with regard to Internet technologies, and pass laws which hold the financial industry accountable to verify and authenticate before issuing credit to possible identity thieves. (Please see S. 233 The Identity Theft Prevention Act of 2003).

III. WHAT COMPUTER USERS CAN AND CANNOT DO TO PROTECT THEMSELVES FROM IDENTITY THEFT WHEN USING PEER TO PEER FILE SHARING

What can computer users do to protect them while using these technologies and other Internet or Network programs? The Internet provides an opportunity for increased knowledge, entertainment, and global communication. At the same time it is provides a free forum for dangers including unsavory hackers, attackers, child molesters, and fraudsters. Since I am not a computer expert, but use my PC everyday for business, education, and communication, I can suggest what I as a specialist in identity theft to my friends and clients.

1 RESEARCH ANY PROGRAM BEFORE INSTALLING IT. As my own computer consultant warns me daily, before you put a new program on your computer, find out everything about the program that you can, and learn what risks there are in using it. Take every precaution that the program advises. And if you aren't highly technical, get some help in deciding whether to even use a program at all. If you decide to use a program, look first to the security and privacy actions to take. This applies to all software you purchase or download.

2. LEARN HOW TO SAFELY STOP SHARING YOUR FILES AND HOW TO BLOCK UNWANTED FILES FROM ENTERING YOUR COMPUTER. If you aren't sure what you are doing get on the website of the software company and get some technical support either by e-mail or by phone to help you correct any miss-configurations you have made. Also have them double check that you have made the right choices. When downloading- don't designate more than one folder for file sharing, and check to see in "tools" if you have inadvertently checked more than one file- if so – immediately unselect the files you don't want to share. If you have problems, delete the program until you know how to limit the shared folders.

3. IF POSSIBLE, WHEN USING PEER-TO-PEER FILE SHARING AND THE INTERNET, USE A COMPUTER THAT DOESN'T STORE SENSITIVE INFORMATION ON IT. This may not be feasible because of the costs. But some companies and individuals have a separate computer for Internet use.

4. PASSWORD PROTECT AND ENCRYPT YOUR SENSITIVE FILES, Make sure that you are carefully protecting information that could be used to steal your identity. Don't tell anyone your passwords and change them from time to time- especially when an employee who had access, leaves your business. Also don't store passwords on your computer.

5. DON'T PUT ANY CONFIDENTIAL INFORMATION IN YOUR E-MAILS UNLESS THEY ARE ENCRYPTED. This is important whether you file share or not. E-mail is like a postcard. Your e-mails at work are not confidential and may be reviewed by your employer. There is no expectation of privacy for e-mails.

6. BE CONSCIOUS ABOUT WHAT INFORMATION YOU SHARE IN YOUR FILES, AT WEBSITES, IN CHAT ROOMS AND IN E-MAIL. Just because you're asked to share information, doesn't mean it is safe. Consider what could be done with the information you disseminate, and then reconsider.

7. READ THE PRIVACY POLICIES OF THE WEBSITES YOU DEAL WITH. If they share your information for marketing purposes, think twice about providing it, since it can be aggregated and sold and used to profile you. Someone getting that information may become your identity clone.

8. MAKE SURE YOU HAVE VIRUS PROTECTION ON YOUR COMPUTERS. Update it often.

9. DON'T ASSUME THAT YOU ARE ANONYMOUS. Remember there is online tracking and monitoring when you use the Internet. Install reputable spy wear and find out about other security measures to take.

10. USE A HARDWARE FIREWALL WHENEVER POSSIBLE. Be especially careful if you have a wireless connection to set up firewalls otherwise you are opening up your entire system to strangers and all your files can be accessed.

For more tips and security suggestions about protecting your privacy and identity on-line see **Fact Sheet 18: Online Privacy at the Privacy Rights Clearinghouse** at www.privacyrights.org. Also visit the Electronic Privacy Information Center at www.epic.org. There are additional resources listed on both websites to educate the novice as well as the most seasoned computer guru.

OTHER IDENTITY THEFT PROTECTIONS MEASURES:

Here are the top four protection measures we suggest:

1. Get a copy of your credit reports at least twice a year. Carefully scrutinize all information and correct all errors, including the inquiries. If something looks strange, call and write to the creditor and place fraud alerts on the credit profiles of the three major credit reporting agencies. If you monitor your reports and fraud accounts are opened, at least you will minimize your losses with early notification. Does your own background search on yourself once a year to see if any fraudulent criminal activity appears?

2. Don't give out your social security number unless required by law. Don't carry it with you and if it is on your health care cards, make a copy redacting the first 5 numbers and carry only the copy with you. Carry as little information about you as possible in your wallet. Don't submit to the use of your biometric information (fingerprint, iris scan, etc) unless required by law and you understand the purpose for which it is collected, how it will be maintained, the secondary use if any, the safeguards ensuring its accuracy and security and the place to contact if a problem arises.

3. Guard your personal information with great caution. Don't give out information at retail stores, on warranty cards, when a company *calls you* on the phone, or on the Internet. Don't keep personal information on your computer if it is accessible on the Internet. Shred all documents that you are discarding, including utility bills, check statements, old wills and trusts, ***anything*** with personal and financial information.

4. When dealing with others in a trusted position, such as a caregiver, or a trusted advisor, make sure you check references, licenses, and other background information. Share as little personal and financial data with this person as possible, and don't give them responsibility to

manage your assets without your approval- don't give out your ATM VISA pin number or allow them to sign checks for you. The less access to your financial and personal data the more secure your identity.

THE MYTH OF PREVENTION OF IDENTITY THEFT

This testimony described many ways that your information could be accessed and used for financial gain or a criminal purpose without your knowledge or control. When I became a victim, my impostor had accessed my credit report from a law office subscription service with a re-seller of credit profiles. She pretended to be a private detective declaring under penalty of perjury that she had a permissible purpose to obtain my credit report. I had no way to prevent this crime from happening, since the information was not within my control. The majority of victims cannot prevent this crime. Therefore, offering computer tips and offline suggestions on how to ***"avoid"*** identity theft would be misleading. Although we may educate ourselves as to vulnerabilities of the Internet and Peer-to-Peer File Sharing, and protect our information off line as well, if someone wishes to steal our identity, the information they need is within their reach in many places and it will un-avoidable. If you are victimized by identity theft go to www.identitytheft.org; www.consumer.gov/idtheft www.privacyrights.org and www.idtheftcenter.org for many pages of free information to help you deal with the ordeal of regaining your identity.

As computer users and concerned citizens, we must educate ourselves, research and understand the programs and technologies we use, and guard our information as best as possible, I urge this committee to take notice that we should **not** give any false sense of security to anyone with regard preventing identity theft. We cannot guarantee anyone that if they don't use Peer-to-Peer File Sharing, they will be safe from identity theft. No matter where a criminal gets your information, it can only be used for financial gain if the creditors and other businesses are not cautious about verifying and authenticating your identity.

For that reason, I have listed below suggested steps that should be taken by governmental and commercial entities to prevent financial identity theft.

IV. PROPOSED ACTIONS TO PREVENT IDENTITY THEFT

1. **Both governmental entities and private industry should limit the use of the social security number since it is the key to identity theft for financial fraud.**

As a member of the advisory committee in the Office of Privacy Protection in the California Office of Consumer Affairs, I had the privilege of assisting in the development of the recently issued " **Recommended Practices for Protecting the Confidentiality of Social Security Numbers"** (July 25, 2002 www.privacy.ca.gov). This document should be considered by both pubic and private sector entities to protect all consumers.

2. **Destruction of Confidential Information-**Governmental Agencies and Private Industry should be required to completely destroy personal information that they are discarding by

shredding, burning or whatever means is necessary to protect the information from dumpster diving.

3. **Governmental and Private industry should be required to truncate credit card numbers** – No company or entity shall print more than the last 5 digits of a credit card number or account number or the expiration date upon any receipt provided to a cardholder.

4. **Security Breach Notification** Governmental Agencies and Private industry should be held accountable to timely notify all employees and or clients or customers of computer security breaches which have exposed their personal identifying information.

5. **Departments of Motor Vehicle Licensing-** Bureaus should establish more stringent monitoring and matching of duplicate licensing and new licenses. A photo ID and a fingerprint could be matched. Rather than developing a "national ID" with various forms of biometric information, credit cards and other unnecessary information which would complicate the process, this national driver's license would have a national data base to help deter interstate identity theft.

6. **Law enforcement agencies** should be required to take a report in the jurisdiction where the identity theft victim lives. Such report should enable the victim to list the fraudulent accounts so that this report could be sent to the credit reporting agencies to comply with their policy of blocking the fraud accounts upon receipt of a valid law enforcement report.

7 **Law enforcement agencies** should be provided funding for task forces in all major metropolitan areas to include the Secret Service, the Postal Inspector, the Social Security Inspector, the FBI, INS, State Attorney General and local law enforcement to collaborate in the investigation and prosecution of these crimes.

8. **Local law enforcement agencies** in conjunction with the judicial system should assist victims of criminal identity theft in other jurisdictions within a nation wide coordinated system. So a victim of criminal identity theft in California whose impostor is in New York could be declared innocent in New York as well as California. This would entail a national database of the criminal information and fingerprints. It would contain the order of the true person's fingerprints for comparison with the fingerprints of the impostor-criminal in New York. The court would enter a declaration of factual innocence and any warrants for the victim would be dismissed. All databases would be corrected so that background checks would not show the victim as having an arrest or criminal record.

9. **Increase penalties for repeat identity theft perpetrators or for "aggravated identity theft" and for those who commit identity theft for the purpose of committing terrorism.**

10. **Set up State and Federal Offices for Privacy Protection-** There should be a federal office of privacy protection as well as state offices. The office of privacy protection should

institute an ombudsmen office to assist the elderly and limited English speakers to resolve identity theft problems.

10. Credit Reporting Agencies:

a. Since most victims do not have notice of the identity theft until they re-finance, apply for a loan, or are contacted by a creditor, the statute of limitations to file a law suit against a credit reporting agency should begin within 2 years of the date at which they ***discover*** or should have known of the fraud.

b. To assist in the monitoring of credit reports, consumers should be entitled to a free credit report at least once a year in every state.

c. Credit reporting agencies should provide to consumers, upon request, an exact copy of the credit reports that vendors and creditors receive since often they are different and the consumer credit report often shows different account information, which causes difficulties for victims in clearing their credit.

d. Consumers should be able to put a complete freeze on their credit reports in order to prevent identity theft. This would enable the consumer to prevent their credit report from being accessed by a creditor without the specific authorization of release. It would be impossible for an impostor to apply for credit if there were a freeze on the file. The consumer would have the right to release the file when he so desires by a password or pin number. This type of legislation recently became law in California.

e. Credit reporting agencies should be required by law to block all fraud including the fraudulent inquiries upon the receipt of a valid law enforcement report (local police, DMV investigators, Secret Service) listing the fraud accounts. The burden then shifts to the creditors to prove that the accounts are not fraudulent. This is presently law in California and should be codified nationwide. Under this scenario the victim of fraud is innocent until proven guilty instead of having the burden of proving innocence.

f. Credit reporting agencies should provide names, addresses and phone numbers of the companies who accessed the consumer's credit report – (inquiries) with the issuance of a consumer report so that potential victims could verify the permissible purpose.

g. Credit reporting agencies should notify a consumer by e-mail or First Class mail when his/her credit report has been accessed. The agency should be allowed to charge a reasonable fee for this service.

h. To provide better enforcement, the Fair Credit Reporting act should be amended to allow for class action lawsuits for violations of the act by creditors and credit reporting agencies.

I. Credit reporting agencies should set up hotlines with live persons to talk to regarding identity theft. The same employee in the fraud department should be assigned to a particular victim.

j. Since many states are providing more privacy safeguards and better identity theft protection for their citizens than federal laws provide under the Fair Credit Reporting Act, the sunset provisions of federal pre-emption should not be re-instated. Several states like California have influenced other states and the federal government to more carefully guards our confidential information from the identity impostors.

11. Banks and other Creditors should be held accountable for protecting consumers and others from identity theft.

a. The fraudsters' most critical need in committing identity theft is to change the victim's address to the impostor's address or mail drop. Creditors either extending credit to a new account or upon being asked to change the address on the account is required to verify the address change if it is different from the address on its records or the address on the credit report. The creditor should be required to send a notification and confirmation to the former as well as the new address. Also if the creditor receives a request for an additional card it should notify the primary cardholder.

b. Creditor's who issue credit to an impostor after a fraud alert is placed on a credit profile, should be held liable and assessed a fixed penalty of at least $1000 per occurrence or actual damages which ever is greater.

c. Upon receiving notification of fraud by a victim of identity theft, a creditor should be required within 15 days to provide copies of all billing statements, applications and other correspondence to the victim. The victim may be required to pay reasonable copying costs.

d. Credit grantors should compare and match with the credit report for verification purposes, at least four pieces of personal information that would identify a consumer applying for credit.

e. Credit grantors should utilize their financial discrimination programs to identify changes in spending habits so they could intervene early and notify consumers of possible fraudulent activity before it gets out of hand.

f. Creditors should not be allowed to send "convenience checks" without a request by the consumer.

g. Credit grantors should not be allowed to send pre-approved offers of credit without the request of the consumer.

12. Regulation of Information Brokers

a. Information brokers should be subject to the Fair Credit Reporting Act as defined by statute so as not to shirk their duty to maintain accurate records.

b. Employers or others who order background checks on a consumer should be required to provide a copy to the consumer upon receipt whether or not the consumer report was used to hire a prospective employee or any other purpose.

Privacy, Security, and Identity Theft Conclusions

Personal, confidential, and financial information is a valued commodity in our society. Marketers and the financial industry buy transfer and sell your aggregated personal profiles which include your income, credit worthiness, buying, spending, traveling habits, heath information, age, gender, race, etc. Facts about our personal and financial lives are shared legally and illegally without our knowledge or consent – on-line and off-line everyday. Privacy protection in the age of data collection is really about limiting access to our records, rather than keeping the information secret. . The only power you have is to educate yourself as to your risks and to the potential dangers of privacy and security invasions. This loss of control over the dissemination of your information has led to the epidemic of identity theft. It's wise to research the perils posed by the Internet, Peer to Peer File Sharing and similar technologies and arm yourself with knowledge, security measures and careful strategies. It's important to expose security flaws in software to the media and Congress, so that companies will make security a top priority and make their programs easier to use. But all this will not stop a fraudster who steals your information from a source outside of your control such as your doctor's patient files, or your accountant's fax machine, your HR department's computer at work, or from the trash behind your bank or insurance company.

To avert ***financial*** identity theft, the burden must be on the creditors who are in the unique position on the front end, to take precautions, require verification, and refuse to issue the credit card or loan to a fraudster. The financial industry has the power prevent a potential identity theft ***before*** the impostor can establish a parallel "shadow credit profile". To limit criminal identity theft, law enforcement has the power to protect potential victims. When a perpetrator is apprehended and gives a victim's name, his fingerprints and mug shot should always be taken, and the information should be stored securely for viewing, in a safe centralized, national law enforcement data base. That way, if a victim learns of a warrant for his arrest in another state, his photo and finger prints can be compared with those of the impersonator in his own state, and his name can be cleared effectively and expeditiously. With a greater emphasis on precluding the facilitation of this crime at its inception-*before* the credit is wrongly issued, there will be a greater trust in law enforcement's abilities to reduce fraud, and the financial industry's commitment to protect its customers.

Thank you for the opportunity to share these concerns and suggestions with this Honorable Committee.

Mari J. Frank, Esq.

Attorney, Mediator, Privacy Consultant
28202 Cabot Road, Suite 215
Laguna Niguel, California 92677
Phone: 949-364-1511
Fax: 949-363-7561
E-mail: contact@identitytheft.org or Mari@MariFrank.com
www.identitytheft.org
www.MariFrank.com

Chairman TOM DAVIS. Thank you very much.

Mr. Farnan.

STATEMENT OF JAMES E. FARNAN, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, ACCOMPANIED BY DAN LARKIN, SUPERVISORY SPECIAL AGENT, FEDERAL BUREAU OF INVESTIGATION

Mr. FARNAN. Good morning, I would like to thank Chairman Davis, Ranking Member Waxman and members of the committee for the opportunity to testify today.

We welcome your committee's leadership in dealing with the serious security and privacy issues associated with identity theft and peer-to-peer sharing.

My testimony today will address the activities of the FBI's Cyber Division, in relation to the Internet and identity theft.

I have asked Supervisory Special Agent, Dan Larkin, Chief of our Internet Fraud Complaint Center to attend, and he will provide specific answers, should the committee have any questions about more technical matters with the Internet Fraud Complaint Center's role in this area.

A May 8th cover story in the Washington Post is nothing new to Americans today. Another group was discovered in possession of a veritable factory of counterfeit credit cards, including newly made cards, credit card numbers downloaded from a major retail store, and 600 pages containing more than 40,000 alleged stolen names and credit card numbers.

As the investigation continues, we will probably find that these criminals have affected the lives of hundreds of victims, perhaps destroying their credit and creating hardships that will take years to abate.

These thefts could be the result of computer hacking, insider theft, and/or social engineering. Stolen information can also be sold and used to establish new identifies for fugitives or terrorists. In these cases, identity theft can have much more serious consequences.

Identity theft is the fraudulent use of individual's personal identifying information. It is normally a component or end result of another crime. Victims of identity theft often do not realize that someone has stolen their identity until their credit has been ruined.

Although we have received no complaints alleging identity theft by peer-to-peer to networks, some factors must be considered.

Peer-to-peer networks primarily serve as a "come and get it" resource on the Internet. In using such a utility, the user specifically searches for the item they want; for example, music, images, or software.

The most significant criminal activity involving peer-to-peer sharing centers largely on music and software privacy, an area in which the FBI has been working closely with the private industry.

The FBI has also seen an increase in peer-to-peer sharing of child pornography files. Peer-to-peer networks are increasingly being identified as sources from which Trojans or back doors were installed on computers during downloads.

Victims sometimes discovered that personal and financial information have been removed from their computer through the back door. It is becoming more common for "bots" or active Trojans to be installed during a peer-to-peer download.

In these instances, the victim computer executes instructions from the "bots" creator. Active "bots" could also be used to retrieve sensitive information from victim computers in furtherance of identity theft schemes. A person using peer-to-peer utilities for unauthorized or illegal purposes is not as likely to tell the FBI that a back door was found on their system, or that as a result, certain personal or financial information may have been taken.

Through the Internet Fraud Complaint Center [IFCC], the FBI has positioned itself at the gateway of incoming intelligence regarding a wide variety of cyber crime matters. The IFCC received 75,000 complaints in 2002, and is now receiving more than 9,000 complaints each month.

We expect that number to increase significantly, as the American and international communities become more aware of our mission and capabilities.

Later this year, the IFCC will be renamed as the Internet Crime Complaint Center, to more accurately reflect its mission. The center receives complaints about various Internet-based crimes, analyzes the complaints for common patterns and perpetrators, and then sends them the appropriate agency for investigation and prosecution.

In summary, cyber crime continues to grow at an alarming rate, and identity theft is a major part of the increase. Criminals are only beginning to explore the potential of crime via peer-to-peer networks.

The FBI is grateful for the efforts of your committee and others dedicated to the safety and security of our Nation's families and businesses. The FBI will continue to work with your committee and aggressively pursue cyber criminals as we strive to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak to you today, and on behalf of the FBI, I look forward to working with you on this very important topic; thank you.

[The prepared statement of Mr. Farnan follows:]

Testimony of James E. Farnan,
Deputy Assistant Director,
Cyber Division,
Federal Bureau of Investigation,
before the
House Committee on Government Reform
May 15, 2003

Thank you for inviting me here today to testify in this hearing at which the Committee is examining privacy and security issues associated with the use of peer-to-peer file sharing programs. This hearing and the Committee's Web page, in which you provide a link to: "Parental Tips for Internet File-Sharing Programs," demonstrate your commitment to improving the abilities of our Nation's families and businesses to be safe, secure, and crime-free while using the Internet as a tool for research, entertainment and commerce. Our work here is vitally important because Internet use grows each day, and each day there are thousands of new victims. My testimony today will address the activities of the FBI's Cyber Division as they relate to a broad spectrum of criminal acts involving identity theft, fraud, information security and computer intrusions.

A May 8th cover story in the Washington Post is nothing new to Americans today. Another gang of thieves was discovered in possession of a "veritable factory for counterfeit credit cards," including "600 pages containing more than 40,000 allegedly stolen names and credit card numbers; more than 100 newly minted cards under 100

different names, featuring the trademark Visa logo." The police also found "stacks of plastic cards, software to create identity cards, laptop computers, machinery to encode magnetic strips, and a 'skimmer' that captures a facsimile of credit card information and stores it...(and) 16-digit credit card numbers, with their expiration dates, that had been downloaded from one major retail store in the area." As the investigation continues, we will probably find that these criminals have affected the lives of hundreds of victims, perhaps destroying their credit ratings and creating hardships that will take years to abate. These thefts could be the result of computer hacking, insider theft and/or social engineering. The FBI treats each of these techniques as criminal acts, and we continue to seek out those who would use them to illegally enrich themselves. Stolen information can also be sold and used to establish new identities for fugitives or terrorists. In these cases, identity theft can have much more serious consequences.

The Federal Trade Commission's annual report lists identity theft as it's most substantial category of reported crime, at 43% of the total. Its impact on citizens and businesses both domestically and abroad, as well as the growing number of ways that such schemes can be initiated or advanced, primarily through the Internet, is a priority interest for the FBI. An understanding of the scope of the problem can only be gained by identifying the variety of acts related to identity theft, including insider theft, hacking, spam, spoofing, account hijacking, auction fraud and peer to peer (P2P) sharing. Below are some examples and definitions:

Identity Theft

Identity theft is the fraudulent use of an individual's personal identifying information, such as a social security number, mother's maiden name, date of birth or bank account number. Identity theft includes alias identity crimes in which an individual's true identity is completely fabricated and not identified with a real person, whether living or deceased. Identity theft is normally a preliminary step toward committing other crimes. Some will engage in identity theft for financial gain, others to avoid arrest or detection, attain legal immigrations status, or obtain government benefits. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill. Identity theft can be a component of many crimes, including bank fraud, telemarketing fraud, Ponzi schemes, credit card fraud, bankruptcy fraud, money laundering, insurance fraud, cyber crimes and unlawful flight to avoid prosecution (fugitives). The FBI's Criminal Investigative Division has recently begun to track identity theft as a component of other criminal activities. Their efforts will statistically measure the increase in crimes involving identity theft.

Spam

Spam generally refers to unsolicited incoming messages inviting an individual to

buy, sell, invest or join a certain club. Significantly, The Internet Fraud Complaint Center (IFCC) is seeing more and more spam referrals in which individuals are being directed to provide certain personal, including financial and password information, to remedy a credit problem, update their account information, or to avoid being part of an undesirable mailing list.

Spoofing

In one investigation, subjects collected individual e-mail addresses from Internet chat rooms and other Internet sources. The subjects then sent e-mail to individuals requesting credit card and personal information. The e-mail appeared to be from the victims' Internet service provider (ISP) (spoofed e-mail) claiming that the victims needed to provide current billing information. Victims would respond and provide their credit card and personal information, believing the information was going to their ISP. The subjects used credit card and personal information to obtain cash advances and purchase items utilizing the Internet.

In another investigation, subjects established a spoofed web-site, which was made to appear to be a U.S financial institution. This site was used to lure victims into providing personal financial information, including credit card and debit card numbers, which were than transmitted abroad to criminals who used the stolen cards at automatic teller machines throughout Europe.

Auction Fraud and Account Hijacking

Over the past year, the IFCC has received many complaints regarding auction sites wherein a customer's account was hijacked. In such cases the perpetrator gains unauthorized access (via computer intrusion) to customer accounts, determines which accounts have a good reference/feedback history, and represent themselves as that individual, selling merchandise, which is ultimately never delivered. Losses in such schemes range from hundreds of dollars to upwards of $100K with numerous victims. These types of schemes can also result in identity theft when unsuspecting customers provide credit card information to the criminal.

Computer Intrusion/Hacking

Computer intrusions are a different category from most fraud schemes. Many intrusions are never reported because companies fear a loss of business from reduced consumer confidence in their security measures or from a fear of lawsuits. Most of the outsider-intrusions cases opened today are the result of a failure to patch a known vulnerability for which a patch has been issued. Theft of consumer information from a computer system can only be facilitated two ways: by insiders or by outside hackers. Insiders have various motivations, including retribution and money. Outsiders are usually motivated by challenge and/or greed.

The IFCC recently received a referral through its website, in which the computer system of a small business that sold certain pharmaceutical products online was compromised by a hacker, who acquired credit card numbers, and the names and addresses of approximately 200 customers. This information was then posted on an Internet message board, where access to this personal data could be gained by anyone with an computer and an Internet account.

The FBI has seen a steady increase in computer intrusion/hacking cases. With the proliferation of "turn key" ("turn key" in that no special knowledge is needed to apply the tool - you only need to download the tool and apply it) hacking tools/utilities available on the Internet, this trend is not surprising. In many cases, computer intrusion incidents may represent the front end of a criminal matter, where credit card fraud, economic espionage, and/or identity theft represent the final result, and the intended purpose of the scheme. In some cases, a computer intrusion may also have been for the purpose of installing a Trojan, or back door that the hacker can later access. The hacker may want to launch a denial of service (DOS) attack, or to access personal financial, or other sensitive data contained on that system.

P2P Sharing

P2P networks primarily serve as a "come and get it" resource on the Internet. In

using such a utility, the user specifically searches for the item they want, e.g. music, images, or software. The most significant criminal activity involving P2P sharing centers largely on intellectual property rights (music and software piracy) matters, an area in which the FBI has been working closely with private industry. The FBI has also seen an increase in P2P sharing of child pornography files.

Although no instances of identity theft have been reported to be associated with P2P networks, there are several dynamics that should also be considered:

The FBI has seen an increasing number of instances where a victim has determined that a Trojan/back door was installed on their computer during a download from a P2P network. In some cases, the victim also learned that personal, financial information had also been removed from their computer via the back door.

In addition to traditional Trojans/back doors, The FBI has seen an increase in matters where certain "bots" (active Trojans) have been installed inadvertently via a P2P download. In these instances, the victim computer, via the bot, essentially reports to a designated Internet relay chat (IRC) site, awaiting further instructions from its creator. The creator of the bot will often use the compromised computers to launch coordinated denial of service attacks against a targeted site or sites. These bots could also be used to retrieve sensitive information from victim computers in furtherance of an identity theft scheme.

A person using P2P utilities for unauthorized or illegal purposes is not as likely to tell the FBI that an exploit (back door) was found on their system, or that as a result, certain personal or financial information may have been taken. The FBI has been made aware of instances where Trojans or bots have been found on computer systems where P2P programs are present, and where certain personal, financial or other sensitive information has been taken.

The FBI is in a unique position to respond to most cyber crimes, because it is the only Federal agency that has the statutory authority, expertise, and ability to combine the counterterrorism, counterintelligence, and criminal resources needed to effectively neutralize, mitigate, and disrupt illegal computer-supported operations.

The FBI's Cyber Division

The FBI's reorganization of the last two years included the goal of making our cyber investigative resources more effective. In July 2002, the reorganization resulted in the creation of the FBI's Cyber Division. In prioritizing Cyber Crime, the FBI recognizes that all types of on-line crime are on the rise.

The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the

United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are focused on cyber related matters.

At the Cyber Division we are taking a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, on-line identity theft, Internet child pornography, theft of trade secrets, and other similar crimes. The other, non-traditional approach consists of Internet-facilitated activity that did not exist prior to the establishment of computers, networks, and the World Wide Web. This encompasses "cyber terrorism," terrorist threats, foreign intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data via the Internet. The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise.

The mission of the Cyber Division is to: (1) coordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist

organizations, foreign government sponsored intelligence operations, or criminal activity and for which the use of such systems is essential to that activity; (2) form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities, and (3) place the FBI at the forefront of cyber investigations through awareness and exploitation of emerging technology.

To support this mission we are dramatically increasing our cyber training program and international investigative efforts. Consequently, specialized units are now being created at FBI Headquarters to provide training not only to the 60 FBI cyber squads, but also to the other agencies participating in existing or new cyber-related task forces in which the FBI is a participant. This training will largely be provided to investigators in the field. A number of courses will be provided at the FBI Academy at Quantico.

The importance of partnerships like law enforcement cyber task forces and alliances with industry can not be overstated. Those partnerships help develop early awareness of, and a coordinated, proactive response to, the crime problem. The cyber crime problem is constantly changing, requiring law enforcement to develop a flexible and dynamically evolving approach as well. Critical infrastructures and e-commerce are truly on the "front lines" and most often better positioned to identify new trends in cyber crime. Similarly, because of the actual and potential economic impact of cyber

criminals, private industry has a vested interest in working with law enforcement to effectively detect, deter and investigate such activity.

The Cyber Division is also embarking on a significant effort to improve our overseas investigative capabilities. We will be training more foreign police officers, and sending FBI personnel throughout the world to help investigate cyber crimes when invited or allowed by a host country. We believe this dramatic increase in high tech training and overseas investigations is justified by the increasing internationalization of on-line crime and terrorist threats.

Through the Internet Fraud Complaint Center (IFCC), established in 1999 in partnership with the National White Collar Crime Center (NW3C), the FBI has appropriately positioned itself at the gateway of incoming intelligence regarding cyber crime matters. The IFCC receives complaints regarding a vast array of cyber crime matters, including: computer intrusions, identity theft, economic espionage, credit card fraud, child pornography, on-line extortion and a growing list of internationally spawned Internet fraud matters. The IFCC received 75,000 complaints in 2002, and is now receiving more than 9000 complaints per month. We expect that number to increase significantly as the American and international communities become more aware of our mission and capabilities. Later this year, the IFCC will be renamed as the Internet Crime Complaint Center (IC3) to more accurately reflect its mission.

If the IFCC received an intrusion report from a company in Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis, while the intruder is routing attacks through Internet providers in California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime Task Force would be assigned the lead on the case. The leads could start in California, but end up in Eastern Europe, Nigeria or even back to Birmingham, if an insider was involved. One of the FBI's Computer Analysis Response Teams (CART) would be called upon to preserve computer forensic evidence, and that evidence could be forwarded to one of our new Regional Crime Forensic Labs, now located in Chicago, Dallas and San Diego. The Lab would determine the extent and duration of the intrusion, and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case can be cracked in a few days or take years. It is important to note again that an intrusion may only be the first indication of another crime. An intrusion could finally result in anything from identity theft, terrorism, or espionage. Cases are routinely complex, and often involve international connections. The following cases serve as examples of typical cyber crimes:

Raymond Torricelli, aka "rolex"

Raymond Torricelli, aka "rolex," the head of a hacker group known as "#conflict," was convicted for, among other things, breaking into two

computers owned and maintained by the National Aeronautics and Space Administration's Jet Propulsion Laboratory ("JPL"), located in Pasadena, California, and using one of those computers to host an Internet chat-room devoted to hacking.

Torricelli admitted that, in 1998, he was a computer hacker, and a member of a hacking organization known as "#conflict." Torricelli admitted that he used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion. Once such computers were located, Torricelli's computer obtained unauthorized access to the computers by uploading a program known as "rootkit." The file, "rootkit," is a program which, when run on computer, allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer.

One of the computers Torricelli accessed was used by NASA to perform satellite design and mission analysis concerning future space missions, another was used by JPL's Communications Ground Systems Section as an e-mail and internal web server. After gaining this unauthorized access to computers and loading "rootkit," Torricelli, under his alias "rolex," used many of the computers to host chat-room

discussions.

Torricelli admitted that, in these discussions, he invited other chat participants to visit a website which enabled them to view pornographic images and that he earned 18 cents for each visit a person made to that website. Torricelli earned approximately $300-400 from per week from this activity. Torricelli also pled guilty to intercepting user names and passwords traversing the computer networks of a computer owned by San Jose State University. In addition, Torricelli pled guilty to possession of stolen passwords and user names which he used to gain free Internet access, or to gain unauthorized access to still more computers. Torricelli admitted that when he obtained passwords which were encrypted, he would use a password cracking program known as"John-the-Ripper" to decrypt the passwords. He also pled guilty to possessing stolen credit card numbers that he obtained from other individuals and stored on his computer. Torricelli admitted that he used one such credit card number to purchase long distance telephone service.

Much of the evidence obtained against Torricelli was obtained through a search of his personal computer. In addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which Torricelli and members of

"#conflict" discussed, among other things, (1) breaking into other computers; (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases; and (3) using their computers to electronically alter the results of the annual MTV Movie Awards. This case illustrates the wide variety of criminal acts which can result from security vulnerabilities.

Raphael Gray, aka "Curador"

On March 1, 2000, a computer hacker using the name "Curador" compromised several e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and stole as many as 28,000 credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites.. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of "Curador," Raphael Gray. Mr. Gray, age 18, was arrested and charged in the UK along with a co-conspirator under the UK's Computer Misuse Act of 1990. This case illustrates the benefits of law enforcement and private industry around the world working together in partnership on computer crime investigations.

Cyber crime continues to grow at an alarming rate, and identity theft is a major part of the increase. Criminals are only beginning to explore the potential of crime via peer-to-peer networks while they continue to steal information by hacking, insider exploitation and social engineering. The FBI is grateful for the efforts of your Committee and others dedicated to the safety and security of our Nation's families and businesses. The FBI will continue to work with your Committee and aggressively pursue cyber criminals as we strive to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak to you today and on behalf of the FBI look forward to working with you on this very important topic.

Chairman TOM DAVIS. Thank you very much. I thank all of you for your input into this. Let me just ask a general question of the panel. The testimony, I think, makes it clear that users of file-sharing programs can expose their most personal files to millions of strangers, many times without the knowledge of the person using the files.

Is there general agreement among the witnesses that file-sharing programs can be confusing to configure, and that most people are unaware that they might be sharing their tax returns, credit card data and other confidential files on these networks? Is there a consensus on that?

Mr. FARNAN. I think so, yes.

Mr. DAVIDSON. I would just say that your mileage may vary, in the sense that different programs do have different capabilities or different defaults. So I think on the one hand, people should not get the feeling that if they use one of these things, they are automatically sharing everything on their hard drive. But the flip side of it is, I think the usability studies have shown that a lot of them could do a lot better job.

Mr. BROES. Also, software companies across the board have taken this secure by default initiative, where the applications, when they install it, it is secure. In the past, not even Microsoft had done that.

So now, today, the standards that everyone is practicing, including Sharman Networks and Altnet, is by the standard, once it is installed, it is locked, and then guides the user and allows the user to unlock it if they see fit.

So for the most part, there are many peer-to-peer applications out there, primarily on the new Tele-base, that are very difficult to understand.

Chairman TOM DAVIS. Obviously, an educated user is the best defense. I do not think there is any question about that. The level of sophistication of people using this is very different.

How widespread is this problem? I mean, we see the potentials; we see an isolated case. Does the FBI have any data on how widespread it is? Do you have any feel for that?

Mr. FARNAN. Let me ask Mr. Larkin if he can address that particular question.

Chairman TOM DAVIS. I am going to have to swear him in.

[Witness sworn.]

Mr. LARKIN. Well, the problem is growing, but it is how we define the problem, I guess, as Mr. Farnan had indicated. What we see with the peer-to-peer networks is not so much identity theft. It is more intellectual property rights and software piracy and that kind of thing.

Although we have not linked it to identity theft, specifically, we do have instances where there are Trojans and "bots" that have been downloaded, at a pretty high rate and a growing rate, giving the unscrupulous creator of that Trojan or that BOT the opportunity to come in and access information on that computer.

Generally, though, it has not been the practice of those subjects out there to go in and look for that data. They are just looking for that computer to use, for some other high speed attack where they need that type of bandwidth for.

Chairman TOM DAVIS. You only need a couple cases, and lives can be completely destroyed.

Mr. FARNAN. That is true.

Chairman TOM DAVIS. Are there any other thoughts on that?

Ms. FRANK. I think the only other thing I would say is, it is so important to realize that most identity theft victims do not know where it is coming from. So what happens is, if they are sharing and somebody gets this information, they will never know, and it is very hard for even the FBI to know.

Chairman TOM DAVIS. Mr. Broes, what steps is KaZaA taking to proactively protect their privacy and security of its users?

Mr. BROES. Well, I cannot speak on behalf of Sharman Networks. But I can tell you that as a partner, we have encouraged them to look at every possible study, such as Mr. Good's study, and they have definitely taken that to heart.

I think many of the things that he has discussed and many of the issues that we are discussing here today will be addressed in the very, very near future, in the future releases.

Chairman TOM DAVIS. In general, are the file-sharing companies doing a good job educating users about the privacy and security risks? Are they doing a better job; are they on to this? What is the consensus on this?

Mr. BROES. Well, I have recently come on board with Altnet. I would say that from my perspective, Sharman Networks, who run KaZaA Media Desktop, have been the most proactive in that.

In the past, coming from the security and technology background, I was the one that was actually hired by the Motion Pictured Association, when they AA to do the analysis of the fast track network, before the legal action was taking place. So I had a unique look at this.

I can tell you from what I have seen, they are taking the most proactive approach. I have encouraged it with some of the other peer-to-peer companies, such as LimeWare and Bearshare, with absolute resistance.

Chairman TOM DAVIS. Thank you very much.

Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman. I think most people do not realize, they are opening up their own files when they go to these peer-to-peer systems.

Mr. Good, in your demonstration, were you actually downloading someone's personal files in real time?

Mr. GOOD. No, during the demonstration, that was recorded beforehand. But no, we did not download anything. We just looked and browsed around.

Mr. WAXMAN. So you can look and browse around. Is the reason that people have their personal files open for others to come in and look around because of the configuration process when they go to the peer-to-peer networks?

Mr. GOOD. If I understand the question correctly, the question was, would people be sharing stuff other than by making a mistake? Is that correct?

Mr. WAXMAN. Well, if you were going to go to a peer-to-peer network, I do not think you are asked the question, are you willing

to open up all your files; or are you asking the question? Do people then check, yes, or are you able to check, no?

Mr. GOOD. Yes, you are not asked directly, do you want to open up all your files. You are asked, what do you want to share with the network.

There are various ways that they do it. Depending on the version, in earlier versions, they offered to search your hard drive for you.

In different versions, just by default, they would not share anything. Then if you decided to change the download folder, you had to understand what it meant to change the download folder. Those assumptions were not stated explicitly. So it really depends.

In the latest version that we downloaded a couple of days ago, it does offer to search to share your files. But it does not ask you that question directly, do you want to share everything or not.

Mr. SCHILLER. If I may jump in?

Mr. WAXMAN. Yes, Mr. Schiller.

Mr. SCHILLER. Just last week, I asked my staff to do a trial run of downloading KaZaA, because I wanted to see how it worked these days because, of course, it keeps changing.

We used a blank computer that was newly installed, fresh, what have you, and downloaded KaZaA. When we installed it, it did ask us the question, do you wish to search your hard drive for files to share. It offered to share the directory where those files are stored.

I said to the guys doing this, you know, that means it is going to search for media files like MP3s and what have you. But then it is going to offer to share the directory that they are in, which might contain other files. Is it only going to share the MP3s or is it going to share all the other files?

Now we are experts, and we did not know. I think most people would not think twice about it. So if you had an MP3 in your "My Documents" folder, and you also had your tax returns in your "My Documents" folder, I would bet even money that the chances are, both wind up being shared.

Mr. GOOD. That is actually a really good point. I mean, it does not state the assumptions that it is using while it is sharing. While it is searching for folders to share, it does not state what those were. As Jeff has mentioned, even experts were not able to really tell what it was looking for.

Mr. DAVIDSON. Right; I think there are two issues. One is sort of what are the defaults; what is easy to do? It turns out that in a lot of these systems, it is very easy to share more than you might expect to.

The other is that in a lot of these systems, you do have to take an affirmative step to share a lot of files, and particularly to share a whole drive.

For example, a system that we tried out in our office did not give you any warning when you decided to share your whole C drive, as it were. There is a lot more that could be done in the design of this software, to make sure that people have some awareness that might not be a good idea.

Mr. WAXMAN. As I understand it, on the KaZaA Network, users get priority for downloads, the more files they share, which is obviously an incentive for them to share more files. That could lead

teenagers to share all of the sensitive files on their parents' computers.

What steps, if any, does KaZaA take to ensure that all users of a particular computer know which files are being shared? Does anybody have any idea of that?

Mr. SCHILLER. If I understand the question correctly, you are asking what measures are taken to educate the user, as to what files they are sharing. I can tell you that it is not true that they do not get a priority. So I do know that. The priority is for uploads and not files that are downloaded.

Mr. WAXMAN. What does that mean?

Mr. SCHILLER. The priority is for an upload. So for upload speeds; that your files will have essentially a greater path. But I am not too certain on this.

Mr. WAXMAN. Does that mean you get a better quality?

Mr. SCHILLER. You get a better quality of download; a better quality of transfer, perhaps. I do not know the specifics.

Mr. WAXMAN. Is it not an incentive then, to open up your files to get the better quality?

Mr. SCHILLER. No, I do not think so. I think the initiative that Sharman and Altnet have always gone by, and this is why Altnet has licensed files, we have an application that is coming out in the next few weeks that will give people points that they can exchange for cash and prizes for sharing legitimate files.

So we are trying to curb the user behavior. Essentially, we are trying to encourage them to not share illegitimate or illegal or illicit files, because they will not have any benefit for doing so. We disclose that right at the beginning. So essentially, you will see on the front page, it says, for downloading or uploading gold files, you get points for and you benefit for that.

So that is really important. We were talking about user behavior or education of the end user, educating them that there is zero benefit to transferring or sharing illegal files; and there is all the benefit in the world for transferring legitimate files. So that is the message that we put forth.

To address some of the issues that we heard here recently, I think that I can tell you that the future versions of KaZaA Media Desktop, it is not public information. I cannot give specifics about what changes have been made. But I can tell you that all the issues that we have just heard with regards to a user mistakenly sharing a folder or sharing an entire directory have been addressed.

Mr. WAXMAN. My time is up, and we will have another round, I am sure. But I just want to ask you a yes or no question. A user maximizes the number of uploads by sharing the most files. Is that not a correct statement?

Mr. BROES. In participation, yes.

Mr. WAXMAN. And it does not distinguish which files?

Mr. BROES. No, that is purely up to the user. The user makes the decision on what files he wants to share.

Mr. WAXMAN. Well, I am going to question that in the next round.

Mr. BROES. Sure.

Mr. GOOD. Mr. Chairman, my-author would like to speak, also. Could we swear him in right now?

[Witness sworn.]

Chairman TOM DAVIS. Thank you, please state your name for the record.

Mr. KREKELBERG. I am Aaron Krekelberg. To address your question, there is nothing that prevents a teenager from sharing their father's files or their parents' files. If the parent were to use that computer, they would not know that that teenager had allowed the sharing of those files.

Mr. WAXMAN. And is there an incentive to share more fields, in order to get better uploads?

Mr. KREKELBERG. There seems to be a new performance level that they are adding. There seems to be an incentive to share more files.

Mr. DAVIDSON. There is a simple answer, which is, in some of these systems, yes, that is absolutely true.

Mr. BROES. Let me just also re-define something. It is not how many files you are sharing. It is how many files are uploaded.

So the user is incentivized to not share thousands of files. They are incentivized to share files that people would like and legitimate files. So by putting 10,000 files in your shared folder, that is not going to help your status.

Mr. WAXMAN. Well, some people who are interested in identity theft or delving into the privacy of others may want those files. I assume what you are saying is that most people who go to peer-to-peer file-sharing are more interested in music, and that is more popular.

But we are opening up a whole new area for a greater popularity to get private information about people what that is available to someone who takes advantage of the opportunity.

Mr. BROES. Well, from my previous experience in analyzing these networks and for precisely what we are discussing here, sharing private information, we saw a rapid decline over the years as people understood how a file-sharing network actually works.

So at the beginning, when it was just a Gnutella-based, initially right after they shut down Napster, we saw this major flood of literally tens of millions of people going to Gnutella.

Of course, they did not understand just how that decentralized network functioned. So we saw a tremendous amount of personal files being shared. But as we continued to monitor, and as we continued to educate, we saw less and less. So today, I actually find far less private files than initially.

Mr. WAXMAN. Is that a statement that others would agree with?

Mr. GOOD. Well, it is a difficult question to answer, Because the KaZaA Network is encrypted. So it is difficult to really tell to what extent the network you are searching in, at any given time; or how much access to the network a given client has.

We ran our study initially in June of last year. Over a 12 hour period, we were able to find about 150 users who were sharing their inboxes, unique users.

We ran a similar study in January, and we ran it for a longer period of time, over a week, and we were able to find about 1,000 users who were sharing their in-boxes.

It is difficult for us to say whether this is an increase or a decrease, because of the encryption, and we're not allowed to reverse engineer it, so we cannot figure out what is going on. But it definitely seems like it is a problem today.

Mr. WAXMAN. Thank you; I have further questions, but I know my colleague, Mr. Shays, wants to ask some.

Mr. SHAYS. My daughter would advise me not to be here, so I would not expose my unbelievable ignorance.

Secretary McNamara, many years ago, always thought there was a solution to every problem. He acknowledged about 10 years ago that he realizes there are some problems without solutions.

As I am listening to this dialog, I am obviously hearing the issue of identity. I am hearing somewhat the issue of virus. I know this is not a hearing about copyright. So we are not going to deal with that issue.

But I am interested to know, are there solutions to the issue of privacy, particularly; and if so, are they regulatory, legislative, what are they? Maybe you could just kind of go down the line here.

Mr. GOOD. Certainly, well, our view is twofold. As I said in the opening statement, we think it is very important to educate people. We live in a world now where people can be connected to the Internet 24 hours a day.

We are going to be living in a world shortly where the Internet is going to be on your cell phone, and location information and this sort of information is going to be available to people, also.

So it is very important for people to understand what it means to be connected to the network, and what sort of information that they could be potentially sharing.

The second and probably the more important thing, especially since I am a researcher in human/computer interaction, we like to think that we can design things so that we are not compromising security and convenience. We want security and convenience to live together, so that things are convenient, but they are also very secure.

Mr. SHAYS. Do you think that is possible?

Mr. GOOD. I think, to a certain extent, it is. I think having very smart defaults, having defaults that really protect the user; and we are starting to see that in the world, as Microsoft now is really trying to push out. So out of the box, things are safest.

This has not always been the case. It has always been the case that when things come out the box, they are pretty much open to anything. This makes the world pretty insecure. But nowadays, we are really seeing a push for having very strong default settings that really make sure that things are secure for people.

I think that there is more we can do in that area. It is a difficult problem. Because as we start getting into more complex ways to manage privacy, it becomes increasingly difficult. But I like to see those two approaches really taken seriously.

Mr. SHAYS. Well, one is education and the other is design, correct?

Mr. GOOD. That is correct.

Mr. SHAYS. Is there anything else?

Mr. GOOD. No, I think that is it.

Mr. SHAYS. Anyone else?

Mr. SCHILLER. I would say that it is great to say that we need to educate people. But, you know, I drive my car every day, and actually, I do know how internal combustion engines work. But in some sense, that should not be a requirement in order to drive a car. So I would say the emphasis has to be on the design of the technology.

My experience is, we see a pendulum that swings. The technology comes out. People tradeoff security to get more convenience. We have hearings like this. People hear about identity theft. They become concerned about the technology. The technologists then react to that and put in better technology, better design, better controls.

I am going to talk a little bit off the top of my head here. I said before that it asks which directories of files you wanted to share. You could easily, for example, say, if we are going to look for music, then let us only share files that end in .MP3, and let us not share files named "In-box."

But, you know, the funny thing is, if I am the guy designing this, and let us all know that there is a copyright issue here, that the designers of this are safer sharing everything than they are trying to just share a particular type of file. Because then it makes it easier to accuse them of, oh, gee, this is really only about sharing music.

One of the defenses people like to use is, oh, know, you can share anything. So that, I think, drives the tradeoff in the wrong direction. But certainly, I do believe it is possible to design this stuff in a way that is, in fact, reasonably secure.

Mr. SHAYS. You know, it is funny, as you all are testifying, there is always someone in the audience that is shaking their head or nodding their head. I feel like I am in a Baptist church without any sound. [Laughter.]

Dr. Hale.

Mr. HALE. Yes, I think I would agree that education is a huge component. I would also concur that our design issues, I would say, is what is designed out of the software, as opposed to what is added to it, that could really help matters.

The security circumvention tactics that are used by the software really make it difficult for a corporation or an academic institution like the University of Tulsa, for instance, to protect its user population from these abuses, if they are even real or imagined. So that is what I would consider to be addition by subtraction.

Mr. SHAYS. Given the number of participants in this hearing, Mr. Chairman, do you mind if I just complete this question with the rest of the witnesses?

Chairman TOM DAVIS. That is fine.

Mr. SHAYS. Thank you.

Mr. DAVIDSON. The Federal Trade Commission actually just had a workshop yesterday on this very question. It is great question about the broader issue of privacy here. I think there are three things besides education that we would talk about.

One is technology or design. The fact is that there are a lot of tools out that can help consumers. We have talked about some of them: encryption, firewalls, which is something that we did not

talk about today. With personal firewalls, you can give consumers more control about how their computer is communicating with.

This broader design question is building programs and systems in a way that are more privacy friendly. A second is best practices on the part of industry. I think there is strong message that needs to be sent and continues to be sent that companies need to act responsibly when they collect information, and many of them do.

But there are real issues about best practices for how people use information that they collect. That is a very powerful possible tool; industry standards, best practices.

The third, and I think it is important, is there is a growing realization that there may be a need for baseline, narrowly tailored legislation about Internet privacy, to deal with bad actors in this setting.

There are some basic components of fair information practices like notice about what information is being collected, meaningful choices for consumers about whether their information is being collected, access to the information that has been collected.

I think there is a growing awareness that we may need something like that, more broadly. I have not emphasized that. We are a supporter of that. I did not emphasize that in my testimony because I think the main issue here of people mistakenly sharing files is not something that you are likely to solve by legislation.

But, for example, the spyware issue that has come up is something, if not remedied through best practices, that might need to be something that is part of a legislative action.

Mr. WAXMAN. Would the gentleman yield?

Mr. SHAYS. Absolutely.

Mr. WAXMAN. It seems to me what you are saying is that technologically, they can develop a design so that private information is reasonably secure.

But is there not a financial incentive for them to try to subvert it, because of spyware and adware, or systems that will allow people to come in and get information, so that they can sell it to others; or get advertisers to know what you might be interested in, so they can direct advertisements directly to you?

Are those two financial incentives, so that you try to subvert it, either through port hopping or tunneling or whatever other way they can design it?

Mr. DAVIDSON. Well, I would just answer by saying I think that is absolutely true. We are concerned that obviously the reason that people are doing some of these things is because there are financial incentives.

Our belief is actually in the long run, a lot of people will realize that the best financial incentive is having customers who trust your stuff. People, if they know about what is going on, will not buy or use products that violate their privacy, if they have options.

So there is a hope that the market will develop and that people will, when they learn about these things, not use the file-sharing product that invades their privacy and has a lot of spyware. But hopefully, the more responsible actors will come on the scene.

Now maybe the answer is that if that does not work, then maybe we do need some kind of baseline legislation.

Mr. WAXMAN. If the gentleman would permit, what you have is a lot of kids who want music for nothing.

Mr. DAVIDSON. Right.

Mr. WAXMAN. So they want music for nothing, even though we should give some idea to people that when you take something that is not yours and you are not paying for it, it is a form of stealing.

So you have got kids who want something for nothing. They are not going to be informed users and worried about privacy. So they are just setting the family up for those who want to take advantage of the situation, to design ways to subvert any attempt to protect their privacy. Maybe some of the technical people can tell us about this. But is that not what we are facing, Mr. Schiller?

Mr. SCHILLER. Well, there are actually two different issues here. There is the accidental subversion of privacy by accidently sharing files you do not wish. That really has nothing to do with the adware and spyware. I would expect to see those issues being addressed, because they do not help anyone except criminals.

But the adware and spyware issue is certainly an issue where there is an incentive to gather that information. Of course, the companies who gather it want only to give it to themselves and not to the whole world.

I think the issue of multiple people using the same computer is really an issue of the design of the computer system. The Windows platform was never really designed to be a time shared, multi-user system. Windows 2000 and XP start to add that stuff, but I do not think they have added in the way that most people know how to use.

But frankly, I have a 20 month old son. When he gets older, he is going to have his own computer. Because I know not to have him get onto mine.

So I think it is a separate issue about the fact that these programs reveal stuff. The fact that it reveals stuff for other users of the computer is just a happenstance.

Chairman TOM DAVIS. Thank you, the gentleman's time has expired; the gentleman from Tennessee?

Mr. DUNCAN. Mr. Chairman, thank you very much, and thank you for calling this hearing. I think these are very important subjects that the panel members are discussing, and I appreciate your doing this.

I usually avoid discussing personal or family type things at hearings. But I heard Ms. Frank briefly mention identity theft.

My wife and I have four children. But the older of my two sons, who is a senior at the University of Tennessee, just yesterday received a notice that they want him to come to Juvenile Court to testify in a case involving apparently a 17-year-old young man who was using my son's identity and that of others to apply for credit cards and I do not know what else. I do not know all the details, yet. But he found out just yesterday that he was a victim of identity theft. So I guess I find that kind of interesting.

What should a person do who has found out that he or she is a victim of identity theft; and how wide-spread is this problem? I have had to be in and out with some constituents.

Ms. FRANK. Right; my written testimony is about 20 pages, and I talk about that quite a bit. But basically, the first thing you do,

if you find out that you are a victim of financial identity theft, with somebody applying for credit cards and credit lines in your name, the first thing you are going to need to do is to put a fraud alert on all of your credit profiles with the three major credit reporting agencies; get those credit reports; and find out what fraud is on there.

There is just a whole list of things to do. Once you find all that and go to law enforcement and make a police report, then you go through the whole process of trying to clean it up and stop it. So that gets into a whole lot of things.

But I have this little kit that I am going to give to the committee, and I will be happy to speak with you afterwards, if you would like.

Mr. DUNCAN. Well, is this problem growing quite a bit?

Ms. FRANK. Yes, it is growing tremendously. After the Gramm-Leach-Briley Act passed, it has actually gotten a lot worse, when that was our financial privacy act.

What we are finding, and let me give you some statistics, at least. I have the statistics in my written testimony. But the Federal Trade Commission shows that it has grown tremendously in terms of the complaints that they have gotten.

But a lot of people who are victims of identity theft have no idea to go to the Federal Trade Commission. So since they go the credit reporting agencies, those are better statistics.

Transunion, one of the three major credit reporting agencies reported in the year 2000 that they got 85,000 calls a month to their hotline. In the year 2001, they got 3,500 calls a day to their fraud hotline, and they did not give us their most recent figures.

The GAO report that came out last year also talked about the tremendous increase in identity theft, because our personal information is everywhere, and that is the key to identity theft, to use the Social Security number.

Right now, there are several bills pending in Congress, including Diane Feinstein's Identity Theft Prevention Act of 2003, with some things.

But there is a real need, which I had brought up in my testimony, for us to have some accountability as to how the financial industry is issuing credit without verification and authentication of persons. So that is what is happening.

Mr. DUNCAN. Well, I will look over that. My time is so short, let me go in another direction. You know, I chaired the Aviation Subcommittee for 6 years. I heard our colleague, John Linder, say at an aviation conference in January that the Federal Government always seems to overreact to any problem.

We seem to have pretty much done that in regard to aviation. They say TSA now stands for thousands standing around and so forth. [Laughter.]

So I think we have done a more than adequate job, let us say, in regard to aviation. But I think that one of our most vulnerable areas must be financial cyber-terrorism.

Do any of you have concerns about that? Do you think that is a potential problem? I read that it possibly is. There are so many people on this panel, I do not know who is the most appropriate person to comment on this.

Mr. FARNAN. Well, sir, I would like to make a comment about that. From the FBI's perspective, the answer is a resounding yes. We are very concerned about cyber-terrorism and how terrorists and others can exploit technology, which is designed to be very beneficial and can really advance all of our causes in many ways. However, that can also be abused and it can be used against us.

So we have an entire unit at the FBI that focuses on that particular issue, to try and stay current with technology, to make sure that we know what is going on out there with the goal of preventing any kind of cyber-terrorist activity.

Mr. DUNCAN. I have read here on the front page of the Washington Post that a 12 year old computer hacker opened the floodgates at the Hoover Dam. What some people are concerned about are our financial markets; yes?

Mr. BROES. That is a very big concern, and it should be a major concern of any company that distributes software that has the potential of being hijacked, so to speak; you know, 100,000 computers, hijacked to attack something specifically.

For instance, recently, Microsoft has talked about some vulnerabilities that were in Passport and instant messenger programs. If you can acquire those computers, certainly you can cause a tremendous amount of damage. That is why companies have to take a genuine responsible approach to this and understand that they have a huge responsibility in adhering to even voluntary standards and practices.

So I think absolutely that companies need to do that. I do not know whether that is legislation. I would say that companies should voluntarily adopt standards and practices, just for the sake of their security.

Mr. DUNCAN. Let me just say that I think that is a possible area of great concern for many of us. Do I have time to ask one more.

Mr. SHAYS [assuming Chair]. Let us do this, we will let Mr. Waxman go, and then we will come back to you.

Mr. DUNCAN. That is fine.

Mr. SHAYS. Mr. Waxman, you have the floor.

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

If there were going to be voluntary standards and industry-wide standards, how would that get done? Does anybody have any ideas? You have different people competing with each other.

Mr. BROES. Well, I think that companies have recently started to adopt those voluntary standards. You know, Microsoft has taken an unprecedented approach by saying, you know, it is secure by default, secure by design, secure by deployment. They stopped programming for a period of time to go back and look at these issues.

So I think that any time you have the leaders in industries taking those initiatives, you are going to find that people will follow, because that is the path of success.

Mr. WAXMAN. That is Microsoft. How about KaZaA; do they have responsibility?

Mr. BROES. Absolutely; I believe that anyone that has the ability or the potential to have their computers hijacked, for any reason whatsoever, via their software, they have a tremendous responsibility to adopt standards and practices of their own.

I believe that if there was legislation that was enacted today, they would have already complied with much of that, if not all.

Mr. WAXMAN. Along those lines, according to media reports, Altnet had planned to launch a program with KaZaA to take advantage of unused computing power of computers connected to the network. Initial reports indicated this might be done without the knowledge of users.

You have now testified that such a program is still in the works, but will be defined by the highest principles of disclosure and consent. What are those principles? Will users have the same access to peer-to-peer networks, if they do not consent to turning over their unused computing power? Unused computing power means their computing power becomes a zombie for someone else, instead having to furnish it themselves.

Mr. BROES. Users will always have the consent. It will never be a default, where it uses any resource. Altnet has been very, very careful in its design.

In fact, it can be uninstalled. With the future release of Altnet, you can uninstall the application that would share those resources. We give very, very deliberate instructions on how you can do that.

At the very beginning, when the application is installed, it says, would you like to share hard drive space in exchange for points, and those points can be redeemed for cash and prizes. That hard drive space and how the design has been built is extremely encrypted.

We have gone through all of the security measures and have adhered to the security standards that Microsoft and every other major software company has adjured to, to develop such an application.

Mr. WAXMAN. Could users be penalized for not consenting?

Mr. BROES. Not at all.

Mr. WAXMAN. What do others on this panel think about this business of how informed the consumer consent is going to be; how much lack of information there is before these consents are given for file-sharing; Mr. Hale?

Mr. HALE. If I may say, I think consent is there; informed consent, I do not know about. I recently read, not KaZaA's, but a competing client's peer-to-peer privacy policy, which I was happily surprised to find that they had.

But quite honestly, it would have been easier to try to decipher my own telephone bill. Maybe that is a topic for another hearing.

But I think in a lot of the click through agreements which, by the way, is not just a peer-to-peer problem, and it is a problem with the software industry; a lot of the click through agreements are fairly easy to click through without having to read what you are agreeing to.

So to sum up, I would say the consent is there. Whether the users are aware of what they are consenting to is an entirely different matter. This has to do with transparency, in my opinion, and clarity.

Mr. DAVIDSON. I think you are really on to something, because we often talk about meaningful choice and meaningful notice. There is, in fact, if you look at a lot of these end user license agreements, it says in there that this software is being installed and it

will do these things, but how many people actually take a look at them?

I could bring you examples of these long agreements, these long privacy agreements. The average consumer is not getting a chance to look at it. So I think we are hopeful, on some level, that people will start to figure this out. I do not want to sugar coat it, though. We think that is a baseline that needs to be met, and it is going to be tough.

Mr. WAXMAN. Mr. Davidson, let me interrupt you, because I see my yellow light is on. I wanted to ask you one more question, and I am afraid I will not get a chance to do it.

Why should people who are going on file-sharing programs and downloading copyrighted music or movies not have the fact that they are doing that provided to the copyright holders? If they are consenting to let their files be searched, because they want something for nothing, why should the copyright holders not have the access to the information that they are doing it?

Mr. DAVIDSON. Right; are you thinking particularly about the subpoena issue that I mentioned in my testimony?

Mr. WAXMAN. Yes.

Mr. DAVIDSON. I think that is a very good question. I do not think that the issue is that people who are, for example, breaking the law should not ultimately be identified and revealed. The question is, how do we do that? We have to make this balance about legitimate people getting access to personal information all the time, in law enforcement contacts and other kinds of privacy contacts.

I think the issue here is that we have a situation where it is not just legitimate uses. In this particular provision of law, it is any copyright holder, and I hazard to guess that most of the people in this room are copyright holders, they can go to a court clerk, make an allegation, and reveal somebody's identity.

Using one of these networks or using the Internet does not necessarily reveal your identity. For some people, some of the activities they do online, they do without revealing their identity, and that is extremely important.

So our feeling is that if identity is going to be revealed, it should be done with some measure of due process, and particularly, people should know that their identity has been revealed.

That is, I think, the flaw here. It is not to say that we cannot find a way to work this out, so legitimate enforcement of the law can happen. It is about the fact that there are actually in this particular provision, very few protections, and that has been our concern.

Ms. FRANK. Let me just add to that, because in California, we have a bill pending right now in our California legislature. If there is going to be a subpoena to find out who somebody is online, that there has to be notice, and that the ISP has to give notice to the user ahead of time, so that they can get a protective order or take some measure with this notice to protect themselves.

We worry about things like stalking; that someone will say, oh, I am a copyright holder, and I need to know who this person is in that chat room, and it is really a stalker and ex-husband. I literally note these kinds of things that happen.

So this is at least to give that person a chance, a 15 day notice, or a 30 day notice, or whatever it is, so that they get a chance to go in and say, look, I do not want to reveal my identity. This person really is my ex-spouse, who is trying to kill me. So that was the idea of due process, if I understand what Alan is talking about.

Mr. DAVIDSON. I cannot say it better than that.

Mr. SHAYS. Mr. Duncan.

Mr. DUNCAN. Let me go in a little different direction. I think when we come into a job like those of us who are Members have, I think we basically sort of tacitly agree to give up our privacy. That really does not concern me, but it does seem a shame to me that there is almost no privacy for private citizens now, it seems to me.

Yet, we seem to have a large segment of the population now, especially young people, who have become almost addicted to the computers, and have almost a worship of the computers. So if anybody asks any questions that are somewhat critical, they almost get offended, and I hope that none of you will get offended.

But it seems to me that, as I say, we have just about done away with privacy. In some ways, maybe it has resulted in good things. What I have in mind, I am thinking about the Dean of the Harvard Divinity School got caught for, I think it was, child pornography or something, and we see that all the time.

I do not see how anybody can feel that there is anything secret anymore or anything private that they put into a computer.

I heard on the CBS national news, 2 or 3 years ago on the radio 1 day as I was driving along, that computer hackers had gotten into the top secret files at the Pentagon, I think it was 250,000 times in the year before. I mean, it is just mind boggling.

It seems that if somebody comes up with a system or a program to develop some privacy for things that people put into their computers, that somebody very shortly comes up with something that breaks that program, or gets into it, or wipes out the privacy. What do you all say about that? Do you have any concerns?

Ms. FRANK. Well, I would just like to say that it is not just computers. It is not just our computers. I wanted to respond to the questions before about consumer education. We do this all the time with identity theft. But the truth is, they are so much beyond our control.

For example, yes, we can be educated and say to people, OK, be careful when you are online or when you are in the chat rooms, or when you are sharing information, or when you are doing e-mail. But the truth is that you can tell people that, but there is so much to know.

I really work at this, but I have a whole other field. I am sure all of you have so many bills that you have to read. I do not know how much of a computer expert you all are.

But I sit on the high tech crime unit of Orange County Sheriff Reserves, and I am the only "non-techy" on there. I have enough information to know that I should be worried. But it is too much of a burden on consumers to ask them to know all this stuff.

So if KaZaA is going to have information and they are going to have software programs that you are going to use, they should definitely give you big pop-ups in very simple language saying, if you

push this button, your whole "C" drive is going to be open. That means that everybody can get into your Quicken or your Quickbooks or your IRS or your resume or whatever it is, and it has to be simple.

Mr. DUNCAN. Well, it is like you said awhile ago, people can now find out almost everything about anybody that they want to find out about: bank records, house records, and everything else.

Ms. FRANK. Right.

Mr. DUNCAN. It amazes me that just from what I read in the newspapers that anybody thinks that anything they do on a computer today is really private; any Web site they visit, any e-mail they send; yes?

Mr. BROES. Security today has changed. We can no longer put a lock on something and assume that it is going to hold. I think the military has learned this, that it is an evolving process, and it is dynamic.

So we are continuing this. It is just like virus applications. They are continually chasing viruses. They are continually updating their data base, and they are continually educating their users as to what is out there and what the threats are, and trying to make them feel more secure about it.

I think that is the process that we are going to see take place in most applications. Certainly, as I said, there are leaders that have taken initiatives from Microsoft, all the way to Altnet and Sherman Networks. They have taken those initiatives to say, we understand there is this issue and we are dealing with that problem.

I do not foresee that changing anytime soon. This is a dynamic situation. The Internet, by nature, is dynamic, and we have to be dynamic in our approach to security and privacy.

Mr. DAVIDSON. I would just add that I think that this is the tip of the iceburg, unfortunately. There are even more interesting and sort of more invasive new technologies. We talked about location information; people building ID tags into products that people can scan and find out what you have, what you are wearing, what you are carrying in your handbag.

We are talking about networks of imbedded computers, intelligent buildings, and intelligent rooms, that are going to collect all sorts of information about people. It is going to be increasingly harder for people to avoid all of these things.

So the simple answer of hey, if you put it on the computer, you should know someone else is going to get it, is going to become, for a lot of people, not a realistic alternative.

If you use your cell phone, location information may be captured. If you go through a toll booth, and your electronic tag records that you have been there.

But even more importantly, I would say the computer is not something we can avoid in life, so we need to figure out how to address these things.

Mr. DUNCAN. Are you saying that Big Brother is already here and there is nothing we can do about it?

Mr. DAVIDSON. I think, there is nothing we can do about it is not right. I think that we need to do something about it, and we are

trying to find ways to do something about it, but we need to keep working on it because we are not there yet.

Mr. DUNCAN. I see some of the panel members laughing.

Mr. SCHILLER. It is not Big Brother. There are lots of Little Brothers.

Mr. DUNCAN. Lots of Little Brothers?

Ms. FRANK. Well, if you want my suggestion as to what I would like to have Congress do, I would like to have them set up a privacy commission. We are the only civilized country in the world that does not have a privacy commission.

If you look at Canada right above us, if you look at all the European nations, we do not have a privacy commission. We have had little privacy czars, but we do not have a privacy commission to look at all these issues.

Privacy in the millennium is not about the right to be left alone. It is the right to control your personal information. I think it is pretty frightening, when we are going on our computer and we do not know about spy-ware. We do not even know where it is. It is hidden somewhere, and we cannot even find it. That is terrifying.

So the result of that is identity theft. All this information that is being taken about us can be used in very insidious ways. So we do need to have the fair information practices that Alan was talking about: the notice, the choice, the security, all those things.

The only way to do it is to really have a real privacy commission that is looking over this whole issue. Because it is the scariest issue, I think, of what we are in, in our society right now.

Mr. DUNCAN. Well, I would agree with the commission, but I am a little skeptical. I think we are almost too far gone, really, now.

Ms. FRANK. It is out there, but access is the difference; in other words, what access and what way to control. For example, you mentioned your family.

Mr. DUNCAN. It was my son.

Ms. FRANK. So the scary thing for him is, he does not know what else has happened. He does not know if he has a criminal record.

So for him to be able to get access to those records and correct them, if you say, well, my information is out there and it is too late; well, what happens when you cannot get on an airplane because the red light comes on and it has nothing to do with you. Your name is mixed up with somebody else's; or your son, who is mixed up with some other person who has been stealing his identity and committing crimes in California and Virginia.

Mr. DUNCAN. Well, the one interesting thing that I did not mention, the young man that they have accused of doing this has a foreign sounding name, that I cannot even really pronounce.

Ms. FRANK. Remember, over half of the terrorists committed identity theft.

Mr. DUNCAN. All right, thank you very much; thank you, Mr. Chairman.

Mr. SHAYS. Ms. Frank.

Ms. FRANK. Yes.

Mr. SHAYS. You basically were kind of dealing with the solution, the education versus the design. It is kind of like your big warning system that flairs up there.

Ms. FRANK. The fact that the education is right when you are using the product, I think, would be helpful.

Mr. SHAYS. Before my time had run out, I think I was with you, Mr. Broes. I do not need to spend a lot of time on this. I just want to know, just simply, the education design, that Mr. Davidson had added some other points, is there anything that you would add to the solutions to the privacy issue, the virus issue?

Mr. BROES. Sure, well, I think it is in our best interests, and any company's best interest, to design their software to be as private and as secure as possible. So I think that, as I said, there is a tremendous amount of responsibility, I believe, with any company that has applications that are distributed to millions of people around the world.

So secure, private, by design, I think is definitely the way to go, and these are voluntary standards. These are standards that every major corporation today that wants to compete is going to have to take, because people just do not want applications on their computers that are not secure and do not provide privacy.

So I think it is going to be natural selection; that companies who are willing to play in the spy war game and not notify people, I think that they are ultimately going to be uninstalled and deleted, and people are going to remove them.

So voluntary standards and practices, I think, are critical. As I said earlier, if it were legislated today, I think that we would have already taken those initiatives.

Mr. SHAYS. I was struck by the fact that Big Brother is dead and Little Brothers are in. It is almost like we need a Big Brother, though, to deal with Little Brothers; Mr. Farnan.

Mr. FARNAN. There are definitely privacy issues involved in what we were talking about today. I think that one of the reminders that we have to give ourselves is that even though we are in an electronic age, a lot of the fundamental rules of life still apply. Things like "buyer beware" still apply.

Just because people are involved in dealing in cyberspace and conducting transactions in a computerized environment does not automatically mean that there are no privacy issues, or that it is somehow inherently safer; because as we are seeing today, it is not.

Second, to follow the analogy of the automobile that was raised a little bit earlier, what is scarey is that sometimes we can have fairly young people, and if they are interested in learning how to drive a car and we put them in a Ferrari, that might be a scarey thing, as opposed to a four cylinder car in a safer environment.

So to reiterate, the theme of education and consumer informness is crucial to this whole area, as are parental controls. Because as we have also heard, children who have access to their parents' computers may be pushing buttons that result in a lot of information leaving that household that was never intended to leave that household.

Mr. SHAYS. I just have one other quick question. I do not need all of you to respond, just one or two. Are we teaching this in school? Are we educating our kids about this?

Mr. HALE. I can speak to this, somewhat. I would say that nationwide, we are beginning to. We are only beginning to. But it is amazing the views that even some of my own students have about

piracy and their privacy, and what they are willing to give up to get the latest recording.

We work at the University of Tulsa with a number of schools: high schools, elementary schools, middle schools. I just was at a high school last week, where I spent almost the entire time talking about peer-to-peer technology and privacy issues, and media piracy, as well.

So we are beginning to, but I think that not enough of us are doing it, just yet. I think that is the key. Because once you get critical mass, then you can start to see results.

I would like to agree with what Mr. Broes said about the natural selection piece of this. I think once consumers and our children are educated, then they will begin to value privacy more. Then the economics pendulum will begin to swing in the favor of the companies that are performing due diligence in the privacy area of their software. But until that happens, the natural selection is going to favor those companies.

Mr. SHAYS. I have just a slight observation. I am struck by this hearing as to one, I would not want to be a professor teaching young people about technology, considering they probably know more than you do, and you always fear that they might.

But the other observation I make is, I am struck by the fact that young people gain these incredible skills to do bad things without necessarily knowing the ethnics behind what they are doing, which is kind of an interesting dilemma.

Mr. Chairman, thank you so much for the hearing, and I thank our witnesses.

Chairman TOM DAVIS. Let me thank all the witnesses, as well, for appearing today, and I thank the staff for working on this from both sides. We heard some very useful information today, that should concern any person who uses file-sharing programs or has them installed in their computers. Obviously, I think peer-to-peer users have to be aware of the files they are making available for sharing.

We are going to follow this up with another hearing in the near future, looking at file-sharing in Government agencies. Again, I thank the witnesses. This is very, very important, as we proceed to understand this better and move forward to whatever we might do.

Thank you very much; the hearing is adjourned.

[Whereupon, at 11:55 a.m., the committee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM – STAFF REPORT
PREPARED FOR REP. TOM DAVIS AND REP. HENRY A. WAXMAN
MAY 2003

FILE-SHARING PROGRAMS AND PEER-TO-PEER NETWORKS
PRIVACY AND SECURITY RISKS

TABLE OF CONTENTS

Executive Summary 1

Background 2

Findings 5

P2P Users Are Inadvertently Sharing Highly Personal Information 5

P2P File-Sharing Programs Introduce Spyware and Adware to User Computers..... 9

P2P File-Sharing Programs Can Spread Viruses, Worms, and Other Malicious Computer Files 11

Conclusion 12

EXECUTIVE SUMMARY

At the request of Reps. Tom Davis and Henry A. Waxman, the chairman and ranking member of the Committee on Government Reform, the staff of the Government Reform Committee examined potential privacy and security risks associated with the use of popular peer-to-peer (P2P) file-sharing programs. This report summarizes the results of the congressional staff investigation.

File-sharing programs are popular Internet applications that allow users to download and share electronic files. Since the first such program, Napster, was shut down by court order, newer file-sharing programs have taken its place and become one of the fastest-growing uses of Internet technology. The most popular file-sharing program, Kazaa, typically has four million simultaneous users. Other popular file-sharing programs include Morpheus, iMesh, BearShare, LimeWire, and Grokster.

Unlike Napster, which was limited to trading of audio files, the new file-sharing programs allow users to download any type of file from other computers connected to the network. This powerful feature creates unique privacy and security risks. In fact, file-sharing programs can potentially make every file on a computer available to millions of other users on the network.

The report finds:

- **Many users of file-sharing programs have inadvertently made highly personal information available to other users.** Committee investigators found that file-sharing programs could be used to obtain tax returns, medical records, attorney-client communications, and personal correspondence from P2P users. A search of one P2P network found at least 2,500 Microsoft Money backup files, which store the user's personal financial records, available for download.

- **P2P file-sharing software tested by Committee investigators introduce "spyware" or "adware" onto users' computers.** In Committee testing, spyware and adware programs, which collect personal information for marketers, were bundled with file-sharing programs. These spyware and adware programs caused computer difficulties, including increased "pop-up" advertisements, increased targeted spam e-mail, unusual browser activity, new and unwanted desktop software installations, and, in some instances, software conflicts and system crashes.

- **P2P file-sharing software can spread viruses, worms, and other malicious computer files.** Computer security experts consulted by the Committee reported that file-sharing programs can place users' computers at additional

risk for viruses and other malicious files due to increased connectivity, flaws in software design, and potential for quick distribution of malicious programs.

BACKGROUND

The Rise of File-Sharing Programs

File-sharing, the trading of electronic files between two or more users, was first popularized in the 1990s by the software company Napster. Napster provided free and easy-to-use software through which users could connect their computers to one another — known as a peer-to-peer (P2P) networking — to trade music files. At its peak in February 2001, Napster had as many as 1.6 million simultaneous users trading music through its centralized servers.[1] In 2000, the recording industry initiated litigation against Napster to protect its copyrights. This litigation resulted in a federal court injunction against Napster, which forced the company to shut down its centralized servers in July 2001.

Popularity of P2P File-Sharing Software Programs

According to a company representative, the Kazaa P2P file-sharing program is on track to become the most popular software download ever by June 2003.

Source: Philip Corwin, Kazaa representative (May 13, 2003).

Following the demise of Napster, a multitude of new file-sharing software programs have arisen. These new programs differ from Napster in two important ways. Whereas Napster limited users to trading electronic music files, these new programs allow users to share any kind of file, including videos and images, as well as text files. And whereas the Napster network was centralized around one computer server which tracked the trading of files, these new programs allow direct user-to-user file trading.

The new file-sharing programs include programs such as Kazaa, Morpheus, and iMesh. They first became available in 2001. Since then, their popularity has surged. In total, six of the most popular file-sharing programs have been downloaded more than 400 million times. Kazaa, the most popular file-sharing program, has been downloaded more than 220 million times, 22 million times in the last two months alone. It is currently the most popular software download on Download.com, a software clearinghouse.[2] *See* Table 1.

---

1 Neo-Napsters Proliferate in the Wake of Napster's Demise, *Broadband Week* (Aug. 2001).

2 Download.com (May 13, 2003) (online at http://download.com.com/3101-2001-0-1.html?tag=dir).

At any given time, these file-sharing programs are being used by millions of people. On a recent day, for example, Kazaa had more than four and a half million users connected to the network simultaneously — more than two and a half times the number of users Napster had at its peak.[3]

Many of the users of these new file-sharing programs are under the age of 18. Research done by Peter D. Hart Research Associates has found that of those who download files through file-sharing programs, 41% are between the ages of 12 and 18.[4] Other data shows that nearly 44% of Americans between the ages of 12 and 17 have downloaded music files from the Internet, including through file-sharing programs.[5]

Table 1

Downloads of Popular File-Sharing Program

File-Sharing Program	*Total Downloads*
Kazaa	222,591,000
Morpheus	111,012,000
iMesh	48,807,000
BearShare	18,269,000
LimeWire	15,336,000
Grokster	7,829,000

Source: Download.com (May 8, 2003) (online at http://download.com.com/3101-2001-0-1.html?tag=dir).

The Purpose of This Report

Almost all news coverage of file-sharing focuses on just one issue: the ability of users to trade copyrighted music, movies, and videos. Reps. Tom Davis and Henry A. Waxman, the chairman and ranking member of the Committee on Government Reform, requested this report to examine another aspect of file-sharing: the potential privacy and security risks posed by the use of today's popular P2P file-sharing programs. An earlier report for Reps. Davis and Waxman examined the exposure of children who use P2P file-sharing programs

---

3 On May 7, 2003, at 4:10 p.m., Kazaa had 4,614,035 concurrent users.

4 Peter D. Hart Research Associates, in-house research conducted for Recording Industry Association of America (undated).

5 *Digital Music Behavior Continues to Evolve*, Ipsos-Reid (Feb. 1, 2002) (online at www.ipsos-reid.com/pdf/publicat/docs/TEMPO_DldingPrevalence.pdf).

to pornographic content, such as x-rated videos.[6]

File-sharing programs raise privacy and security issues because at the same time that they allow users to download files from other computers, they also allow others to download files from the user's computer. Within minutes of installing a P2P file-sharing program, new P2P users can find their electronic files being downloaded from their computers by other users on the network. The ease with which files can be shared on the P2P networks raises concerns about the potential sharing of personal information, especially by users unfamiliar with the potential risks. According to a June 2002 study by researchers working for HP Laboratories:

> While primarily intended for sharing multimedia files, programs such as Gnutella, Freenet, and Kazaa frequently allow other types of files to be shared. Although this has no doubt contributed to P2P filesharing's growing popularity, it raises serious security concerns about the types of files that users are aware of sharing with others.[7]

Privacy and security issues are also raised by the bundling of third-party software programs known as "spyware" and "adware" with file-sharing programs and by the potential for the spread of viruses, worms, and other malicious computer files on the peer-to-peer networks.

At the request of Reps. Davis and Waxman, this report seeks to address three issues:

1. Is there evidence that P2P users are sharing personal documents on the P2P networks? If so, what are possible reasons that may contribute to the sharing of personal information?
2. Are third-party software programs known as "spyware" and "adware" bundled with popular P2P file-sharing programs? If so, what are the privacy and security concerns associated with their installation?
3. Does the use of P2P file-sharing programs pose a significant risk of infecting a computer with viruses, worms, or other malicious computer programs beyond that posed by web use?

---

6 Committee on Government Reform, *Children's Exposure to Pornography on Peer-to-Peer Networks* (Mar. 2003).

7 Information Dynamics Laboratory, HP Laboratories Palo Alto, *Usability and Privacy: A Study of Kazaa P2P File-Sharing* (June 5, 2002).

This report focuses on the privacy and security issues raised by current versions of peer-to-peer file-sharing programs. It is not intended to reach conclusions about the underlying peer-to-peer file-sharing technology itself.

FINDINGS

P2P Users Are Inadvertently Sharing Highly Personal Information

The Committee staff found that users of file-sharing programs are making personal files and information – including tax returns, social security numbers, and other personal and financial information – available for sharing on P2P networks. The Committee testing was done using the Kazaa program. Consistently, personal information was easily found, often within the first set of results returned by simple keyword searches.

The kinds of specific files found included:

- Completed tax returns with social security numbers, names and social security numbers of spouses and dependents, income and investment information
- Medical files, including medical records of military personal and military medical supply records
- Confidential legal documents such as attorney-client communications regarding divorce proceedings and living wills
- Personal correspondence, including entire e-mail inboxes of individuals
- Business files, including contracts and personnel evaluations
- Political records, including campaign and political records and private correspondence with constituents
- Resumes with personal addresses, contact information, job histories, salary requirements, and references

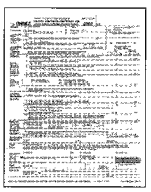
Figure 1 displays some examples of the kinds of personal information about individuals that are available for sharing and downloading on the Kazaa network.

Figure 1
Examples of Personal Files Found on Peer-to-Peer Networks

Completed 1040 Tax Form Youngstown, OH

Completed 1040 Tax Form Adamstown, MD

1040 Tax Form Cordova, TN



Completed 1040 Tax Form Walla Walla, WA

Narcotics Inventory of Naval Ship

Navy Medical Record of Service Member

Letter from Client to Attorney Regarding Divorce Proceedings

Living Will

Resume of NFL Coach

Business Correspondence Regarding Personnel Evaluation

Letter from State Senator to Constituent

Personal E-mail Inbox

Source: Committee staff test using Kazaa file-sharing program (April—May 2003) (*images blurred to obscure personal details*).

Once one personal file is discovered on a P2P user's computer, a feature on Kazaa called "Find More from Same User" will reveal every file being shared on that user's computer. Use of this feature can result in the disclosure of a wide range of highly personal information about the user. Table 2 displays examples of the kinds of personal files found by Committee staff using this feature.

Table 2
Examples of Personal Files Being Shared by Selected P2P Users Found Using Kazaa's 'Find More from Same User' Feature

Kazaa User	*Personal Files Shared by User*
User 1	• Completed 1040 tax return • Correspondence from the office of a state senator to constituents • Internal correspondence on state political organization
User 2	• Internal business records • Sensitive business correspondence, including memos on board of directors decision making
User 3	• Navy medical records • Military medical manuals • Shipboard medical supply inventories • Military information on chemical warfare • Mass casualty drill guidelines
User 4	• Correspondence with realtor on home buying • Correspondence with attorney on child's legal situation, divorce proceedings
User 5	• Personal correspondence including job experience at U.S. embassy in South America • Resume and cover letter • Personal statement • Recommendation letters
User 6	• Completed 1040 tax return • Job resignation letter including details of nursing home employment
User 7	• Two resumes of family members • My Money backup file
User 8	• Resume • Outlook Inbox file

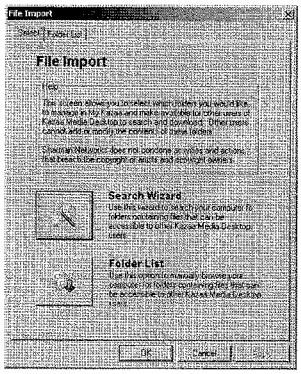
Source: Committee staff test using Kazaa file-sharing program (April—May 2003).

To estimate the scope of sharing of private financial records, the Committee asked MediaDefender, a company with expertise in peer-to-peer networks, to count the number of Microsoft Money backup files available for download. Microsoft Money is a popular financial software program. Its backup file contains the personal financial data entered by the user and can include online banking account numbers and credit card account numbers. In the program's default configuration, the backup file is saved to the "My Documents" folder on a user's computer.

MediaDefender monitored the FastTrack network for one five-day period. This is the network which is used by Kazaa, iMesh, and Grokster. MediaDefender found 2,504 unique Microsoft Money backup files available for sharing and download over this period.[8]

There are several possible causes of the unintentional sharing of personal information over P2P networks. Many users may inadvertently share personal files on the P2P network as a result of how the program is configured on their computers during the installation process. The installation process for Kazaa, the most popular file-sharing program, creates a shared folder on the user's computer in which the uploaded and downloaded files are placed by default. The creation of this shared folder would not expose personal information on the user's computer to other network users unless the user moved the information to the shared folder.

Figure 2
Kazaa Installation File Import Process



Source: Committee staff test (May 13, 2003).

The next step of the Kazaa installation process, however, gives the user two options by which they can select which files to share on the network: a Search Wizard or a Folder List. *See* Figure 2.

If the user elects the Search Wizard option, as many users will, the installation program will search the user's computer and select for sharing any folders containing image, music, or video

---

8 MediaDefender, original research conducted for the Committee on Government Reform (May 14, 2003).

files. This creates a significant risk of inadvertent sharing of information. For example, a user who uses the Search Wizard option would expose the entire contents of his or her "My Documents" folder to file-sharing if the user had stored any music or image files in that folder.

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 the entire computer available for file sharing without thinking about the types of files stored on the computer by his or her parents.

To some extent, "frequent user" preferences associated with file-sharing programs may also encourage sharing of personal information. Kazaa users receive a "Participation Level" based on the numbers of files they share that other users download, and users with higher participation levels enjoy higher priority on popular downloads. LimeWire users who choose to not share files on the network are labeled as "freeloaders" and can be prevented by other users from downloading files. These features may induce users to configure their file-sharing programs to maximize the number of files available for sharing.

P2P File-Sharing Programs Introduce Spyware and Adware to User Computers

In the course of program testing, Committee staff installed six popular P2P file-sharing programs: Kazaa, Morpheus, iMesh, BearShare, LimeWire, and Grokster. In each case, the default installation of these popular programs installed third-party programs commonly referred to as "spyware" or "adware" on the Committee computer. Both spyware and adware programs monitor the user's web browsing habits and collect other personal data.

The specific spyware and adware programs installed on the Committee computer included Cydoor, eZula, Gator, Hotbar, SaveNow, and Xupiter. Installation of Kazaa on the Committee computer, for example, resulted in the installation of Cydoor and SaveNow, software programs which track a user's e-mail address and data on his or her Internet browsing

Adware "installs itself after you click 'I agree' or legally consent to having the program on your computer. The software might monitor your Web browsing habits or ask for your demographic data to generate 'targeted ads' based on your interests."

Spyware "often installs itself without your consent. The software might monitor your Web browsing habits or record your passwords, credit card information or other e-commerce data."

Source: CNET News.com (online at http://news.com.com/2009-1023-885144.html).

activity.[9]

Installation of LimeWire resulted in the installation of Xupiter, a particularly virulent spyware program. This program, which was also for a time bundled with Grokster, has been called "the most evil thing on the Internet" by Wired Magazine.[10] Like other spyware and adware programs, it can redirect a user's homepage to a different website, install a new browser toolbar, insert entries into the user's browser bookmark list, reinstall itself after uninstallation, and ultimately crash a user's system.[11]

The spyware and adware programs bundled with file-sharing programs caused numerous problems on the Committee computer systems, including browser redirection and networking difficulties. In fact, one Committee computer was rendered inoperable by software conflicts caused by the programs bundled with the P2P file-sharing programs. On this computer, even the computer technicians employed by the House of Representatives were unable to remove the offending programs completely. These experts suggested hard drive reformatting as the only way to resolve the resulting computer difficulties.[12]

Spyware and adware programs are bundled with file-sharing programs in order to generate revenue for the programs. PC Magazine reported that it is through spyware and adware that "file-sharing vendors make money while not charging for their products. In a sense, you are paying, but the coin is privacy, not money."[13]

Kazaa's policy on spyware, available on the Kazaa.com website, states: "Kazaa Media Desktop contains banner advertising and the option to install other third party applications in order to remain free to the user. Sharman Networks [parent company of Kazaa] does not condone the use of 'spyware' and does not use 'spyware' in Kazaa Media Desktop." Kazaa then defines spyware as software which operates on a user's computer "without their knowledge or explicit

---

9 Safersite.com (online at www.safersite.com/PestInfo/C/Cydoor.asp) (assessed May 14, 2003); Computer Incident Advisory Capability, United States Department of Energy (online at www.ciac.org/ciac/techbull/CIACTech02-004.shtml) (accessed May 14, 2003).

10 *Xupiter Mongers Deal Spam, Scams*, Wired.com (Feb. 5, 2003) (online at www.wired.com/news/infostructure/0,1377,57553,00.html).

11 *Users Fume at Grokster 'Drive-by Download'*, Vnunet.com (March 3, 2003) (online at www.vnunet.com/News/1138433).

12 Testing was done while computers were not connected to the House network in order to protect the privacy and security of Committee files.

13 *Spyware—It's Lurking on Your Machine*, PC Magazine (Apr. 22, 2003) (online at www.pcmag.com/article2/0,4149,977889,00.asp).

permission." However, Kazaa users agree to the monitoring software bundled with Kazaa when they agree to Kazaa's extensive end-user license agreement.[14]

P2P File-Sharing Programs Can Spread Viruses, Worms, and Other Malicious Computer Files

Another privacy and security issue that has been associated with file-sharing programs is the risk of contracting a computer virus, worm, or other malicious computer file. According to news reports, eight worms infected P2P networks between May and September 2002 alone.[15] For example, the Benjamin worm, which created and shared new Kazaa folders, masked itself as popular music and other multimedia files, such as "Metallica – Until it Sleeps" and "Johann Sebastian Bach – Brandenburg Concerto No 4."[16]

Virus: "A virus is a manmade program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised as games or images with clever marketing titles."

Worm: "Computer worms are viruses that reside in the active memory of a computer and duplicate themselves. They may send copies of themselves to other computers."

Trojan Horse: "A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect."

Source: McAfee.com (online at www.mcafee.com/anti-virus/default.asp).

To assess these security and privacy risks, the Committee staff contacted experts in computer security in academia and the private sector. These experts expressed significant concern about security vulnerabilities associated with file-sharing programs.

Kevin Rowney, Chief Technology Officer of Vontu Incorporated, an independent company with expertise in corporate network security, said that the presence of P2P programs on networked computers "poses a set of potentially serious threats to corporate networks" including viruses and worms. In Mr. Rowney's opinion, "banning P2P systems is definitely part of any reasonable best-practices approach to network security."[17]

---

14 Kazaa.com (accessed May 7, 2003) (online at www.kazaa.com/us/privacy/spyware.htm).

15 *The Rise of P2P Worms--and How to Protect Yourself*, ZDNet.com (Sept. 8, 2002) (online at www.zdnet.com/anchordesk/stories/story/0,10738,2880466,00.html).

16 *Benjamin a Ploy for Profit*, About.com (accessed May 7, 2003) (online at http://antivirus.about.com/library/weekly/aa052002a.htm).

17 Communication with Committee staff (May 13, 2003).

Dr. John Hale, Director of the Center for Information Security at the University of Tulsa, told the Committee that "several factors conspire to make the risks induced by security vulnerabilities in P2P file-sharing clients much more serious" than the risks of surfing the web. Dr. Hale said that these factors included the increased connectivity of computer systems running P2P programs, the ability of widespread dissemination from computer to computer, and the fact that "P2P file-sharing networks expose systems to untrusted hosts and software, and offer little in the way of protection."[18]

Another feature that can induce security risks is the ability of these programs to circumvent firewalls. P2P file-sharing programs, like all Internet applications, connect a computer to an outside network through specific computer ports; network firewalls can block the use of certain Internet applications by blocking access to the specific port known to be used by that application. Popular file-sharing programs, Kazaa among them, have been reprogrammed to attempt accessing the Internet through a number of different ports as a way of maneuvering around network firewalls and the network security protections they provide. According to Jeff Schiller, Network Manager at Massachusetts Institute of Technology, the makers of these P2P programs "continue to modify and adapt their programs with the apparent goal, among others, of subverting attempts to control them."[19]

CONCLUSION

P2P file-sharing programs are popular Internet applications that allow users to download and share electronic files. There are potential privacy and security risks associated with the use of P2P file-sharing programs. Many users of P2P file-sharing programs have inadvertently made highly personal information available to other users. P2P file-sharing programs also introduce spyware and adware – programs which collect personal information for marketers – onto users' computers. And P2P file-sharing programs can place users' computers at additional risk for viruses and other malicious files due to increased connectivity, flaws in software design, and potential for quick distribution of malicious programs.

---

[18] Communication with Committee staff (May 14, 2003).

[19] Written testimony submitted to the Committee on Government Reform (May 13, 2003).