INADVERTENT FILE SHARING OVER PEER-TO-PEER NETWORKS

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 24, 2007

Serial No. 110–39

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

40–150 PDF WASHINGTON : 2008

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

COMMITTEE ON OVERSISGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
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
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

CONTENTS

INADVERTENT FILE SHARING OVER PEER-TO-PEER NETWORKS

TUESDAY, JULY 24, 2007

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

The committee met, pursuant to notice, at 10 a.m. in room 2154, Rayburn House Office Building, Hon. Henry A. Waxman (chairman of the committee) presiding.

Present: Representatives Waxman, Cummings, Tierney, Clay, Watson, Yarmuth, Norton, Cooper, Hodes, Welch, Davis of Virginia, Shays, Cannon, Issa, and Jordan.

Staff present: Phil Schiliro, chief of staff; Phil Barnett, staff director and chief counsel; Kristin Amerling, general counsel; Roger Sherman, deputy chief counsel; Earley Green, chief clerk; Teresa Coufal, deputy clerk; Zhongrui "JR" Deng, chief information officer; Leneal Scott, information systems manager; Tony Haywood, Information Policy, Census and National Archives staff director; Kerry Gutknecht and Will Ragland, staff assistants; David Marin, minority staff director; Larry Halloran, minority deputy staff director; Jennifer Safavian, minority chief counsel for oversight and investigations; Keith Ausbrook, minority general counsel; Ellen Brown, minority legislative director and senior policy counsel; Charles Phillips, minority counsel; Allyson Blandford, minority professional staff member; Patrick Lyden, minority parliamentarian and member services coordinator; and Benjamin Chance, minority clerk.

Chairman WAXMAN. The meeting of the committee will come to order.

Just over 4 years ago, the Committee on Government Reform held a hearing entitled "Overexposed: the Threats to Privacy and Security on File-Sharing Networks." Then, as now, the hearing was part of a bipartisan effort to investigate and understand the uses and risks of peer-to-peer file-sharing networks, also known as P2P networks.

The committee previously looked at two problematic aspects associated with P2P networks: children's exposure to pornography on these P2P networks, and the privacy and security risks created by these networks.

That investigation found that P2P networks were making highly personal data, such as tax returns and financial information, available to anybody using popular P2P applications like Kazaa, Morpheus, LimeWire, and Grokster. These documents were being shared with millions of computer users without the knowledge of their owners.

After the hearing, numerous P2P file-sharing program distributors adapted a voluntary Code of Conduct to prevent inadvertent disclosures of sensitive information. Along with other Members, I had hoped the problem had been solved.

In March, however, the Patent and Trademark Office released a report suggesting the inadvertent file sharing may still be a serious problem. Moreover, following the release of the PTO study, several news reports revealed that individuals and government entities were unknowingly sharing highly confidential information, including files from National Archives, the Department of Transportation, a Naval Hospital, and the Department of Defense.

The committee staff did its own investigation. We used the most popular P2P program, LimeWire, and ran a series of basic searches. What we found was astonishing: personal bank records and tax forms, attorney/client communications, the corporate strategies of Fortune 500 companies, confidential corporate accounting documents, internal documents from political campaigns, government emergency response plans, and even military operations orders.

All these files were found in unpublished Microsoft Word document format. All were found in limited searches over the past month. It is truly chilling to think of what a private organization, an organized operation or a foreign government could acquire with additional resources.

In light of these developments, Ranking Member Davis and I agreed that the committee should take another look at the privacy and security issues posed by P2P networks. We will use this hearing to examine three basic questions.

Does inadvertent file sharing over P2P networks create unacceptable risks for consumers, corporations, and Government?

If so, how extensive is the problem?

Does Congress need to intervene in this matter with legislation, or can the problems be addressed through available oversight tools and enhanced consumer education?

We are fortunate to have with us a distinguished panel of experts. They include Government officials, representatives from computer security firms, academics, and the head of LimeWire. They can provide the committee with a wide range of perspectives on the risks and benefits of P2P networks.

The purpose of this hearing is not to shut down P2P networks or bash P2P technology. P2P networks have the potential to deliver innovative and lawful applications that will enhance business and academic endeavors, reduce transaction costs, and increase available bandwidth across the country.

At the same time, however, we must achieve a balance that protects sensitive government, personal, and corporate information and copyright laws.

The goal of this hearing is to gain insights into how to strike this balance and ensure that inadvertent file sharing does not jeopardize the public's privacy and security.

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

Opening Statement of
Rep. Henry A. Waxman, Chairman
Committee on Oversight and Government Reform
Hearing on
Inadvertent File Sharing Over Peer-to-Peer Networks

July 24, 2007

Just over four years ago, the Committee on Government Reform held a hearing entitled: "Overexposed: The Threats to Privacy and Security on Filesharing Networks." Then, as now, the hearing was part of a bipartisan effort to investigate and understand the uses and risks of peer-to-peer file-sharing networks, also known as P2P networks.

The Committee previously looked at two problematic aspects associated with P2P networks: children's exposure to pornography on P2P networks and the privacy and security risks created by these networks.

That investigation found that P2P networks were making highly personal data such as tax returns and financial information available to anybody using popular P2P applications like Kazaa, Morpheus, Limewire, and Grokster. These documents were being shared with millions of computer users without the knowledge of their owners.

After the hearing, numerous P2P file sharing program distributors adopted a voluntary *Code of Conduct* to prevent inadvertent disclosures of sensitive information. Along with other members, I hoped the problem had been solved.

In March, however, the Patent and Trademark Office released a report suggesting that inadvertent file sharing may still be a serious problem.

Moreover, following the release of the PTO study, several news reports revealed that individuals and government entities were unknowingly sharing highly confidential information, including files from the National Archives, the Department of Transportation, a Naval hospital, and the Department of Defense.

The Committee staff did its own investigation. We used the most popular P2P program, LimeWire, and ran a series of basic searches. What we found was astonishing: personal bank records and tax forms, attorney-client communications, the corporate strategies of Fortune 500 companies, confidential corporate accounting documents, internal documents from political campaigns, government emergency response plans, and even military operation orders.

All these files were found in unpublished, Microsoft Word document format. All were found in limited searches over the past month. It is truly chilling to think of what private information an organized operation or a foreign government could acquire with additional resources.

In light of these developments, Ranking Member Davis and I agreed that the Committee should take another look at the privacy and security issues posed by P2P networks. We will use this hearing to examine three basic questions:

- Does inadvertent file sharing over P2P networks create unacceptable risk for consumers, corporations, and government?

- If so, how extensive is the problem?

- Does Congress need to intervene in this matter with legislation or can the problems be addressed through available oversight tools and enhanced consumer education?

We are fortunate to have with us a distinguished panel of experts. They include government officials, representatives from computer security firms, academics, and the head of LimeWire. They can provide the Committee with a wide range of perspectives on the risks and benefits of P2P networks.

The purpose of this hearing is not to shut down P2P networks or bash P2P technology. P2P networks have the potential to deliver innovative and lawful applications that will enhance business and academic endeavors, reduce transaction costs, and increase available bandwidth across the country.

At the same time, however, we must achieve a balance that protects sensitive government, personal, and corporate information and copyright laws.

The goal of this hearing is to gain insights into how to strike this balance and ensure that inadvertent file-sharing does not jeopardize the public's privacy and security.

The Chair now wishes to recognize Ranking Member Tom Davis, and we will call on Members for brief opening statements.

Mr. Davis.

Mr. DAVIS OF VIRGINIA. Mr. Chairman, thank you.

Let me just say something at the beginning, and that is that last Thursday night an event took place on the Mall on a level playing field where the Waxman Team played the Davis Team in a softball game. I am happy to say that, for the first time this year, our side won something with this committee, an 8–7 victory. For the record, I had a hit and scored a run. The Cougar team of the chairman's staff was without the services of the chairman. He was detained on business that evening, or the score might have been different. But I just wanted to note that for the record.

Chairman WAXMAN. You would have won by a bigger number. [Laughter.]

Mr. DAVIS OF VIRGINIA. We did have a couple interns. One plays on the Harvard Baseball Team, and another on the Swarthmore Baseball Team. They helped us. Oh, and we had a Rhodes Scholar in left field that made a great catch. We will be ready for a rematch any time.

I want to thank you again for this hearing today, Mr. Chairman. Four years ago, this committee undertook a detailed examination of peer-to-peer file-sharing programs. Since then, technology has advanced. Legal actions have been initiated, and the landscape of companies and programs has changed. But the risk to sensitive personal information and confidential records still exists.

I am pleased the committee is continuing an effort we began 4 years ago. At that hearing we examined the growing problem of pornography, including child pornography, on these networks. The testimony was surprising and shocking. At the second hearing we examined issues similar to those we are focusing on today. We asked why highly personal information could be found on these networks. We looked at the prevalence of spyware or adware hidden within these programs, and we examined the growing risk of downloading computer viruses from files shared on these programs.

Under my direction the committee prepared and released a staff report highlighting the types of sensitive personal information available on these networks.

Four years later it appears these problems persist. As I said then, users of these programs may accidentally share information because of incorrect program information. We will learn today exactly what people are sharing, whether they know it or not.

As I have noted before, secure information is the lifeblood of effective government policy and management; yet, sensitive personal and classified information continues to be placed at risk. The examples we will hear today will illustrate how far we have to go to reach the goal of strong, uniform, Government-wide information security policies and procedures, but this hearing will show the unique risks that we face.

I have focused on Government-wide information, management, and security for a long time. The Privacy Act and the E-Government Act of 2002 outlined the parameters for the protection of personal information. The incidents we will examine today highlight the importance of establishing and following good security practices

for safeguarding personal information, whether at home or at work. They highlight the need for proactive security breach notification requirements for organizations, including Federal agencies, dealing with sensitive personal information. And they demonstrate the need for personal vigilance and responsibility when online.

Federal agencies present unique data security requirements and challenges, and this has been our focus. These incidents demonstrate the importance of strengthening the laws and rules protecting personal information held by Federal agencies. We need to do this quickly.

As we have seen, our computers hold sensitive personal and classified information on every citizen and on every subject. We need to ensure this information remains where it should and the public knows when its sensitive personal information has been lost or compromised. Public confidence in Government in this area is essential.

It is important for us to recognize that file-sharing programs can be beneficial. As file size increases and demands for bandwidth expands, these programs can move huge amounts of data efficiently among a large number of users, but I think the volume and type of sensitive information out there will surprise people. And if this information is being harvested and shared through deceptive practices or manipulative programs, then it must stop.

For the past several years we have focused on improving and enhancing the information security posture of Federal agencies, because in the end the public demands effective Government, and effective Government depends on secure information, so this is an issue that must remain a priority for all of us.

Mr. Chairman, thank you for continuing the committee's work in this important area.

I want to welcome our witnesses and thank them for appearing today.

[The prepared statement of Hon. Tom Davis follows:]

Statement of Ranking Member Tom Davis
Oversight and Government Reform Committee Hearing
"Inadvertent File Sharing Over Peer-to Peer Networks"
July 24, 2007

Mr. Chairman, four years ago, this Committee undertook a detailed examination of peer-to-peer file sharing programs. Since then, technology has advanced, legal actions have been initiated, and the landscape of companies and programs has changed. But the risk to sensitive personal information and confidential records still exists. I am pleased the Committee is continuing an effort we began together.

At that first hearing, we examined the growing problem of pornography, including child pornography, on these networks. The testimony was surprising and shocking. At the second hearing, we examined issues similar to those we're focusing on today. We asked why highly personal information could be found on these networks. We looked at the prevalence of "spyware" or "adware" hidden within these programs. And we examined the growing risk of downloading computer viruses from files shared on these programs.

Under my direction, the Committee prepared and released a staff report highlighting the types of sensitive personal information available on these networks.

Four years later, it appears these problems persist. As I said then, "users of these programs may accidentally share information because of incorrect program information." We will learn today exactly what people are sharing – whether they know it or not.

As I have noted before, secure information is the lifeblood of effective government policy and management. Yet sensitive personal and classified information continues to be placed at risk. The examples we will hear today will illustrate how far we have to go to reach the goal of strong, uniform, government-wide information security policies and procedures. And this hearing will show the unique risks we all face.

I have focused on government-wide information management and security for a long time. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. The incidents we'll examine today highlight the importance of establishing and following good security practices for safeguarding personal information – whether at home or at work. They highlight the need for proactive security breach notification requirements for organizations – including federal agencies – dealing with sensitive personal information. And they demonstrate the need for personal vigilance and responsibility when online.

Federal agencies present unique data security requirements and challenges, and this has been my focus. These incidents demonstrate the importance of strengthening the laws and rules protecting personal information held by Federal agencies. We need to do this quickly.

As we have seen, our computers hold sensitive personal and classified information on every citizen and on every subject. We need to ensure this information remains where it should, and the public knows when its sensitive personal information has been lost or compromised. Public confidence in government in this area is essential.

It's important for us to recognize that file sharing programs can be beneficial. As file size increases and demand for bandwith expands, these programs can move huge amounts of data efficiently among a large number of users. But I think the volume and type of sensitive information out there will surprise people. And if this information is being harvested and shared through deceptive practices or manipulative programs, then it must stop.

For the past several years, I have focused on improving and enhancing the information security posture of federal agencies. Because in the end, the public demands effective government. And effective government depends on secure information. So this issue must remain a priority -- for all of us.

Mr. Chairman, thank you for continuing the Committee's work in this important area. I would like to welcome our witnesses and thank them for appearing today.

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

I want to recognize Members who wish to make a brief opening statement, but I would like to point out to my colleagues that we have a long list of very distinguished panelists to make a presentation to us, so keep the opening statements as brief as possible, and certainly no longer than 5 minutes.

Mr. Cummings.

Mr. CUMMINGS. No statement at this time.

Chairman WAXMAN. Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman.

Mr. Chairman, this is a very important hearing on peer-to-peer file-sharing networks. I want to thank all the witnesses in the distinguished panel who are here today.

We are in an age when new technologies are constantly allowing us to share information in new ways, but these innovations bring with them new security threats, and with the rise of peer-to-peer sharing networks we are seeing new challenges on how to protect our society as it moves into a technologically advanced age.

Unimaginable advances and the spread of home computers, laptops, work stations are now a part of everyday life, and significant concerns are raised and should be by peer-to-peer file-sharing networks: threats to individuals, personal financial security, the danger to our children, assaults on our national security, the possibility that peer-to-peer sharing networks allow terror groups to piece together classified information, and danger to banks and other corporations who may be inadvertent sharing confidential financial or proprietary information.

I would like to be just parochial for a moment and welcome someone from my own District who is testifying here today. M. Eric Johnson is director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and professor of operations management at the Tuck School of Business at Dartmouth College.

We welcome your testimony, Mr. Johnson, along with the rest of the panel. I am sure you are enjoying drier weather here in Washington than they are experiencing in New England.

I yield back. Thank you, Mr. Chairman.

Chairman WAXMAN. Thank you, Mr. Hodes.

Mr. Cannon.

Mr. CANNON. Thank you, Mr. Chairman. I would like to thank you particularly for holding this hearing on what I think is an extraordinarily important topic. I think that the peer-to-peer is a profoundly important concept. It has problems, as we are going to deal with today, but it is a powerful tool that can have significant effects in health care and various other areas.

I would like to introduce in the audience today we have Lee Hollaar, professor at the University of Utah, who is the co-author of the FTC Report that is referenced in the committee memo. Mr. Hollaar has been a profoundly important person in the area of technological development and understanding the legal context in which that happened.

In fact, if you read the Grokster Opinion by the Supreme Court, it follows very closely the amicus brief that Professor Hollaar had submitted. He was heavily involved when I first met him. He was working with Senator Hatch on the Digital Millennial Copyright

Act, and just this last week we actually got included in the markup of the patent reform bill in the Judiciary Committee a proposal for a special master's trial that I think may have a profound effect on our patent litigation system that he was deeply involved with.

We are now working together on making some adjustments to trademark law that would allow users to control who has access to their computers with what kind of information in a way that would profoundly change, I think, the issue of pornography and how that is promulgated on a system that is still a little bit like the wild west.

So I want to welcome Mr. Hollaar here today.

Again, thank you, Mr. Chairman, for holding this hearing, and Mr. Davis. I yield back.

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

Mr. Cooper.

Mr. COOPER. No statement, thank you, Mr. Chairman.

Chairman WAXMAN. Mr. Welch.

Mr. WELCH. No, thanks, Mr. Chairman.

Chairman WAXMAN. Mr. Tierney.

Mr. TIERNEY. No.

Chairman WAXMAN. Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman. I will be very brief.

Since everyone is introducing somebody, I should recognize General Wesley Clark, who was twice my battalion commander when I was a Reservist. He's one of my claims to fame. I have very few, as you can imagine.

But more to the subject here to day, Mr. Chairman, I think your calling this hearing is very timely because of the risk to the well-being of the Internet and the well-being of people who go on to the Internet. Although I can't submit this for the record until it is properly redacted, I took the liberty of having my staff just quickly go onto the LimeWire network, and we were able to download Natalia Gonzales' complete 2003 tax records, California resident. We now know about her un-reimbursed employee business expenses. We are very familiar with all of the California deductions and her gross and net taxes as a result of it, all of which was available.

I hope today at the end of this hearing not only will we have started a trend for better responsibility by those who set up peer-to-peer networks, but I also hope that we will have informed the public of the need for them to question whether or not a service is inherently on their side or exposing their computers to the worst of all losses that they could imagine, including their Social Security number and even classified information.

I will put the rest of my opening statement in for the record, and I truly appreciate your calling this hearing today and yield back.

[The prepared statement of Hon. Darrell E. Issa follows:]

DARRELL E. ISSA
49TH DISTRICT, CALIFORNIA

WASHINGTON OFFICE:
211 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3906
FAX: (202) 225-3303

DISTRICT OFFICE:
1800 THIBODO ROAD, SUITE 310
VISTA, CA 92081
(760) 599-5000
FAX: (760) 599-1178

SOUTHWEST RIVERSIDE COUNTY
(951) 693-2447

www.issa.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515–0549

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEES:
DOMESTIC POLICY—RANKING MEMBER
FEDERAL WORKFORCE, POSTAL SERVICE & THE DISTRICT OF COLUMBIA

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEES:
COURTS, THE INTERNET & INTELLECTUAL PROPERTY
CONSTITUTION, CIVIL RIGHTS, & CIVIL LIBERTIES

REPUBLICAN POLICY COMMITTEE

July 24, 2007

Opening remarks for Full Committee Hearing on Inadvertent File Sharing over Peer-to-Peer Networks

Thank you Mr. Chairman and Ranking Member Davis for holding this hearing.

Although, peer-to-peer file sharing is useful for research and other safe and legal activities, the use of this type of file sharing software and networks has long been a problem for owners of copyrighted material. In 2005, in the case of MGM v. Grokster, the U.S. Supreme Court ruled that providers of software designed to facilitate file-sharing of copyrighted works may be held liable for copyright infringement. Since that time, most companies that provided software to enable peer-to-peer file sharing have either folded or have found a legal way for consumers to pay for their use of copyrighted content.

There are many legal questions associated with peer-to-peer file sharing. In addition to facilitating piracy, peer-to-peer file sharing allows anyone with access to the network to have access to files on every other computer on the network. These files are not limited to the (illegally downloaded) music and movie files, but can also be information of a personal nature including tax returns, social security numbers, credit card information and medical records, or other sensitive information such as legal documents or classified material.

This inadvertent information sharing may be an unintentional consequence, rather than a sanctioned use, of the use of peer-to-peer file-sharing software, but even accidental consequences can be damaging. There is a very real possibility that through use of a peer-to-peer file sharing enabler such as LimeWire, a user can engage in illegal practices (other than pirating copyrighted material) such as identity theft, or gain access to sensitive or confidential material without the original possessor of the material knowing. The threat to government information is real; there have been instances in which federal employees have accidentally shared sensitive information while working from computers in their home.

It would not take much for a terrorist, under the guise of someone using peer-to-peer to "innocently" download music or movies, to gain access to a network where any number of private sector or government employees or even military personnel are unknowingly sharing files containing confidential or even classified information.

This is not at all hard to do. Right here I have the product of a few, cursory searches using terms such as "tax return," "password, and "credit;" only the searches also yielded social security numbers, credit reports, credit card numbers and banking information, legal documents concerning health records and claims, and an Army National Guard training memo.

The availability and ease of access to information that is unwittingly shared using peer-to-peer file sharing software and networks, coupled with the possibility of information getting into the wrong hands signals serious problems with companies like LimeWire. This is a dangerous practice for consumers and one that can have serious consequences for the government and even for our national security.

I look forward to hearing from our witnesses and further discussing consequences of peer-to-peer file sharing.

Chairman WAXMAN. Thank you, Mr. Issa.

Mr. Jordan.

Mr. JORDAN. No opening statement, Mr. Chairman.

Chairman WAXMAN. Thank you.

Without any other Members seeking recognition, let me introduce the panelists.

Tom Sydnor is one of the authors of the PTO Report detailing the risks of inadvertent file sharing. He is currently serving as an Attorney Advisor in the Office of International Relations at the U.S. Patent and Trademark Office.

Mary K. Engle is the Associate Director for Advertising Practices for the Federal Trade Commission's Division of Advertising Practices. She has been a staff attorney for the FTC since 1990.

Daniel Mintz is the Chief Information Officer for the U.S. Department of Transportation. He serves as the principal advisor to the Secretary on matters involving information resources and information services and mortgage mitigation.

M. Eric Johnson is director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and professor of operations management at the Tuck School of Business, Dartmouth College. His teach and research focused on the impact of information technology on supply chain management.

Mark Gorton is the founder and chief executive of the Lime Group, which owns Lime Brokerage, LLC; Tower Research; Capital, LLC; Lime Medical, LLC; and LimeWire, LLC, a leading maker of file-sharing technology.

General Wesley K. Clark retired from the U.S. Army after 34 years, rising to the rank of four-star general. His last position was as NATO Supreme Allied Commander and the Commander-in-Chief of the U.S. European Command. In 2004 he started Wesley K. Clark and Associates, a strategic advisory and consulting firm, where he serves as chairman and CEO. In November 2006 he joined the Advisory Board of Tiversa, Inc.

And Mr. Robert Boback, is co-founder and chief executive officer of Tiversa, Inc. As a result of his work at Tiversa, Mr. Boback has become a leading authority in the consequences of inadvertent information sharing, the P2P network.

We are pleased to have all of you here for our hearing today.

It is a practice of this committee that all witnesses take an oath. I would like to ask each of you if you would stand and please raise your right hands.

[Witnesses sworn.]

Chairman WAXMAN. Let the record show that the witnesses each responded in the affirmative.

We are pleased to have you with us. Your prepared statements will be in the record in full. We would like to ask if you would to try to limit the oral presentation to around 5 minutes.

Mr. Sydnor, why don't we start with you?

We will have a clock that will give you a yellow light when there is 1 minute left, the red light meaning the time is expired. We hope all of you, not just you, alone, will be mindful of that and try to summarize at that point.

Thank you.

STATEMENTS OF THOMAS D. SYDNOR II, ATTORNEY-ADVISOR, COPYRIGHT GROUP, OFFICE OF INTERNATIONAL RELATIONS, U.S. PATENT AND TRADEMARK OFFICE; MARY KOELBEL ENGLE, ASSOCIATE DIRECTOR FOR ADVERTISING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; DANIEL G. MINTZ, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION; GENERAL WESLEY K. CLARK, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, WESLEY K. CLARK AND ASSOCIATES, BOARD MEMBER, TIVERSA, INC.; ROBERT BOBACK, CHIEF EXECUTIVE OFFICER, TIVERSA, INC.; M. ERIC JOHNSON, PROFESSOR OF OPERATIONS MANAGEMENT, DIRECTOR, GLASSMEYER/MCNAMEE CENTER FOR DIGITAL STRATEGIES, TUCK SCHOOL OF BUSINESS, DARTMOUTH COLLEGE; AND MARK GORTON, CHIEF EXECUTIVE OFFICER, THE LIME GROUP

STATEMENT OF THOMAS D. SYDNOR II

Mr. SYDNOR. Thank you. I would like to thank this committee for holding this hearing on the issue of inadvertent file sharing. Other witnesses here today will focus on the consequences of inadvertent sharing; I want to focus on why inadvertent sharing occurs.

When the U.S. PTO realized that inadvertent sharing was occurring, my co-authors and I were asked to prepare the U.S. PTO report, File-Sharing Programs and Technological Features to Induce Users to Share. This report analyzed publicly available data on five popular file-sharing programs to determine why their users share files inadvertently. It reached several disturbing conclusions.

First, it concluded that the distributors of the five programs studied had repeatedly deployed at least five features that had a known or obvious tendency to cause inadvertent sharing of downloaded or existing files. Of these five features, the two most dangerous were the share folder and search wizard features condemned in the 2002 study Usability and Privacy, and in this committee's 2003 hearing. This committee had good reason to think that these features had been eliminated, as promised during its hearing.

Many distributors soon devised a self-regulatory Code of Conduct that would have prohibited their use. The authors of this code told Congress that it rendered further concerns about inadvertent sharing completely without foundation, a mere urban myth. Nevertheless, in 2004 and 2005 we found similar share folder features in four of the five programs we studied, and search wizards in at least two.

To illustrate what these features could do, consider what would happen to my family if a visiting friend installed one of these programs on my home computer and tried to store downloaded files in its My Documents folder so they would be easy to find. I would end up sharing bank statements; tax returns; passwords for investment accounts; scans of legal, medical, and financial records; all my family photos; my children's names, addresses, and Social Security numbers; and a scan of the sign that designates the car authorized to pick up my daughter from preschool. And I would also share

over 3,000 copyrighted audio files. With one mistake, I could be set up for identity theft, an infringement lawsuit, or far worse.

The situation becomes even more disturbing, because the U.S. PTO report also concluded that these five features had been deployed in waves. One study showed that many users were learning how to disable features previously deployed, new sets of features appeared and proliferated.

Why might this be happening? In the Grokster case, the U.S. Supreme Court unanimously found overwhelming evidence that two distributors of popular file-sharing programs intended to induce users of their programs to infringe copyrights. On remand, the District Court found that nearly 97 percent of files requested for downloading on these networks were or were highly likely to be infringing.

It also found that the distributor of one of these programs had claimed that the advantage of its business model was that it had no product cost to acquire music and an ability to get all the music. This business model also had a disadvantage. Modern file-sharing networks are not completely interconnected like the Internet. A given user can locate and download only a tiny percentage of the files available on the network. As a result, this business model would require many users to share many infringing files. But studies showed that when users were sued for sharing infringing files, their propensity to do so plunged.

Then the deployment of features that could dupe users into sharing files unintentionally proliferated.

As a result, it has become important to understand why features that had a known propensity to cause inadvertent sharing kept on being deployed. If this conduct was the result of error, then the risk of inadvertent sharing might be expected to decrease. Over time, mistakes should tend to be fixed. But if these features were intended to dupe users into sharing infringing files inadvertently, then the risk of inadvertent sharing might be expected to increase. Over time, duping schemes should tend to persist and proliferate.

Consequently, the most disturbing thing about today's hearing is that it had to occur again. In 2003, this committee held a hearing on inadvertent sharing after the distributor of the then most popular file-sharing program deployed recursive sharing, search wizard, and share folder features. Today, this committee is holding a hearing on sharing after the distributor of today's most popular file-sharing program deployed recursive sharing, search wizard, and share folder features.

The U.S. PTO report was written in the hope that by documenting conduct that occurred over the last few years, we could help ensure that neither inadvertent sharing nor hearings like this one will continue to recur.

Thank you.

[The prepared statement of Mr. Sydnor follows:]

Testimony before the House Committee on Oversight and Government Reform

Thomas D. Sydnor II,
Office of International Relations,
United States Patent and Trademark Office

July 24, 2007

Chairman Waxman and Ranking Member Davis, thank you for holding a hearing on the important problem of inadvertent filesharing. Together with Professor Lee Hollar and Mr. John Knight of the Department of Computer Science at the University of Utah, I am a co-author of the USPTO Report, *Filesharing Programs and "Technological Features to Induce Users to Share."*

Unbeknownst to many, users of popular filesharing programs are "sharing" files they do not intend to provide to thousands of strangers. These files may contain copyrighted works that users cannot legally distribute; they may also contain sensitive or proprietary data belonging to the user or a family member's employer. This problem can be called "inadvertent sharing."

Right now - and completely unknown to them – Americans are sharing sensitive personal data—their bank records, credit-card numbers, passwords, tax returns, and letters, to name a few. Without their knowledge, businesses are sharing confidential data about their customers, employees, and strategic plans. Federal, state, and local governments are also affected—and sensitive data has been exposed. Worse yet, Internet criminals know this, and they are data-mining filesharing networks.

Any program or service that lets users make files or data available to other users of the Internet *could* cause inadvertent sharing—regardless of whether it was a "centralized" server-based social-networking website or a fully "decentralized" peer-to-peer filesharing network.[1] In itself, the use of peer-to-peer networking should not affect whether users of a given program or service share or upload files unintentionally.

This Committee has shown great prescience in investigating filesharing. Back in 2003, this Committee investigated inadvertent sharing, even though the consequences seemed somewhat hypothetical: Then, it was unclear that inadvertent sharing could result in identity theft. Now, leading security experts, like Howard Schmidt, co-author of the Administration's *National Cyber-Security Policy*, conclude that inadvertent sharing is "a major part of the current identity theft problem." For example, Denver District Attorney Mitchell Morrissey recently indicted a gang of identity thieves who were buying crystal meth by downloading inadvertently shared financial data with LimeWire.

---

[1] For example, corporations and other entities often maintain complex networks of computers, network drives, and webservers in order to provide differentiated access to files and data: Some files and data are accessible to any user of the Internet, some only to those authorized to access a corporate "intranet," and others can be accessed only by particular employees or groups of employees. Even when such systems do not use peer-to-peer networking, files or data can be shared more broadly than was intended if permissions are managed incorrectly or if files or data are stored in the wrong location.

Surprisingly, inadvertent sharing by consumers has rarely been reported outside of the context of filesharing. The designs of popular social-networking, photo-sharing or blog-hosting sites explain why. Creators of these programs and services avoided designs that would tend to cause inadvertent sharing: Just like the developers of some early filesharing programs, they ensured that users would have to take multiple, affirmative steps before they would share or upload any given file. However, in recent years, distributors of file sharing programs have deployed features that may promote inadvertent file-sharing.

Four years ago, this Committee, and then the Senate Committee on the Judiciary, held hearings on *Usability and Privacy,* and inadvertent sharing. During both hearings, several legislators expressed concerns that unless distributors of file-sharing programs eliminated these features and their effects, their programs could compromise national security In response to these concerns, many distributors developed "voluntary standards and practices" to prevent inadvertent sharing. The resulting standards were complied in an industry *Code of Conduct.* This *Code* imposed three obligations to prevent inadvertent sharing:

- **The "Conspicuous Confirmation Requirement:** "[Our] software ... shall conspicuously require the user to confirm the folder(s) containing the file material that the user wishes to make available to other users...."

- **The "Reasonable Design" Requirement**: "[Our] software ... shall be designed to reasonably prevent the inadvertent designation of the contents of the user's ... principle data repository ... as materials available to other users."

- **The "Ready Uninstall" Requirement**: "A method by which [our] software ... readily may be uninstalled shall be provided to users."

However, even with the *Code of Conduct,* inadvertent file sharing kept reoccurring—and causing the very problems that this Committee had documented or foreseen in 2003. For example, the Department of Homeland Security soon reported that inadvertent sharing was disclosing classified data: "Multiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P."

When reports like this came to the attention of the USPTO, Jon Dudas, the Undersecretary of Commerce for Intellectual Property, directed me to find out why this supposedly solved problem was recurring. I then enlisted the computer-science expertise of my coauthors. We created a set of reporting criteria, and examined how the sharing-related features of five popular filesharing programs had evolved.

Our findings were presented in the USPTO Report, *Filesharing Programs and "Technological Features to Induce Users to Share."* It analyzed five popular filesharing programs, as well as *two* types of inadvertent sharing that could harm users.

Some users might inadvertently share *downloaded* files acquired through the filesharing program. Sharing of downloaded files can expose the user to a copyright-enforcement

lawsuit because such files may be infringing: One study found that almost 97% of the files requested for downloading were infringing or highly likely to be.

Users might also inadvertently share *existing* files created by other programs and stored on the user's computer. Sharing existing files can expose families to identity theft, job loss, and an infringement lawsuit: Most computers contain sensitive personal data, employers' data, and large collections of audio files ripped from legally purchased CDs.

The USPTO Report concluded that the distributors of the five programs studied had repeatedly deployed five "features" that had a known or obvious tendency to cause inadvertent sharing of downloaded or existing files, or both:

- **Poorly Disclosed Redistribution Features**: By default, most filesharing programs will cause users to share files that they download. If poorly disclosed, these features can cause inadvertent sharing of downloaded files.

- **Share-Folder Features**: These features let a user select a different folder to store downloaded files—but they do not warn the user either that the folder selected will be shared or that its subfolders will be shared recursively. These features can cause users to share existing *and* downloaded files inadvertently: A user who tries to store downloaded files in an accessible location like "C:\" or "My Documents" will tend to "share" all of their personal files *and* their collection of audio files ripped from purchased CDs.

- **Search-Wizard Features**: These features search a user's hard drive, or drives, and either recommend or cause the sharing of folders that contain enough "media" files, including document, image, audio, and audiovisual files. They often recommend that new users share "My Documents" and all of its subfolders.

- **Partial-Uninstall Features**: These ensure that when a user uninstalls a filesharing program, the process will leave behind a data file. If another copy of that program is ever installed again on the user's computer, it will read that data file and share all folders shared by the "uninstalled" copy of the program. The user may receive no notice of this changed default behavior. These features can cause inadvertent sharing of downloaded or existing files.

- **Coerced-Sharing Features**: These provide misleading feedback that makes it look like a user has disabled sharing even though files are still being shared. These features can cause inadvertent sharing of downloaded files and inadvertent sharing of existing files if deployed with a share-folder feature.

Appendix A to this statement illustrates each of these features. While all can cause inadvertent sharing, the search-wizard and share-folder features criticized by *Usability and Privacy* are particularly troubling. In most programs, they cause *recursive sharing*: Not only will the user "share" most or all files stored in a folder selected by a wizard or used to store downloaded files, the user will also "share" most or all files stored in *all subfolders* of that folder. These share-folder and search-wizard features became *more*

widely used and their implementations *more* aggressive *after* distributors had created a *Code of Conduct* that should have prohibited use of KaZaA-like share-folder or search-wizard features.

The continuing use of these five "features" is also troubling because they appeared and proliferated in waves: As users of filesharing programs learned how to disable some of these features, new ones appeared.

During 2002, share-folder, search-wizard, and partial-uninstall features appeared. By mid-2003, they were widely deployed in many filesharing programs. But then, the district-court decision in *Grokster* forced copyright holders to sue users sharing hundreds or thousands of infringing files. Predictably, users tried to stop sharing infringing files.

Then, coerced-sharing features began to proliferate. By July of 2005, four out of the five programs studied contained coerced-sharing features.

Certain "business models" worked only if many users of file-sharing programs shared many infringing files. When users were sued for doing that, their propensity to share infringing files plunged—and "technological features" that could "induce users to share" files inadvertently proliferated. As a result, the worst effects of inadvertent sharing—widespread identity theft and dangerous breaches of personal, corporate and national security—may have increased.

I will conclude by stressing two factors that make the prevention of inadvertent sharing particularly important. Each was stressed during this Committee's 2003 hearing. Each remains valid today.

First, filesharing programs are designed to go where they are not wanted and to thwart the security measures that could exclude them. As Dr. Hale told the Committee in 2003, "P2P software is commonly designed to circumvent network security services.... 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.... [T]here is no reason for [port-hopping] other than to allow network software clients to avoid detection." LimeWire now agrees "that it is inappropriate for file-sharing programs ... to be installed on any computer with highly sensitive information." But it has made it difficult and expensive for computer owners to prevent this result. This makes it particularly important to ensure that users of its program never share any files inadvertently.

Second, as Chairman Waxman noted in 2003, "The users of file-sharing programs are predominantly teenagers." Today, filesharing programs are still widely used by teenage or preteen children—and used to break the law: In the *Grokster* case, evidence showed that "[a]lmost 97% of the files actually requested for downloading were infringing or highly likely to be infringing." Popular filesharing programs do have lawful uses, but many of their actual users use them to break the law much of the time.

This has safety implications: When teenagers or pre-teens use filesharing programs, they enter a shadowy network of anonymous strangers and mislabeled files that look like

popular songs, but contain child pornography or dangerous spyware. The USPTO Report makes one point clear: When people enter these networks, no one will be looking out for them.

The conduct described in the USPTO Report is disturbing because it continued—in public—for nearly five years. Law-abiding adults did not detect it because they had no reason to use filesharing programs. So it was not detected by consumer advocates or the vast information markets that surround most popular consumer products. Even tech-savvy public-interest groups that focused on filesharing were blinded: They seem to have had no knowledge of how the public was being affected out on the electronic frontier.

Nor could users of filesharing programs complain to enforcement agencies when inadvertent sharing affected them. As the FBI told this Committee in 2003, when people are harmed while breaking the law, they have strong incentives to avoid involving law-enforcement agencies. If virtually every one using these programs is using them to break the law, then no one can complain if they are harmed.

For all of these reasons, it is important to understand why inadvertent sharing occurs and why the features known to cause it kept on being deployed. If the continued use of these features resulted from error, then the risk of inadvertent sharing might be expected to decrease: Over time, mistakes should tend to be fixed. But if these features were intended to dupe users, then the risk of inadvertent sharing might be expected to increase. People do not like to be tricked: Over time, duping schemes should thus tend to evolve, proliferate, and become more deceptive. The disturbing persistence of inadvertent sharing—the same "features" in the same programs repeatedly causing the same problems—thus raises important questions with broad implications.

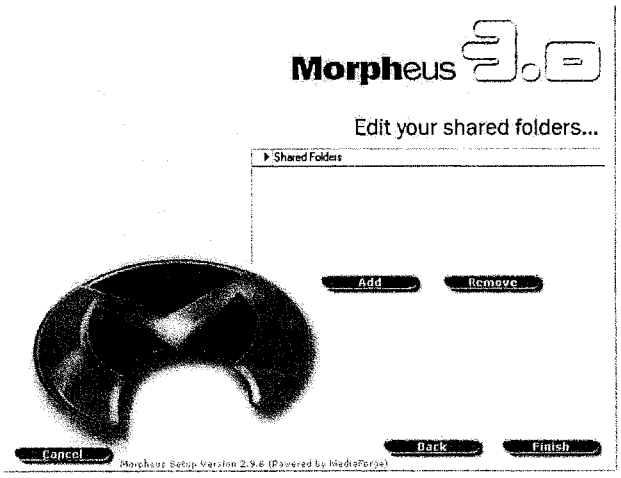
Appendix A to
the Testimony of Thomas D. Sydnor II,
Office of International Relations,
United States Patent and Trademark Office
July 24, 2007

The following five pages illustrate each of the five "features" discussed in the USPTO Report.

Redistribution Features

Description: By default, almost all filesharing programs will share all files that a user downloads from a filesharing network. Programs usually do this by creating a new, empty folder when they are installed; this folder has a name like "Shared" or "My Downloads." By default, this folder stores downloaded files, and all files in it are shared. So unless a user changes the default settings or physically moves downloaded files, all downloaded files will be shared.

Users may receive no or misleading information about redistribution features during a filesharing program's installation-and-setup process: Some programs, like eDonkey, do not inform users about redistribution during their installation. Other programs provide potentially misleading information: For example, the installation process of a 2003 version of Morpheus makes it look like *no* folder would be shared by default. But this version of Morpheus had a redistribution feature—the folder used to store downloaded files was shared by default.

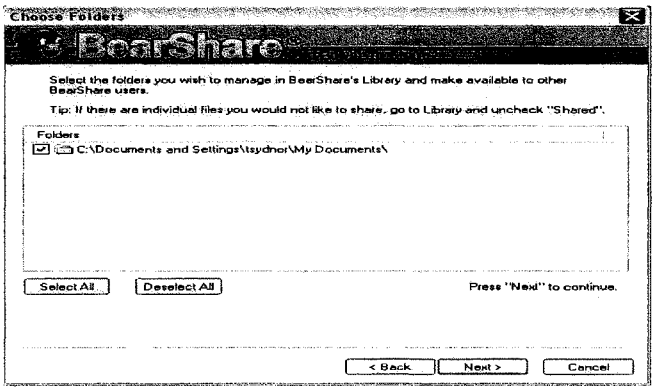


Users may receive no or little information about sharing when a filesharing program is operating: Research shows that most users of filesharing programs do not want to share files from their computers; they only want to search for and download files shared by others. Some programs, like eDonkey, provide download-only users with no information about their shared files on their main interface. Other programs do provide very little information about sharing on the main interface. LimeWire, for example, provided *less* information about shared files on the main interface over time.

Search-Wizard Features

Description: A search wizard scans the hard drive of a user's computer and presents the user with a list of folders that the user might want to share with others. Sharing caused by search wizards is usually recursive: The user will share not only all files stored in a folder selected by the wizard, but also all files stored in any of its subfolders.

Problems: The problems with search wizards are evident in this screenshot of the results screen of a BearShare search wizard from 2005:



Wizards will "recommend" the sharing of folders that are inherently unsafe to share: This wizard recommends that the user share "My Documents." By default, almost all user-created files will be stored in this folder or its subfolders. It would never be wise to share "My Documents." But the wizard recommends that the user do so.

Wizards may not disclose recursive sharing: This wizard tells the user that the folder "My Documents" has been selected for sharing, but not that the *files* stored in this folder will be shared. More importantly, it does not disclose that this folder will be shared *recursively*: All of the hundreds of files stored in its scores of *subfolders* will also be shared.

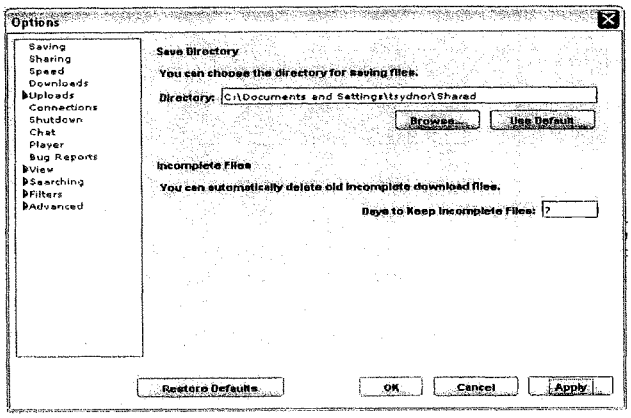
A user must have perfect information about the location of all his files and folders to respond rationally to a wizard's recommendations: *Usability and Privacy* reminded distributors that computer users are "notoriously bad" at remembering folder-subfolder structures and relationships. Unless users understand exactly how folders recommended for sharing relate to all other folders on their computers, they cannot evaluate the wizard's recommendation.

Wizards usually run during the installation-and-setup process, when the user will be most unfamiliar with the program and its potential effects: Users will encounter wizards when they are least familiar with a program and its capabilities—and thus most likely to defer to "recommendations" from its distributors.

Share-Folder Features

Description: When filesharing programs are installed, they create an empty folder, (usually called "Shared" or "Downloads"), that will store copies of downloaded files. A share-folder feature lets the user select another folder in which to store downloaded files, but it does so through an interface that fails to warn the user that existing files in the selected folder will be shared or that subfolders will be shared. Share-folder features usually cause recursive sharing: The program will share not only existing files stored in the selected folder, but also existing files stored in all subfolders of the selected folder.

Problems: The problems with share-folder features are evident in this screenshot of the Share-Folder feature in a 2004 version of LimeWire:



Nothing on this screen indicates that this feature will *share* files: Users are only told that they are selecting a "Save Directory" to store files downloaded from other users. They are not told that all files in this folder will be shared.

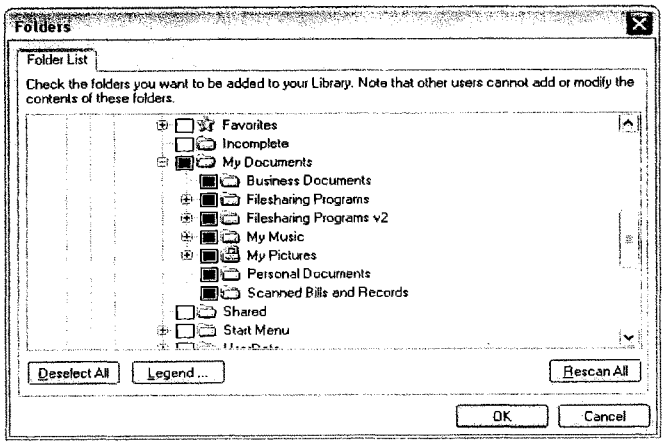
Recursive sharing is not disclosed: The share-folder feature also fails to disclose that the "Save Directory" will be shared recursively: The program will share not only all files stored in the folder selected as the "Save Directory," but also all files stored in all of its subfolders.

"Librarying" is not disclosed: This share-folder feature has a button labeled "Use Default." If the user has set the "Save Directory" to a folder that would not be safe to share, like "My My Music," pressing "Use Default" will reset the "Save Directory" to the special folder that LimeWire creates when it is installed. But the program still keep sharing "My Music" recursively, even though it is no longer the "Save Directory." We called this "librarying." In short, *every use of a librarying share-folder feature will cause the user to share more files and folders, never less.*

Partial-Uninstall Features

Description: If a user "uninstalls" most filesharing programs, (for example, by using the "Remove Program" function on the Control Panel in Microsoft Windows), these programs will appear to uninstall. But the process will leave behind a data file that will cause any subsequent installation of any version of the same program to automatically share all folders that were shared by the "uninstalled" version of the program.

Problems: The problems with partial-uninstall features are evident in the following screen shot, which shows the folders that were shared by default, without notice to the user, when a 2005 version of BearShare was installed on a computer on which no filesharing program was installed.



Thanks to a partial uninstall feature, this user is now sharing his "My Documents" folder recursively, by default, and with no notice.

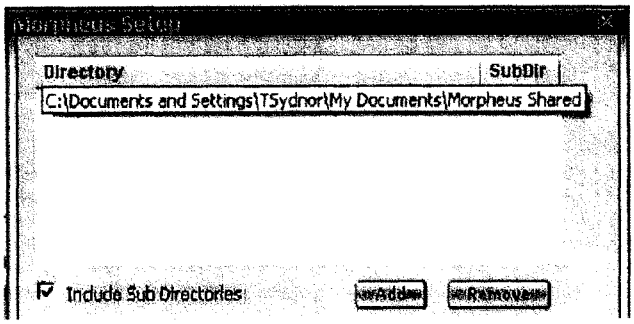
These features prevent users from correcting mistakes by removing the program: Users who discover that they are inadvertently sharing files might well try to correct their errors by removing the program and "starting over" with a new default installation. These features ensure that there is no starting over.

These features are particularly dangerous when more than one person uses a given computer: Users have been warned to avoid inadvertent sharing by using the "default" settings created when a filesharing program is installed. But when more than one person uses a computer, like a family computer, users have no way to know how a "default" installation of a filesharing program will behave.

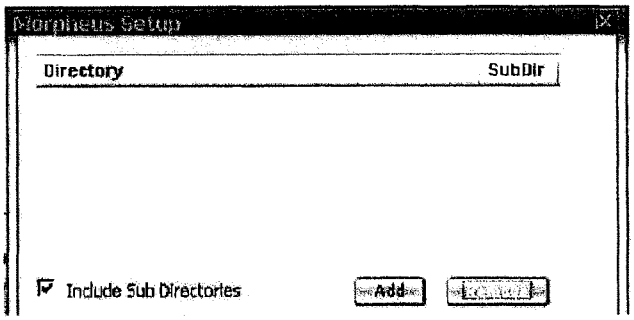
Coerced-Sharing Features

Description: Coerced-sharing features make it more difficult for users to halt sharing caused by redistribution, search-wizard, share-folder and partial-uninstall features. Different programs achieve this different ways, but most coerced-sharing features ensure that users who try to stop sharing particular folders will fail while thinking that they have succeeded.

Problems: The problems with coerced sharing features are evident in the following two screenshots taken during the installation-and-setup process of a 2006 version of Morpheus:



Users who guess that this screen lists the folders that users will share might realize that Morpheus has a redistribution feature. These users might then try to halt sharing of downloaded files by selecting this folder and clicking the "Remove" button. If so, Morpheus will provide the following feedback on the effects of the users' actions:



The list of shared folders is now empty, so users would probably conclude that they will not share downloaded files because they have halted all sharing of all folders. But this would be wrong: The users' actions have had no effect; the folder that stores downloaded files will still be shared. This sort of misleading coerced-sharing feature also makes it more difficult for users to correct the effects of all the other features discussed above.

A Reply to

"LimeWire Response to Questions addressed to Mark Gorton by the Committee on Oversight and Government Reform"

from Thomas D. Sydnor II, John Knight, Lee A. Hollaar

On June 19, 2007, Chairman Waxman and Ranking Member Davis sent a letter, (the "Committee's Letter"), to LimeWire LLC. It asked LimeWire to respond to nine questions and to *Filesharing Programs and "Technological Features to Induce Users to Share"* (the "USPTO Report"). On July 5, 2007, LimeWire provided a 47-page response consisting of cover letter, a response to the nine questions, an Appendix on the USPTO Report, and a "Walkthrough" of inadvertent sharing precautions in LimeWire (collectively, the "Response"). In order to assist the Committee's investigation, we provide this reply to LimeWire's Response.

Based upon public data, the USPTO Report concluded (1) that distributors of popular filesharing programs had deployed at least five features that they knew or should have known would cause users to share files inadvertently, and (2) that these features may have been intended to cause inadvertent sharing because (a) they became more prevalent and more aggressive after their potential to cause inadvertent sharing was known, and (b) they were deployed in waves—new "features" appeared as users learned to disable those previously deployed. LimeWire's Response identifies no material defects in the Report's analysis or in its conclusions.

While we can reply point-by-point reply to each objection or claim in the Response, doing so would bury and disperse information about the five problematic features discussed in the USPTO Report. Consequently, this reply will focus on those features, and discuss them in the order presented in the USPTO Report. It will focus, in particular, on the most disturbing features deployed in LimeWire: Share-folder and search-wizard features like those condemned in the 2002 study *Usability and Privacy* and this Committee's May 15, 2003 hearing.

These share-folder and search-wizard features are critical for two reasons. First, on a home computer, they can cause catastrophic inadvertent sharing that results in emptied bank accounts, lost jobs, *and* a copyright-infringement lawsuit. Second, the problems with these two features were exhaustively detailed in *Usability and Privacy* and the congressional hearings that prompted distributors to develop the *Code of Conduct* that should have precluded their use.

1. LimeWire's Redistribution Feature.

The USPTO Report (pp. 14-15) criticized LimeWire for replacing its once-useful main-interface display of the number of files a user was sharing, "Sharing 42 files" with a cryptic number, "42." LimeWire's Response (p. 9, Fig. 8 & p. A8, FigA7) repeatedly asserts that if a user hovers a mouse pointer over this number, a tooltip will explain its meaning, "You are sharing 42 files."

This claim surprised us: When preparing the USPTO Report, we had looked for, but never seen, a floating (or clickable) tooltip in LimeWire 4.10.9. Then we re-examined Figure 8 in the Response. As the Committee and its staff probably know, Windows-based programs are often

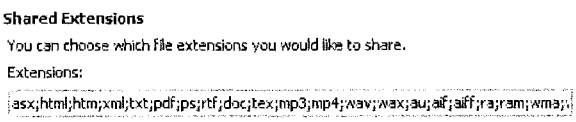
run in full-screen mode. But they can also be run in "windowed mode," in which the program runs in a smaller window that occupies only some of the screen. Figure 8 shows LimeWire in windowed mode, and the tooltip appears *below* the bottom of the window running LimeWire.

Because most users are likely to do so, we run LimeWire in full-screen mode. Doing so made the tooltip *invisible*: It "appeared" behind the opaque Windows "Start" menu. This is what we saw when "hovering" a mouse over the cryptic number:

When we ran LimeWire 4.12.15 on another computer, we could get the tooltip to appear on-screen, but on this computer, LimeWire looked like this when running in windowed mode:

In any case, these screenshots, and Figure 8 of the Response undermine LimeWire's claim, (p.A7), that the clarifying information in the tooltip was removed from the main screen, "with screen real-estate constraints in mind." In the horizontal bar in which the cryptic number appears, "screen real estate" is available, and unused.

While have not parsed them all, other screenshots in the Response show the Committee information not shown to most LimeWire users. For example, the "Shared Extensions" window shown in Figure 6 of the Response, (p. 8), indicates that all users opening LimeWire's "Sharing" menu will see that ".doc" and ".pdf" files will be shared by default:



But this is wrong. When important data cannot be completely displayed on-screen, programs usually warn users: This is illustrated by the ellipses (...) in Figures 4 and 9 of the Response, (pp.6, 10). But the "Shared Extensions" window shown in Figure 6 *does not* warn that it displays only 16% of the file types LimeWire shares by default. Worse yet, if users guess this, click into the window, and try to see if other file types are shared, most will try to scroll to the *right* because they usually read information from left-to-right. Doing so will indicate that "Shared Extensions" window display all file types shared by default. Only if LimeWire users scroll to the *left*, (for about 15 seconds), will they learn that LimeWire shares ".doc" and ".pdf" files by default.

2. LimeWire's Share-Folder Features.

The Committee's Letter asked LimeWire to "explain why warnings which were included in previous versions of LimeWire, which seem to have been intended to help users avoid inadvertent sharing, have been removed in more recent versions." The pop-up warnings referenced were those displayed in the "Saving" menu of LimeWire 2.0.4, as shown in the USPTO Report (p.27, Fig. 10). These warnings, while not ideal, (*see id.* at p. 28 & n.35), did distinguish the "Save Directory" in LimeWire 2.0.4 from the KaZaA share-folder feature criticized by *Usability and Privacy* and this Committee because (1) they warned the user that a folder used to store downloaded files could be shared; (2) they let the user chose *not* to share this folder; and (3) they warned the user that this folder, if shared, would be shared *recursively* (all of its subfolders would also be shared).

LimeWire's Response, (p.11), claims that these warnings were never removed: "[C]urrent versions do include a warning intended to help users avoid inadvertent sharing. We are not aware of a time when warnings were not included; if these warnings were ever omitted from a released version, the exclusion was due to a bug that was quickly fixed." These claims are based on "the recollection of the developers," (p.A10).[1]

The USPTO Report, (p. 23-26 & Figs. 8-10), shows that the share-folder feature in a 2004 version of LimeWire (v. 4.0.7) displayed no such warnings. LimeWire thus claims that it does not "recall" that the share-folder feature in LimeWire 4.0.7 lacked pop-up warnings, but if it did, this was "due to a bug that was quickly fixed."

LimeWire's recollections appear to be wrong. Public data indicates that the pop-up warnings displayed in LimeWire 2.0.4 were removed from LimeWire in June of 2003. For the next two years, its share-folder feature displayed *no* pop-up warnings. Nor have the LimeWire 2.0.4 warnings *ever* reappeared. *Different pop-up warnings* did appear in LimeWire 4.9.0 and later. But these warnings can mislead users about LimeWire's most dangerous behavior: Its recursive sharing of all subfolders of a shared folder.

a. From June of 2003 to June of 2005, LimeWire's share-folder feature did not warn users that a "Save Directory" would be shared, or shared recursively.

The USPTO Report (pp. 23, 25; Figs. 6, 8-9), displayed the share-folder feature in LimeWire 4.0.7 because it behaved like all other studied versions of LimeWire released between June of 2003 and June of 2005. Because LimeWire's does not "recall" that these versions behaved as the Report's claims, we re-verified our analysis using the best available public data.

---

[1] LimeWire later claims, (p.A4), that one of these developers cannot correctly describe the behavior of 2006 versions of LimeWire. LimeWire also claims that the warnings could not have been removed because this is not noted in LimeWire's *Features History*. (p. A10). Since the *Features History* records neither the addition nor the removal of LimeWire's search-wizard feature, it cannot be a reliable source of information about the removal of the share-folder warnings.

As LimeWire CEO Mark Gorton noted in a recent interview with *IEEE Spectrum*, various versions of LimeWire are widely available on the Web—collections are housed at www.oldversion.com, www.oldapps.com, and other sites. We thus were thus able to download and run copies of the following versions of LimeWire: 3.0.2; 3.4.4; 3.6.15; 3.8.6; 4.0.7; 4.4.5. We also re-checked screenshots of the behavior of the share-folder feature in 4.8.0.[2]

No pop-up warnings appeared in any copy of any of these versions of LimeWire. Consequently, we again conclude that available public data indicates that *no version* of LimeWire released from June of 2003 to June of 2005 displayed *any* warning when a user activated its share-folder feature. The behavior of LimeWire 4.0.7 appears to be neither atypical nor "due to a bug that was quickly fixed."

b. Since June of 2005, LimeWire's share-folder features and its "Sharing" menu displayed warnings that could cause inadvertent sharing.

LimeWire's Response, (p.2), cites several "newly added" warnings that it claims will prevent inadvertent sharing. But these warnings have been deployed for over two years. This raises a question: Why does LimeWire keep causing catastrophic incidents of inadvertent sharing? Two factors may explain why these recent warnings fail to prevent inadvertent sharing.

First, the USPTO Report, (p.33), criticized LimeWire for implementing anti-inadvertent-sharing measures in ways that denied their benefits to users upgrading from the past versions of their program that had necessitated such measures. Consequently, the vast majority of LimeWire users who had once used pre-4.9.0 versions of LimeWire will not benefit from recent changes in the program: Their sharing settings will not be rechecked or reset, so they will never see the warnings—even if they are sharing a "sensitive" folder like "Documents and Settings."

Second, the recent warnings LimeWire identifies differ from the warnings in LimeWire 2.0.4 in two ways: (1) they do not disclose that sharing a given folder will recursively share all shareable files in all of its subfolders, and (2) most indicate that sharing *will not be recursive*—that the user will share only "this folder," the one folder selected through a share-folder feature or displayed in a pop-up sensitive-folder warning.

We will reply below to LimeWire's unsubstantiated claim that "[r]ecursive sharing is the behavior that most experienced computer users expect." For now, even were this claim relevant and accurate, (and it is neither), recursive sharing would still cause inadvertent sharing if a program that shares folders recursively indicates that it does not.

(1) The share-folder feature in LimeWire's setup process indicates that sharing will *not* be recursive.

---

[2] Because LimeWire is an open-source program, we should have been able to cross-check public data by compiling executable copies of older versions of LimeWire from the code stored in LimeWire's Concurrent Versioning System (CVS) depository. Unfortunately, the data needed to compile versions of LimeWire prior to 4.13.1 appears to have been removed from LimeWire's public CVS depository.

Since June of 2003, LimeWire has deployed a share-folder feature in its setup process. This share-folder feature will be encountered mostly by new users installing LimeWire for the first time—by those who are least likely to be familiar with LimeWire and its capabilities. This share-folder feature is shown in LimeWire's Walkthrough (p. 9, Fig. 10).

It displays the default "Shared" folder and lets the user choose to store downloaded files in a different folder. Unlike the share-folder feature and "Sharing" menu within LimeWire, this share-folder feature displays *no* pop-up warnings: Users cannot avoid sharing a selected folder, and they will not be warned if they select a "sensitive" folder.

Worse yet, while the feature does disclose that a folder selected as the download folder will be shared, it also indicates—wrongly—that sharing will *not* be recursive: "*This folder* will also be shared...." (emphasis added). This wording is inexcusable: *Usability and Privacy* warned, five years ago, "The word "folder" is singular, implying one folder, and does not hint that all folders below it will be recursively shared with others."

(2) The pop-up warning in LimeWire's internal share-folder feature fails to disclose recursive sharing.

LimeWire's Response, (p. 6), claims that its internal share-folder feature will display a pop-up "recursive-sharing warning." This claim is facially wrong: When LimeWire disclosed recursive sharing, it did so as follows: "Subfolders of shared folders will also be shared." USPTO Report p. 28, Fig. 11. It used similar language in its 2.0.4 pop-up warnings. *Id.* at 27, Fig.10. The Response, (p.6, Fig. 4), shows that no similar language appears in current pop-up warnings.

It thus appears that LimeWire claims that its current warning discloses recursive sharing because it refers to "your new save folders." That "s," LimeWire seems to claim, informs even young or inexperienced users that storing downloaded files in a "C:\" directory that contains no existing files will recursively share their entire drive.

The Response, (p.6, Fig. 4), reveals the flaw in this claim. LimeWire has altered its share-folder feature so users can select *multiple* "download locations" for different types of files: Users can now store downloaded audio files in "My Music," documents in "My Documents," and image files in "My Pictures." As a result, the share-folder feature that used to recursive share only *one* folder per use can now recursively share up to *six* folders per use. Indeed, Figure 4 shows a user being asked whether they want to share *two* "new save folders" as a result of one use of the share-folder feature.

Users could thus reasonably conclude that the "s" in "new shared folders" reflects this new multiple-folder-sharing capability, not that shared folders would be shared recursively. In any case, LimeWire cannot reasonably claim that recursive sharing can be effectively disclosed through warnings more opaque than those given in the search-wizard feature that it eliminated because it had "the potential to be misused by inexperienced users," (p.5).

(3) The sensitive-folder warning in LimeWire's "Sharing" menu indicates that sharing will *not* be recursive.

LimeWire's Response, (p. 2, 9), repeatedly touts pop-up "sensitive-folder" warnings that will appear if someone using its "Sharing" menu tries to share a folder likely to contain sensitive data. While such warnings could be helpful, the Response overlooks three factors that, collectively, may make these sensitive-folder warnings misleading.

First, sensitive-folder warnings could mislead if they are provided inconsistently. The list of "sensitive" Windows folders in the Response, (p.2), contains some obvious omissions:

- "My Documents": LimeWire's *Code of Conduct* dictates that this folder is "sensitive." The Response (p.9, fig. 7) suggests that this omission may have been inadvertent.
- "My Music": Popular media players save audio files ripped from purchased CDs in subfolders of "My Music." As a result, sharing "My Music" would cause many or most users to share thousands of infringing audio files and thus become targets for lawsuits.
- "My Pictures": Many digital cameras will store photographs in subfolders of "My Pictures," and many scanners or multifunction printers will also store scanned documents, (like bills, statements, tax records, etc.), in subfolders of "My Pictures."

Second, as LimeWire notes, three different interfaces in LimeWire 4.12.15 will share folders: (1) the "Sharing" submenu of its Options menu; (2) the "Saving" submenu of its Options menu; and (3) its "Library" interface. The sensitive-folder warnings will appear *only* if folders are shared through the "Sharing" submenu: In the Library, a user receives no warning if he shares "Documents and Settings," (and thus recursively shares the "My Documents" folders of all users of that computer).

Third, the sensitive-folder warning does not disclose that a "sensitive" folder, if shared, will be shared recursively. Indeed, the warning indicates, (p.9, Fig.7), that sharing *will not be recursive*: "You are attempting to share *a* folder that is likely to contain sensitive information... Share *this* folder?" (emphasis added). This could mislead even alert users. For example, *recursive* sharing of a "Documents and Settings" folder will be disastrous, but users who think that sharing is non-recursive could examine their "Documents and Settings" folder and conclude that "this folder" contains no sensitive files.

For all of the above reasons, LimeWire 4.12.15 appears to be neither the version most compliant with LimeWire's *Code of Conduct* nor the version least likely to cause inadvertent sharing. This seems attributable to LimeWire's instance that recursive sharing, (p.12), "is the behavior that most experienced computer users expect." No supporting evidence is cited, but the Response seems to claim, (p.6), that because selecting a folder in Windows Explorer will recursively select its subfolders, then "most experienced computer users" will expect filesharing programs to share folders recursively. For several reasons, this claim is both irrelevant and wrong.

LimeWire's claim is irrelevant because it knows—as do Chairman Waxman and Ranking Member Davis—that many or most users of filesharing are not experienced computer users.

Many or most are teenagers or pre-teen children who may be neither experienced nor particularly safety-conscious. As the USPTO Report notes, (p.8), LimeWire itself has referred to users of filesharing programs as "the Munchkins" and "the little guys."

LimeWire's claim also appears to be wrong. As the Response notes, (p.A5), users of filesharing programs may not expect them to behave like computer operating systems or any "other class of software." The consequences of selecting folders in Windows differ profoundly from those of "sharing" whole trees of folders and files with thousands of anonymous strangers. Users need not—and should not—expect the latter act to be no more difficult than the former.

Moreover, five years ago, *Usability and Privacy* warned distributors of filesharing programs that folders should *not* be shared recursively. It warned that recursive sharing—even if disclosed—imposed upon users a burden that too many will be unable to bear: Even if users *do know* that sharing will be recursive, they can assess its implications only if they have "detailed knowledge" of (1) what types of files a given program will share, (2) the structure of their folder hierarchy and (3) the contents, locations, and sensitivity of all files it contains. If most users could retain this detailed structural and substantive knowledge, Windows would not contain a file/folder search system—and filesharing programs would not have contained search-wizard features.

During the last five years, LimeWire has been testing its contrary theories about the obviousness of recursive sharing on the public. The results of its experiments speak for themselves.

3. LimeWire's search-wizard feature.

LimeWire's Response to the Committee's question about its search-wizard feature is unhelpfully vague. The Response admits, (pp. 5, 14, A8), that LimeWire did deploy—but has "recently" stopped deploying—a search-wizard feature. It does not disclose when it was first deployed or when it was removed.

We have thus re-analyzed public data to provide the Committee with information on these issues. We first found a search wizard in LimeWire 3.8.6, released in February of 2004. We found it in each subsequent studied version through 4.12.12, which was available in June of 2007. LimeWire thus deployed a search wizard for about 3½ years. In all studied versions, the search wizard tended to "recommend" recursive sharing of the user's "My Documents" folder and all of its subfolders—the user's "principle data repository."

This search-wizard feature did not differ materially from the KaZaA search-wizard features condemned by *Usability and Privacy* and this Committee. In some ways, it was slightly worse: Unlike the KaZaA wizard, it would be triggered by default during the setup process, and the LimeWire wizard told users that it would search for "media files"—the Response now admits, (p.A8), that this was wrong. In other ways, it was slightly better: It did disclose that selected folders would be shared recursively—but as the Response concedes, (p.5), this failed to eliminate its "potential to be misused by inexperienced users." In the end, LimeWire had to do what KaZaA did in mid-2003: Remove the search wizard from its program.

LimeWire states, (p.5), that the *Code of Conduct* it drafted, published, and promoted in 2003 imposed "common-sense" obligations. While we agree, those obligations also responded to two specific problems—share-folder and search-wizard features—identified in *Usability and Privacy* and emphasized in the Committee's 2003 hearing. Nevertheless, LimeWire's Response, (p.2), claims "strict adherence" to the *Code* while the search wizard was deployed.

We disagree. LimeWire's *Code* stated that its program must be designed "to reasonably prevent the inadvertent [sharing] of the contents of the user's ... principle data repository." For about 3½ years, LimeWire would tend to recommend that new and inexperienced users recursively share their "My Documents" folder. A program does not "reasonably prevent" sharing of a "principle data repository" by recommending that the user share it. Nor does a "reasonably designed" program make "recommendations" that would be unreasonable for almost anyone to accept.

4. LimeWire's partial-uninstall feature.

LimeWire's Response provides a misleading and inaccurate answer to the Committee's question, "How can users completely uninstall the LimeWire program without leaving behind files that might affect subsequently installed versions of its program?" The instructions given, (p.12), will not work for users of *almost all* versions of LimeWire and they omit a key detail that makes them useless to users of the *current* version of LimeWire. These instructions are flawed because they do not acknowledge a critical change in LimeWire partial-uninstall feature.

In studied versions of LimeWire from mid-2003 through mid-2006, the datafile used by the partial-uninstall feature was stored in a *visible* folder called ".limewire" located in C:\Documents and Settings\[username]. Deleting this folder would disable the partial-uninstall feature.

Very recently, LimeWire *relocated* the relevant datafile. LimeWire 4.12.15 now stores it in a subfolder within the user's "Application Data" folder. By default, the "Application Data" folder is a *hidden folder*: Users can neither see that it exists nor delete any of its subfolders. In short, LimeWire recently changed its partial-uninstall feature in a way that prevents even users who *once* knew how to disable it from doing so again.

The rest of LimeWire's explanations for its partial-uninstall feature are not credible. First, it argues that this is an "industry standard" (p.12). But "everyone else was doing it" is no answer—particularly in an industry that has pledge to provide "a method by which [its] software may readily be uninstalled."

Second, it argues that saving user-defined settings can make it easier for users to upgrade to new versions of a program (pp. 12, A11). No one disputes that user-defined settings can be retained when a *presently installed* version of a program is upgraded to a new version.[3] Nor does anyone

[3] The Report does note, however, that if a distributor upgrades a filesharing program to remediate the effects of potentially dangerous or misleading features deployed in previous versions of the program, then user-defined settings *should be* reset or at least re-confirmed. If this is not done, the "upgrade" might look better, but it will perpetuate the effects of previous errors. USPTO Report at 33. LimeWire's Response does not dispute this point.

assert that all programs must delete all user-defined settings when uninstalled. Problems like those caused by partial-uninstall features arise only if (1) non-deleted user-defined settings could have potentially dangerous consequences, and (2) a program being installed was specially designed to re-use—rather than overwrite—any non-deleted datafiles containing those potentially dangerous user-defined settings.

If a program does this, then no one can predict the consequences of merely installing it on a computer. LimeWire's Response states (p.6): "No files are marked for sharing unless the user has explicitly chosen that file, a folder containing that file, or a folder containing a parent folder of that file...; or the user has initiated a download of the file." LimeWire's partial-uninstall feature ensures that this statement can be dangerously wrong.

Finally, LimeWire claims (pp. A10-A11) that while its partial uninstall-feature could reinstate settings *more* dangerous than the usual defaults, it might also perpetuate settings *less* dangerous than the defaults: "[I]f the previous user had wanted complete privacy and prevented all sharing, then LimeWire would automatically perpetuate that privacy and continue not sharing." Again, this claim is wrong: As discussed below, LimeWire's "Individually Shared Files" feature ensures that the lucky user who unwittingly inherits settings that *once* "prevented all sharing," will begin sharing as soon as they begin downloading.

5. LimeWire's coerced-sharing, "Individually-Shared-Files" feature.

LimeWire's Response, (pp. 12, A3), repeatedly denies that its Individually-Shared Files (ISF) feature is a coerced-sharing feature. But its alternative explanation for this feature cannot explain its behavior. LimeWire claims, (p.A11), "ISF was added along with the 'Download As' feature, to allow a user to save a download to an arbitrary location." But LimeWire will tag downloaded files as "Individually Shared Files" even if they were *not* downloaded using its "Download As" feature. LimeWire has thus failed to offer any credible alternative to the explanation proposed in the USPTO Report (pp. 35-36, 44-45): ISF is a form of coerced-sharing feature implemented because too many LimeWire users had learned how to stop sharing files.

6. Other Issues.

Only one other issue raised by LimeWire requires a reply: Its Response persistently reveals a troubling attitude toward LimeWire users and the problem of inadvertent sharing. In 2003, distributors of filesharing programs that had caused inadvertent sharing acknowledged their duty to protect their users. One told this Committee, "I firmly believe that it is the responsibility of peer-to-peer file-sharing companies to proactively protect the privacy and security of the users of their software application." *Overexposed* at 59.

LimeWire's Response, (A10), displays a different attitude toward users and their safety: "LimeWire recognizes that a file-sharing program's purpose is to share files, and has stated that it found it odd when people complain about files being shared by such programs." Similar statements litter the Response, (pp. 1, 13, A5, A6). LimeWire thus portrays inadvertent sharing

as a stupid-user problem to be blamed on "ill informed," "careless," "inexperienced," "negligent," users who "drive[] software developers crazy" (pp. 1, 5, 13, A9).

For example, the USPTO Report, (pp. 25-26), showed why a user who had inadvertently shared thousands of legally acquired audio files via the share-folder feature in LimeWire 4.0.7 might think that the sharing caused by that feature could be cured by clicking the provided "Use Default" button that *seems* to restore its default setting. LimeWire's Response, (p.A8), belittles the user who fails to realize that in LimeWire, sharing caused by one menu must be corrected in a different menu: "[T]his is an example of precisely the sort of user who drives software developers crazy.... In this case the user navigates to an option titled "Saving" instead of the option titled "Sharing" when that user wishes to change what is being shared."

With all due respect, the problem illustrated resides in the *program*, not the user. Ordinarily, no one would think that a "Saving" menu dedicated to the saving of files would affect the sharing of folders. In LimeWire, it does. When "saving" causes "sharing," it is reasonable to expect a user who discovers this—and thus realizes that she has shared sensitive *folders* by changing the default setting for *saving* files—to return to the menu that caused the problem and click its "Use Default" button to restore its default setting.

Unfortunately, this attitude that pervades LimeWire's Response is evident in the latest version of its program: Today, users of LimeWire 4.12.15 who try to halt inadvertent sharing of recursively-shared "Save Directories" by using its share-folder feature's "Use default" or "Reset" buttons will receive no pop-up warnings—just the same potentially misleading feedback that users of LimeWire 4.0.7 received in 2004.

People make errors—especially in a program in which "saving" causes "sharing," and mistakes made in one menu must be corrected elsewhere. Developers of filesharing programs must anticipate and account for the inevitability of human errors. But program developers are also human: They also make errors. To accommodate this shared trait of program users and developers, the USPTO Report, (p. 56), devised reporting criteria intended to minimize the risk that developers' honest errors in interface design might be reported as potential evidence of duping. The Report discussed only features that met those reporting criteria—even though we did discover troubling features that did not meet them because they were idiosyncratic to particular programs. Consequently, we cannot agree that the continuing prevalence of inadvertent sharing can be blamed mostly on the users of filesharing programs.

Chairman WAXMAN. Thank you very much, Mr. Sydnor.
Ms. Engle.

STATEMENT OF MARY KOELBEL ENGLE

Ms. ENGLE. Mr. Chairman and members of the committee, I am Mary Engle, the Associate Director for Advertising Practices at the Federal Trade Commission. I appreciate this opportunity to provide an update regarding the FTC's work involving peer-to-peer file-sharing issues.

We have submitted our written statement today, which reflects the FTC's views. My oral statements are my own and do not necessarily reflect the views of the Commission.

Although P2P technology offers significant benefits, such as allowing for faster file transfers and easing computer storage requirements, it also poses risks to consumers. P2P file-sharing programs may come bundled with spyware or with viruses. In addition, as the recent Patent and Trademark Office report emphasizes, consumers may end up inadvertently sharing many sensitive files that are on their hard drive.

The FTC has worked with industry to improve the disclosures of risk information on P2P file-sharing Web sites. They have also brought law enforcement actions where appropriate, and have taken steps to educate consumers and businesses on the risks involved.

In December 2004, the FTC held a public workshop to consider the many issues raised by P2P file sharing. In June 2005, we issued a report on that workshop which concluded that the risks involved with P2P file sharing stem largely from the result of how individuals use the technology, rather than being inherent in the technology, itself.

The report emphasized that many of the risks posed by P2P file sharing also exist when consumers engage in other Internet-related activities, such as surfing Web sites, using search engines, or e-mail.

In the report, the FTC staff recommended that industry do a better job of informing consumers about the risks of P2P file sharing. Over the past 3 years, we have periodically reviewed the risk disclosures provided on major P2P software Web sites and found that these disclosures have steadily improved. We also reviewed P2P Web sites to determine if they were a source of spyware.

In the fall of 2005 we downloaded the 10 largest P2P file-sharing programs to determine whether the distributors were bundling spyware or adware with their programs, and, if so, whether they were disclosing that fact. We found that, of those 10 programs, 2 bundled undisclosed spyware or adware. One of those programs is no longer being distributed, and the other we referred to foreign consumer protection law agencies.

In addition to protecting consumers by encouraging better disclosures, the FTC has brought two successful law enforcement actions related to P2P file sharing. In the case of *FTC* v. *Cashier Myricks,* the Commission sued the operator of the Web site MP3DownloadCity.com for making allegedly deceptive claims that it was 100 percent legal for consumers to use the file-sharing pro-

grams that the operator promoted to download and share movies, music, and computer games.

In the case of *FTC* v. *Odysseus Marketing,* we filed suit against the operator of the Web site Kazanon.com for allegedly encouraging consumers to download software that the defendants falsely claimed would allow consumers to engage in anonymous P2P file sharing.

In both cases, the defendants entered into settlement agreements that prohibit the alleged misrepresentations and required them to disgorge their ill-gotten gains.

Educating consumers and businesses of the potential risks of file sharing is vital. In July 2003, the FTC issued a consumer alert warning consumers about these risks, including the risk of inadvertently sharing sensitive files and of receiving spyware, viruses, copyright-infringing materials, and unwanted pornography.

The alert, which we updated this past December, recommends that consumers carefully set up file-sharing programs so that they don't open access to information on their hard drives, such as tax returns, e-mail messages, medical records, photos, or other personal documents. The consumer alert has been accessed on our Web site over 1.3 million times.

In addition, the FTC's general Internet education Web site, OnGuardOnline.gov, contains information about the risks of P2P file sharing, including quick fax, an interactive quiz, and additional resources and lessons from i-SAFE, an organization that educates children and teens about Internet safety.

The FTC will continue to assess the risks associated with P2P file sharing, education consumers, monitor and encourage industry self-regulation, and investigate and bring law enforcement actions when appropriate. In particular, we are closely examining the findings of the PTO report to determine if Commission involvement is appropriate.

Thank you. I look forward to your questions.

[The prepared statement of Ms. Engle follows:]

Prepared Statement of

The Federal Trade Commission

Before the

Committee on Oversight and Government Reform
United States House of Representatives

Washington, D.C.

July 24, 2007

I. Introduction

Chairman Waxman, Ranking Member Davis, and members of the Committee on Oversight and Government Reform, I am Mary Engle, Associate Director for Advertising Practices at the Federal Trade Commission (the "Commission" or "FTC"). I appreciate this opportunity to provide an update regarding the Commission's work involving Peer-to-Peer ("P2P") file-sharing technology issues.[1]

As the federal government's principal consumer protection agency, the Federal Trade Commission has a broad mandate to prevent unfair and deceptive acts or practices in the marketplace. The FTC is the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy.[2] The agency enforces laws that prohibit business practices that are harmful to consumers because they are anticompetitive, deceptive, or unfair, and it promotes informed consumer choice and understanding of the competitive process.

Although P2P technology confers significant benefits, such as allowing for faster file transfers, conserving bandwidth and storage requirements, and saving on maintenance and energy costs, it also has been associated with risks to consumers.[3] When consumers download and use

---

[1] The written statement presents the views of the Federal Trade Commission. Oral statements and responses to questions reflect the views of the speaker and do not necessarily reflect the views of the Commission or any Commissioner.

[2] The FTC has broad law enforcement responsibilities under the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq.* With certain exceptions, the statute provides the agency with jurisdiction over nearly every economic sector. Certain entities, such as depository institutions and common carriers, as well as the business of insurance, are wholly or partly exempt from FTC jurisdiction. The agency has enforcement responsibilities under more than 50 statutes and more than 30 rules governing specific industries and practices, in addition to the FTC Act.

[3] *See, e.g., P2P File-Sharing Technology: Consumer Protection and Competition Issues*, Federal Trade Commission Staff Report (June 2005).

P2P file-sharing software programs, they face risks such as downloading spyware or adware programs that come bundled with some P2P file-sharing programs, or receiving files infected with viruses that could impair the operation of their personal computers. In addition, through their use of P2P technology, consumers may unintentionally share personal or other sensitive files residing on their hard drives. Individuals also risk receiving or redistributing files that may subject them to civil or criminal liability under laws governing copyright infringement and pornography. Finally, because of the way some files are labeled, consumers, including children, may be exposed to unwanted pornographic images.

Over the past three years, the FTC has worked to address the risks to consumers presented by P2P file-sharing software programs through three key efforts. First, FTC staff have worked with industry to improve the disclosure of risk information on P2P file-sharing web sites so that consumers can make informed choices regarding their use of P2P file-sharing programs. Second, the FTC has brought law enforcement actions related to P2P file-sharing programs against particularly egregious actors. Finally, the agency has taken steps to educate consumers and businesses about the risks associated with these programs and provide guidance so that they are better able to protect themselves.

I. FTC's Involvement with Peer-to-Peer File-Sharing Technology Issues

A. Policy Development – Peer-to-Peer File-Sharing Technology Workshop

As part of the FTC's ongoing efforts to examine consumer issues relating to new technologies, in December 2004, the FTC held a two-day public workshop to consider the consumer protection, competition, and intellectual property issues raised by P2P file-sharing. The workshop included seven panels featuring more than 40 representatives from the P2P file-

sharing software industry, entertainment industry, high-technology research firms, government agencies, academic institutions, and consumer groups. Participants explored such topics as how P2P file-sharing technology works and what risks consumers may face when using this technology. Panelists and commenters also discussed efforts by both the government and private sector to address some of these risks.

In June 2005, the FTC released a staff report based on the information received in connection with the workshop.[4] The report analyzed a wide range of public policy issues relating to P2P file-sharing programs. The FTC staff concluded that P2P file-sharing, like many other consumer technologies, is a "neutral" technology. That is, its risks result largely from how individuals use the technology rather than being inherent in the technology itself.

The staff report emphasized that many of the risks to consumers associated with P2P file-sharing are not unique, but also exist when consumers engage in other Internet-related activities such as surfing web sites, using search engines, downloading software, and using e-mail or instant messaging. At the Commission's workshop, participants offered conflicting views as to whether the risks arising from P2P file-sharing were greater than other Internet-related activities. For example, one commenter argued that P2P file-sharers were substantially more likely to be infected with spyware than Internet users in general.[5] In contrast, one participant opined that the

---

[4] *P2P File-Sharing Technology: Consumer Protection and Competition Issues*, Federal Trade Commission Staff Report (June 2005), available at www.ftc.gov/reports/p2p05/050623p2prpt.pdf.

[5] *See id.*, Comment 9, The CapAnalysis Group (citing Stefan Saroiu, Steven D. Gribble, Henry M. Levy, "Measurement and Analysis of Spyware in University Environment" (Mar. 2004) (finding that spyware infection rate among university computers using KaZaA file-sharing software was 5 to 22 times greater than infection rates among computers using the Internet alone)).

spyware risks are the same, because those risks are attributable to problems with the design of Windows-based operating systems. Overall, however, workshop participants submitted little empirical evidence concerning the relative risks arising from P2P file-sharing compared to the risks from other Internet-related activities.

In the report, the staff recommended that industry decrease risks to consumers through technological innovation and development, industry self-regulation (including improved risk disclosures), and consumer education. The report also recommended that government investigate and bring law enforcement actions when warranted, work with industry to encourage self-regulation, and educate consumers about the risks associated with using P2P file-sharing software. Finally, the report recommended that policymakers balance the protection of intellectual property and the freedom to advance new technologies, thereby encouraging the creation of new artistic works as well as economic growth and enhanced business efficiency.

B. Review of Peer-to-Peer File-Sharing Program Risk Disclosures

In response to industry complaints and Congressional inquiries,[6] in 2004, FTC staff reviewed the risk disclosures on the web sites of the ten most popular P2P file-sharing program distributors to determine if the web sites misrepresented or failed to disclose risks associated with downloading and using their programs. Commission staff concluded that, although the risk disclosures were not false or misleading, they could be improved. Accordingly, in summer 2004, the Commission staff sent letters to the ten largest distributors of P2P file-sharing programs

[6] *See, e.g.,* Letter from the Committee on Government Reform, United States House of Representatives, to Timothy Muris, Chairman, Federal Trade Commission (Aug. 10, 2004) (on file with the Commission) (expressing concerns about the risks posed by P2P file-sharing programs).

recommending that the distributors better inform consumers about the risks inherent in downloading and using P2P file-sharing programs.[7] As additional guidance to these distributors, the staff enclosed copies of the FTC's brochure for consumers about the risks of file-sharing and the FTC's business guidance document addressing how to disclose information online.[8]

In December 2004, the two main P2P industry trade associations at that time, P2P United and the Distributed Computing Information Association, both announced self-regulatory measures under which member P2P file-sharing program distributors would disclose risk information on their web sites and during the installation process, including warnings about copyright infringement, data security, unwanted exposure to pornography, spyware, and viruses.[9] Since then, FTC staff has periodically reviewed P2P file-sharing programs and download sites to

---

[7] *See* Letter from Mary K. Engle, Associate Director, Division of Advertising, Bureau of Consumer Protection, to P2P file-sharing distributors (June and July 2004, on file with the Commission).

[8] *See Dot Com Disclosures: Information About Online Advertising,* available at www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf.

[9] *See P2P File-Sharing Technology: Consumer Protection and Competition Issues*, Federal Trade Commission Staff Report (June 2005), at pp. 17-18 and Appendix B and C. Whereas the P2P United Code of Conduct announced in 2003 only touched on risk disclosures regarding copyright infringement and the exposure to children of inappropriate file content, the self-regulatory measures that P2P United announced in December 2004 contained detailed descriptions of the risk disclosures that members promised to make concerning copyright infringement, data security, unwanted exposure to pornography, spyware, and viruses. The Code of Conduct also covered principles beyond the scope of risk disclosures, including members' commitments to only install P2P software after receiving a user's informed consent and to provide an uninstall tool; to require confirmation of which folders the user wishes to make available to others; to design P2P software to prevent the inadvertent designation of the user's entire hard drive as material available to other users; to comply with the Children's Online Privacy Protection Act; to cooperate with government agencies to combat child pornography; to post privacy principles; to incorporate features, where technically feasible, into their software that enable adults to restrict use of the software to certain members of the household; and to not disclose information about the user. P2P United is no longer in existence.

monitor industry implementation of its risk-disclosure promises. In addition, in 2005, the FTC sent letters to P2P file-sharing distributors reminding them of their commitments to comply with the industry self-regulatory program.[10] FTC staff's reviews have confirmed that the major P2P file-sharing programs steadily improved their risk disclosures. In March 2006, FTC Chairman Deborah Platt Majoras sent interested members of Congress an update on the staff's most recent review of P2P sites.[11] In summary, as of March 2006, only one major operating P2P site, Blubster, failed to make the promised risk disclosures. Blubster is located in Spain, and Commission staff referred its findings to the appropriate consumer protection authorities there.

The FTC staff also has reviewed P2P sites to determine if they were failing to disclose bundled adware or spyware. As part of that investigation, in fall 2005, the FTC staff downloaded and installed the ten largest P2P file-sharing programs to determine whether P2P file-sharing program distributors were bundling adware or spyware with their programs and, if so, whether the distributors were disclosing that fact. Of those ten programs, eight either did not contain any bundled spyware or adware, or contained bundled adware but disclosed that fact. Of the two programs that did not disclose bundled spyware or adware, one is no longer being distributed, and the other has been referred to foreign consumer protection authorities.

---

[10] *See, e.g.*, Letter from Lydia B. Parnes, then-Acting Director, Bureau of Consumer Protection, Federal Trade Commission, to P2P file-sharing distributors (Mar. 1, 2005, on file with the Commission).

[11] *See, e.g.*, Letter from Deborah Platt Majoras, Chairman, Federal Trade Commission, to Henry Waxman, Member of the House of Representatives (Mar. 6, 2006) (on file with the Commission).

A. FTC Law Enforcement Actions Involving Peer-to-Peer File-Sharing

In addition to protecting consumers by encouraging the disclosure of risk information, the FTC has brought two successful law enforcement actions related to P2P file-sharing programs. In *FTC v. Cashier Myricks Jr.*,[12] the Commission filed suit against the operator of the web site MP3DownloadCity.com for making allegedly deceptive claims that it was "100% LEGAL" for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games. The defendant entered into a settlement agreement with the FTC that barred misrepresentations about P2P file-sharing products or services, required the operator to disclose the civil and criminal liability risks of downloading copyrighted material without the owner's permission, and required the operator to refund more than $15,000 to the customers he allegedly duped into buying memberships to the web site.

In *FTC v. Odysseus Marketing, Inc.*,[13] the FTC filed suit against the operator of the web site Kazanon.com. According to the FTC's complaint, the defendants encouraged consumers to download free software that they falsely claimed would allow consumers to engage in anonymous P2P file-sharing. The FTC also alleged that the defendants deceptively failed to disclose that their free software installed spyware and adware on consumers' computers. The defendants entered into a settlement agreement with the FTC that prohibits secret downloads in the future, prohibits the operators from exploiting security vulnerabilities to download software, and bars future misrepresentations. In addition, the defendants agreed to disgorge their alleged ill-gotten gains.

---

[12] Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sept. 27, 2005).

[13] Civ. No. 05-330 (D.N.H., filed Sept. 21, 2005)

Combating twenty-first century consumer protection issues such as P2P file-sharing requires cutting-edge, twenty-first century law enforcement tools. For example, the FTC maintains Consumer Sentinel, a secure, online fraud and identity theft complaint database. Consumer Sentinel contains over 3.9 million fraud and identity theft complaints and is accessible to more than 1,650 law enforcement agencies, which use the database to share information, coordinate investigations, and pursue case leads. The FTC also has an Internet Lab, which provides FTC lawyers and investigators with high-tech tools to investigate high-tech consumer problems. It allows investigators to search for fraud and deception on the Internet in a secure environment. To capture web sites that come and go quickly, the lab also provides FTC staff with the necessary equipment to preserve evidence for presentation in court.

B. Consumer and Business Education

Education of consumers and businesses is integral to the Commission's consumer protection mission. With respect to P2P issues, the FTC has sought to inform consumers of the potential risks of file-sharing so that they can better protect themselves. In July 2003, the FTC issued a consumer alert entitled, "File-Sharing: A Fair Share? Maybe Not."[14] The alert warns consumers about the potential risks from downloading and using P2P file-sharing software, including the risk of inadvertently sharing files or receiving spyware, viruses, infringing materials, or unwanted pornography mislabeled as something else. The alert recommends that consumers carefully set up the file-sharing software, checking the proper settings when the software is installed, so that consumers do not open access to information on their hard drives

[14] The FTC updated and renamed this consumer alert in December 2006. *See P2P File-Sharing: Evaluate the Risks*, available at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm.

such as tax returns, e-mail messages, medical records, photos, or other personal documents. It also recommends that consumers run trusted anti-spyware and anti-virus programs on a regular basis if they are using P2P file-sharing programs, and that consumers close their Internet connections when not online to prevent file-sharing from continuing at any time. The consumer alert has been accessed on the FTC's web site over 1.3 million times since it was released.

In addition, the FTC's Internet education web site, OnGuardOnline.gov, contains downloadable information about the risks of P2P file-sharing software, including quick facts about P2P file-sharing, an interactive quiz, and additional lessons, resources, and activities from i-SAFE, an organization involved in Internet-safety education.[15] OnGuardOnline.gov is an innovative multimedia web site designed to educate consumers about basic computer security practices. OnGuardOnline has become the hallmark of the Commission's larger cybersecurity campaign. The site is built around seven timeless tips about online safety,[16] and information on topics such as P2P file-sharing, social networking, identity theft, phishing, spyware, and spam. OnGuardOnline features up-to-date articles from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), including a piece entitled "Risks of File Sharing."

OnGuardOnline serves about 250,000 unique visitors each month. The site, which was developed through a partnership with cybersecurity experts, consumer advocates, online marketers, and other federal agencies, is an excellent example of public-private cooperation. The

---

[15] *See* www.onguardonline.gov.

[16] Such tips include: protect your personal information; know who you are dealing with; user security software and a firewall; make sure your operating system and web browser are set up properly; protect your passwords; back up important files; and learn who to contact if something goes wrong online.

agency deliberately branded OnGuardOnline independently of the Federal Trade Commission to encourage other organizations to make the information their own and to disseminate it in ways that reach the most consumers.

As stated above, none of the risks associated with P2P file-sharing programs is exclusive to that technology. For example, P2P file-sharing is just one technology by which personal data can be unintentionally disclosed. Thus, other consumer and business education outreach initiatives that the FTC has undertaken apply equally in the P2P file-sharing arena. For example, the FTC recently published a general data security business education guide, *Protecting Personal Information, A Guide for Businesses*,[17] designed to assist different types of businesses in addressing data security issues. In that publication, the Commission recommends a sound data security plan built on five key principles: know what personal information you have in your files and on your computers ("Take stock"); keep only what you need for your business ("Scale down"); protect the information that you keep ("Lock it"); properly dispose of what you no longer need ("Pitch it"); and create a plan to respond to security incidents ("Plan ahead"). Many of these same methods of securing personal data will help prevent the inadvertent disclosure of that data caused by P2P file-sharing programs.

In addition, the FTC's online publication *Dot Com Disclosures: Information About Online Advertising*, provides guidance to businesses regarding how to make clear and conspicuous disclosures online.[18] This publication received almost 70,000 unique visitors last

---

[17] Available at www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf.

[18] *See Dot Com Disclosures: Information About Online Advertising,* available at www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.pdf.

year. As mentioned earlier, the FTC provided copies of this publication to the ten largest distributors of P2P file-sharing programs to guide them in better informing consumers about the risks inherent in downloading and using P2P file-sharing programs.

III. Conclusion

The FTC will continue to assess the risks associated with P2P file-sharing technology, educate consumers, monitor and encourage industry self-regulation, and investigate and institute law enforcement actions when appropriate in the P2P file-sharing arena. The FTC thanks this Committee for the opportunity to describe how the FTC has addressed the consumer protection issues raised by P2P file-sharing technology.

Chairman WAXMAN. Thank you very much, Ms. Engle.
Mr. Mintz.

STATEMENT OF DANIEL G. MINTZ

Mr. MINTZ. Mr. Chairman, Ranking Member Davis, and members of the committee, I would like to thank you for the opportunity to appear today to discuss the important issue of peer-to-peer file sharing and briefly mention an incident that occurred at the Department, and to talk about some of the actions we have been taking, both on an ongoing basis and in response to the incident.

My name is Dan Mintz. I am the Chief Information Officer for the Department of Transportation, where I have been since May 1, 2006. I came to the Government from SUN Microsystems, where I chaired a corporate-wide team that studied the protection of sensitive Government information within SUN's corporate systems. The lessons learned from that experience have proven valuable during my time at the Department.

Responsible peer-to-peer software can provide Government agencies with many benefits, including increased productivity and efficiency. Unfortunately, it also poses a significant risk to agencies' systems and networks and information, as well as to home computers, and problems with peer-to-peer software can be difficult to detect.

A few incidents have occurred within Government recently. One involved a Department of Transportation employee, when her child, a teenager, unbeknownst to the employee, downloaded software on the employee's personal computer. The daughter did not realize this would expose information on the family computer to others using the same or compatible software.

These incidents illustrate the challenges we face and the need for due diligence on all of our parts. At the Department we are continually improving overall security. We have policies in place regarding file sharing, and we have a training program already that emphasizes these policies. At the same time, I wanted to mention five areas where we are doing work related to this.

First, we are performing an in-depth review of the security architecture that we have now integrated at our Department's new headquarters building at the Southeast Federal Center that we just finished moving into, and consolidating what had been individually managed networks run by each of the departmental operating administrations.

Second, we are working with the Federal Aviation Administration to combine our two separately managed incident reporting centers into a single center to create an integrated approach for Department-wide monitoring of such incidents.

Third, we are doing a review of the policies. We have asked the Department's IG to work with us to examine the policies and determine which ones are being effective right now, need auditing, and which ones where there are gaps that we need to fill in terms of the overall policies.

Fourth, relating to telework, we are expanding our emphasis to move our employees to laptops. Right now the vast majority of employees have desktops; only a small percentage have laptops. We want to increase the percentage of laptops which, by policy and by

practice, are encrypted, away from the traditional desktop configurations. In this fashion, we will increase the percentage of employees, when they do work at home, to be using Government-owned equipment and Government-owned equipment that is encrypted.

Fifth, we will be improving the messaging regarding peer-to-peer software to new employees, and particularly those who are involved in our telework program. We find that the issues we are coming across are, in large part, cultural as well as they are technological.

In closing, progress has been made at DOT in managing these threats stemming from peer-to-peer file sharing, but we will have to remain vigilant in educating our employees about these dangers and developing and implementing policies, procedures, and technologies which will safeguard the networks and our sensitive data. We also need to recognize that, regardless of the policies we write and put in place and how we make these policies available to our employees, we have to continually audit their performance and how they are used and reinforce them in order to have them be effective.

Again, I would like to thank you for the opportunity to comment on the topic and I look forward to answering any questions that you have.

[The prepared statement of Mr. Mintz follows:]

TESTIMONY OF DANIEL G. MINTZ
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF TRANSPORATION
BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

July 24, 2007

Mr. Chairman, Ranking Member Davis, and Members of the Committee, thank you for the opportunity to appear today to discuss the important issue of Peer-to-Peer (P2P) file sharing.

My name is Dan Mintz; I have been the Chief Information Officer (CIO) for the Department of Transportation (DOT) since May 1, 2006. My responsibilities include serving as the Senior Agency Official for Privacy (SAOP) and the Secretary's lead for the Department's Identity Theft Task Force. I came to the Government from Sun Microsystems. During my last year at Sun, I chaired a corporate-wide team that studied protection of Federal Government sensitive information within Sun's corporate information systems. The lessons learned from that experience have been of substantial use during my time at the Department of Transportation.

The incident that I will discuss shortly that affected one of my own staff is a classic example of what the Committee has been warning about. Mr. Chairman, as early as May 2003, you said in a statement to this Committee that, "The users of file-sharing programs are predominantly teenagers. We parents and grandparents are too often left struggling to keep up." In my staff member's case, her teenage daughter downloaded LimeWire without informing her parents. LimeWire is a free and readily available

software program that facilitates peer-to-peer file sharing. The result was that a number of Government documents were accessed remotely by a Fox News reporter.

I would like to briefly discuss the Department's approach to security and explain the policies we have put in place relating to P2P software, provide an overview of the P2P incident involving my staff member and, finally, summarize the lessons learned and associated actions we are taking to minimize the likelihood of such incidents occurring in the future.

DOT Policy Efforts as a Result of Federal Information Security Management Act (FISMA) and P2P Software

The Department's Information Assurance Program has made steady progress in recent years to reinforce existing and introduce new security program measures to mitigate the impact of the potential risks posed by P2P applications and other vulnerabilities.

The Department's FISMA score went from a C- in FY05 to a B in FY06 based on these and related steps. However, we continue to be focused on further educating, training, and improving our capabilities in cyber protection particularly as we work to support the Secretary's goal to increase the Department's telework capabilities and capacities.

The Office of Management and Budget's (OMB) inclusion of a question in the annual FISMA reporting requirements regarding department and agency incorporation of policies and training with respect to P2P first began in the FY2005 FISMA reporting cycle.

On May 11, 2006, I issued DOT Information Technology and Information Assurance Policy Number 2006-17: Peer-to-Peer (P2P) Software Policy. This policy

provided updated procedures and assigned responsibilities for ensuring protection against security incidents related to Peer-to-Peer (P2P) software applications. Complementing the issuance of this policy, the Department's annual security awareness training program was updated to include information discussing the vulnerabilities associated with the use of P2P file sharing software as part of the annual training material.

I would like to emphasize two key provisions of our current P2P policy:

- DOT users are not authorized to install or use software applications on DOT computers and networks unless expressly authorized in writing by my office. Written authorization must be provided prior to installation of P2P software, if the need has been determined to allow the use of P2P.
- All DOT networks are monitored to identify the use of P2P software. If the use of P2P software is identified and if no written authorization exists for the use of the software, it will be removed immediately and appropriate disciplinary action should be considered.

As further background on our policy approach, the Department issued its first policy and guidelines addressing P2P file sharing applications on November 7, 2003, two years before this issue was included in the annual FISMA reporting requirements. In September, 2004, OMB issued guidelines for the use of file sharing technology. The Department's initial policies and later updates responded to those guidelines including: creating policies, training, and implementing security controls.

DOT Efforts to Manage Peer-to-Peer (P2P) Software Usage

P2P software poses a significant risk to Departmental systems and networks as well as home computers. Others will focus on the details of how such software works and its potential impact, therefore, I will not deal with those topics here.

However, I do want to point out that peer-to-peer networks can be difficult to detect by intrusion detection systems (IDS), and most firewalls do not stop peer-to-peer traffic, because the peer node on the inside of the firewall initiates a connection to other peers. Once the internal node connects to an external network, any other peer node in the world will have access to the user's desktop. Since the user desktop is a portal to critical DOT assets and resources, the internal peer node could provide any user in the world access to DOT systems.

Moreover, the current method of detecting P2P is through the installed base of Intrusion Detection Systems, which is less than perfect. The detection of P2P traffic using network based IDS's generates numerous false positive alerts, because the detection approach is to look at specific ports on the network for P2P activity. Often legitimate software will utilize the same ports that P2P software is traditionally seen on, creating a false positive alert.

Security incidents at the Department are recorded and managed by the Transportation Cyber Incident Response Center (TCIRC). The TCIRC provides the Department's IT infrastructure cyber-situational awareness. It is also the sole organization that coordinates and correlates all cyber-events with the Department of Homeland Security. The TCIRC is used by my office for major portions of FISMA

compliance reviews and maintains a continuous monitoring capability to address the cyber-health and welfare of the DOT information technology (IT) systems and network.

The TCIRC treats detected P2P activity just as it does any other cyber security issue. When P2P activity is identified, the TCIRC staff use several tools in an attempt to identify the offending system. After identifying the offending system, the TCIRC works with security staff to identify the physical location of the system and take action to remove the system from the network and remove the P2P software from the system. It is current TCIRC policy that all P2P activity identified on any DOT system be reported to the United States Computer Emergency Readiness Team (US-CERT). US-CERT is a partnership between the Department of Homeland Security and other public and private sectors established in 2003 to help protect the nation's Internet infrastructure.

DOT cannot restrict the use of peer-to-peer software on personal laptop or desktop computers. However, DOT policy prohibits employees and contract staff from using, processing, storing, or accessing DOT information or systems if P2P software is installed or suspected of being installed on an employee's personal computer.

Overall, DOT maintains a constant vigilance on any cyber event that could cause harm to our networks. P2P detection is one of those events.

DOT Implementation of OMB Policies

There are two policies that OMB has issued that DOT uses to provide guidance regarding protecting and responding to breaches of personally identifiable information, M-06-16, issued June 2006, and M-07-16 issued May 2007. As part of on-going security

and privacy efforts, DOT has worked to implement the requirements of OMB M-06-16 and OMB M-07-16. Specifically, we have:

- Established a departmental policy for the protection of personally identifiable information (PII) and sensitive personally identifiable information (SPII), including core requirements for encryption of SPII at rest, in transit and in store.
- Created the procedures described above for handling incidents involving the suspected or confirmed loss of personal information.
- Surveyed all IT system owners on the administrative, technical, and physical safeguards in place to protect personal information. The 2007 system survey is currently underway as part of our broad review of PII holdings.
- Deployed a best-in-class FIPS 140-2 compatible encryption solution on all Department laptops.
- Established a senior official team to respond to large-scale breaches.
- Moved to reduce the unnecessary collection and use of Social Security Numbers in programs and systems, and to mask those numbers whenever possible, if their use or collection is necessary.
- Initiated the revision of policies and procedures to reflect new requirements aimed at preventing and responding to breaches involving PII.
- Selected a solution for providing enhanced security training to all employees and contractors involved in the handling of PII and launched annual privacy awareness training.

- Used broadcast messages and other mechanisms to remind employees and contractors of new security and privacy issues and to remind them of their responsibilities to safeguard personal information.

While we have made important strides at DOT in the area of privacy and security protection, we are reminded by incidents, such as the P2P event, that we must remain vigilant about keeping employees informed of new threats as well as instituting new policies, procedures, technologies and tools to protect the data that resides on our networks.

DOT P2P Incident

My staff member, like many employees at the Department of Transportation, performs work at home. She does so because she has received approval to telework and also because there are times when she needs to perform work in the evenings or on weekends.

In about March of this year, her teenage daughter downloaded LimeWire—most likely to share music or similar files—without at the time informing her parents. In early May, a news reporter for Fox News accessed my employee's personal computer and several Government documents.

On May 4th, the reporter contacted my staff member by email, and informed her that he had accessed her personal computer and a number of Government-related documents. She contacted her manager, who reports to me, and we put her in touch with the DOT Office of the Inspector General (DOT OIG).

As part of their investigation, the DOT OIG performed a forensics analysis on the thousands of files on her computer, and identified approximately 93 DOT-related

documents and approximately 260 National Archives-related documents, where she worked before coming to DOT in January 2007. Not all of those documents were publicly accessible at the time. The OIG has found that 30 of the approximately 93 DOT-related documents were publicly accessible at the time via LimeWire or other P2P software by virtue of residing in a "shared folder," while 36 of the approximately 260 National Archives-related documents were in a shared folder and thus publicly accessible. None of the DOT documents identified contained sensitive personally identifiable information (SPII) about any other employee other than my staff member herself.

The DOT OIG has briefed me on their investigation and is completing a final report. Assuming nothing unexpected turns up as the DOT OIG concludes its review, we are planning to close the incident without a formal personnel action. The person in question has been an excellent and valued employee at the Department; she made a mistake. While we do not believe that disciplinary or other personnel action involving our employee is warranted, the CIO Office has assigned her a number of tasks directly related to reviewing current policies on home computer use and potential problems associated with peer-to-peer networking and providing recommendations for strengthening these policies. In addition, the employee will assist in developing appropriate training for agency employees concerning the proper handing of SPII.

Lessons Learned

In many ways, this incident and the nature of the people involved illustrate the challenges we face and the need for continuing due diligence on all of our parts. An incident occurred involving an employee who has consistently performed well and

approached her work in a professional manner, at a Department that has been improving its overall security, with policies in place that cover these issues in general and P2P specifically, and a training program that emphasizes these policies.

Yet, in this case, none of these were sufficient to prevent access to Government documents when a young family member downloaded software that she did not realize would be capable of exposing these documents to anyone else using the same or compatible software.

In response to this, the Department will be taking a number of initiatives that we strongly believe will both make the security infrastructure more robust and more aggressively make these issues more visible to DOT staff. The first three are broad initiatives dealing with the overall security organization and policy, the remainder deal with specifics relating to P2P.

First, we are performing an in-depth review of the security architecture that has now been integrated at the Department's new headquarters building at the Southeast Federal Center (SEFC). Historically, the Department has had individually managed networks run by each Departmental agency. Administrative rights policies, hardware and software configurations, and network implementations were often inconsistent and inconsistently applied. The Department has committed to follow the recently promulgated standards for Microsoft Operating Systems put together by the Air Force, Microsoft, and OMB, and will shortly be putting in place rules and a transition strategy to simplify the overall network. This, plus the installation of centrally managed network security software, will make us better able to monitor the usage of permitted software and detect the usage of non-approved P2P software.

Second, the Federal Aviation Administration and the rest of the Department are moving to merge the two incident centers that each currently separately manages to create a single, integrated approach for Department-wide monitoring. This will make more efficient use of Departmental resources and establish an additional step in increasing the security posture to monitor these kinds of incidents.

Third, we have asked the DOT OIG to work with us in reviewing the totality of the policies that currently exist and help us determine which ones are effective and where there are gaps in the policy that need to be filled.

Fourth, we are expanding our emphasis to move employees to laptops from their more traditional desktop configurations. In this fashion, we will increase the percentage of employees who have Government owned equipment at home. And by policy and practice, all laptops are encrypted with FIPS 140-2 compatible Department of Transportation provided software. Agencies of the Department, such as the Federal Railroad Administration and the Pipeline and Hazardous Materials Safety Administration have already moved many of their employees to laptops. We will work with the DOT Telework Committee to identify those employees who have already been approved for telework plus those that would likely be key participants in any Continuity of Operations (COOP) event and be the first candidates to move to laptops when we perform a desktop refresh.

Fifth, we will be implementing a number of steps to improve the messaging regarding P2P to new employees and in particular those who will be involved with telework.

- We will prepare examples of home desktop configuration guides that teleworkers can use to set-up their home PC. While these will only be guidelines, it is clear that home workers are looking for advice on how to secure their systems. As a supplement to our current annual security training for all DOT employees, we will be creating telework specific training which will include information on threats facing home PCs.
- Finally, we will ask all employees upon their departure from the Department to verify that all Departmental information has been removed from the employee's home computer.

Summary

In conclusion, it is my observation and experience at DOT that while progress has been made in managing threats stemming from P2P file sharing, we must remain vigilant about educating our employees about these dangers and developing and implementing policies, procedures and technologies aimed at safeguarding our networks and sensitive data. At the same time, we must balance this vigilance against the many positive, legitimate uses of P2P for improving government efficiency and productivity.

Finally, we need to recognize that regardless of the policies that we put in place and how we make those policies available to our employees, the continual audit of their effectiveness and continual reinforcement of our policy goals will in large part determine their effectiveness.

Again, I thank you for the opportunity to comment on this important topic, and I look forward to answering any questions that you may have.

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

STATEMENT OF M. ERIC JOHNSON

Mr. JOHNSON. Chairman Waxman and Ranking Member Davis and members of the committee, I am Eric Johnson and it is a great honor to testify here today.

You might wonder why is a business professional studying peer-to-peer security threats. First, let me be clear: I have no financial stake in the security industry, nor have I accepted funding from the recording industry. I became interested in peer-to-peer security risks as part of my ongoing research on information security in large corporations.

My research center, the Center for Digital Strategies at the Tuck School of Business at Dartmouth, is focused on the problems facing chief information officers of Fortune 500 companies. In 2002, with Cisco Systems, we founded the Thought Leadership Roundtable on Digital Strategies to bring CIOs together to talk about shared business problems.

Over the past 5 years, security and trust have consistently been at the top of many CIOs' agendas, so as part of the I3P Research Consortium and through grants from the Department of Homeland Security, NIST, and the Department of Justice, we have been researching the challenges of information security in large, extended enterprises.

For example, with the DHS funding we have been conducting workshops for chief information security officers and, driven by the key issues raised in those discussions, we have focused much of our attention on information leakage and inadvertent disclosure.

Today we examine a common but widely misunderstood source of inadvertent disclosure, peer-to-peer file sharing.

In the next few minutes I will summarize the results of two of my research papers, one that is forthcoming and one that has already been published in a peer-reviewed scientific publication.

First, to illustrate the threat of P2P file sharing, we ran a set of honey pot experiments in conjunction with Tiversa. We posted the text of an e-mail containing an active Visa debit number and AT&T phone card in a music directory that was shared via LimeWire. We observed the activity on the file and tracked it across the P2P network. By the end of the first week, the Visa card had been used and its balance depleted. We observed its use through the accounts transaction statement posted by Visa on the Web.

Not knowing the exact balance of the card, the users used PayPal and Nochex, both processors of online payments, to drain the funds from the card.

Within another week, the calling card was also depleted. Examining the call records, all the calls were made from outside the United States into two U.S. area codes in the Bronx and Tacoma. This illustrates the threat both within and outside the United States.

And even more interesting, long after we stopped sharing the files, they kept moving, continuing to new clients as they were leaked over and over again.

In our second study we examined bank-related documents we found circulating on peer-to-peer networks over a 2-month period. Focusing on the Forbes Top 30 U.S. banks, we collected and analyzed their user-issued searches and leaked documents. First we found an astonishing number of searches targeted to uncover sensitive documents and data. For example, a user-issued search for Bank of America data base, Wachovia Bank online user ID, or CitiBank balance transfer. Now, keep in mind these were searches issued in music-sharing networks, not the worldwide Web. Such directed searches clearly illustrate the intent of finding some confidential information.

Next we examined thousands of bank-related documents circulating on the networks. Many of the documents were customer related, leaked by the customers, themselves, such as statements, dispute letters, completed loan application forms. Typically these documents contained enough information to easily commit identity theft or fraud.

We also found business documents leaking from the banks' employees and suppliers, including performance evaluations, customer lists, spreadsheets with customer information, and clearly marked confidential bank material.

From our sample of banks, we analyzed tens of thousands of relevant searches and documents, and we found a statistically significant link between the linkage and the firm employment base.

We also found that, for many firms, coincidental association with a popular song brand or venue represented another problem we called digital wind. Millions of searches for that song increased the likelihood of exposing a sensitive bank document. Either by mistake or by curiosity, these documents are exposed and sometimes downloaded to other clients, thus spreading the file and making it more likely to fall into the hands of those who will try to exploit it.

For example, someone looking for a live performance from the Wachovia Center would likely find documents related to the bank. Likewise, the popular rap singer PNC creates wind for PNC Bank. Such digital wind increases the P2P security threat for many organizations.

Thank you.

[The prepared statement of Mr. Johnson follows:]

Testimony of Professor M. Eric Johnson

Director, Center for Digital Strategies
Tuck School of Business
Dartmouth College

Before the

Committee on Oversight and Government Reform

United States House of Representatives

on

Inadvertent File Sharing Over Peer-to-Peer Networks

July 24, 2007

Introduction

Chairman Waxman, Ranking Member Davis, and members of the committee, it is an honor to testify before you today about this important national security issue.

Peer-to-peer (P2P) software clients have become part of the standard suite of PC applications for many users. With millions of users world-wide sharing music, video, software, and pictures, file movement on these networks represents a significant percentage of internet traffic. Beyond the much discussed copyright infringement issues, P2P networks threaten both corporate and individual security. Our research shows that confidential and potentially damaging documents have made their way onto these networks and continue to do so. The research also shows that criminals trawl P2P networks and opportunistically exploit information that they find.

You might wonder why a business professor is studying P2P security threats? First, let me be clear that I have no financial stake in the P2P security industry nor have I accepted any funding from the recording industry. I became interested in P2P security risks as part of my ongoing research on information security in large corporate enterprises. My research center, the Center for Digital Strategies, at the Tuck School of Business at Dartmouth, is focused on the problems facing Chief Information Officers (CIOs) in global 1000 firms. In 2002, we founded, with Cisco Systems, the Thought Leadership Roundtable on Digital Strategies to bring together CIOs to discuss shared business problems. Over the past five years, security and trust have consistently been at the top of many CIOs agendas. So, as part of the I3P research consortium and through grants from the Department of Homeland Security (DHS), NIST, and the Department of Justice, we have been researching the challenges of information security in large

extended enterprises. With the DHS funding, have been conducting workshops for Chief Information Security Officers (CISOs) and driven by the key issues raised in those discussions (Johnson and Goetz 2007), we have focused much of our attention on information leakage and inadvertent disclosures. Today, we examine a common, but widely misunderstood source of inadvertent disclosure: peer-to-peer file sharing networks.

In the next few minutes, I will summarize the results of two of my recent and forthcoming research articles, published in peer-reviewed, scientific publications (Johnson et al 2007, Johnson and Dynes 2007). First, to illustrate the threat of P2P file sharing, we ran a set of "honey-pot" experiments in conjunction with Tiversa, Inc. We posted the text of an email message containing an active VISA (debit) number and an AT&T phone card in a music directory that was shared via Limewire. We observed both the activity of the file on our client and further tracked the file's movement across the P2P network. The file was quickly taken and retaken by a number of different clients. By the end of one week, the VISA card was used and its balance depleted. We observed its use through the account's transactions statement posted by VISA on the web. Not knowing the exact balance of the card, the taker(s) used Paypal and Nochex (both processors of online payments) to drain funds from the card. It appears that two takers of the card were able to obtain funds as the activity was split into two groups and because one taker used Paypal, which is more US-centric, while the other used Nochex, which is UK-centric. Within another week, the calling card was also depleted. Examining the call records of the card, all of the calls were made from outside of the US to two US area codes - 347 (Bronx, NY) and 253 (Tacoma, WA), illustrating the P2P threat both within

and outside of the US. Even more interesting, long after we stopped sharing the file, we observed the file continuing to move to new clients as some of the original takers leaked the file to others.

In a second study, we examined bank-related documents we found circulating on P2P networks over a two-month period. Focusing on the Forbes top 30 US banks, we collected and analyzed both user-issued searches and leaked documents. First, we found an astonishing number of searches targeted to uncover sensitive documents and data. For example, user-issued searches for "bank of america database", "wachovia bank online user id", or "citi bank balance transfer." Keep in mind, these were searches issued in music-sharing networks – not the world-wide web. Such directed searches were clearly issued with the intent of finding confidential information. Next we examined thousands of bank-related documents circulating on these networks. Many of these documents were customer-related, leaked by the customers themselves, such as bank statements, dispute letters, and completed loan application forms. Typically these docuements contained enough personal information to facilitate identity theft and fraud. We also found business documents leaking from bank employees and suppliers including performance evaluations, customer lists, spreadsheets with customer information, and clearly marked confidential bank material. For our sample of banks we analyzed tens of thousands of relevant searches and documents. We found a statistically significant link between leakage and firm employment base.

We also found that for many firms, coincidental association with a popular song, brand, or venue represented another problem we call "digital wind." Millions of searches for that song increase the likelihood of exposing a sensitive bank document. Either by

mistake or by curiosity, when these documents are exposed, they are sometimes downloaded to other clients, thus spreading the file and making it more likely to fall into the hands of someone who will try to exploit its information. For example, someone looking for a live performance from the Wachovia center would also likely find documents related to the bank. Likewise, the popular music rapper PNC creates wind for PNC bank. Such "digital wind" increases the P2P security threat for many organizations.

We believe that P2P file sharing networks represent a significant and poorly understood threat to business, government, and individuals. Given the nature of the threat, we would argue that many individuals may be experiencing identity theft and fraud without ever knowing the source of their misfortune. Furthermore, we see many of the current P2P trends increasing the problem. We urge both corporate executives and government officials to educate themselves and their constituencies to the risks these networks represent.

References

Johnson, M. Eric and Eric Goetz (2007), "Embedding Information Security Risk Management into the Extended Enterprise," *IEEE Security and Privacy,* May-June, 16-24.

Johnson, M. Eric and Scott Dynes (2007), "Inadvertent Disclosure: Information Leaks in the Extended Enterprise," *Proceedings of the Sixth Workshop on the Economics of Information Security*, Carnegie Mellon University, June 7-8.

Johnson, M. Eric, McGuire, Dan, and Nicholas D. Willey (2007), "Why File Sharing Networks Are Dangerous," forthcoming in *Communications of the ACM.*

Why File Sharing Networks Are Dangerous

M. Eric Johnson, Dan McGuire, Nicholas D. Willey*

Center for Digital Strategies
Tuck School of Business
Dartmouth College,
Hanover NH 03755
{M.Eric.Johnson}@darmouth.edu

Forthcoming in *Communications of the ACM*

Peer-to-peer (P2P) software clients have become part of the standard suite of PC applications for many users. With millions of users world-wide sharing music, video, software, and pictures[1], file movement on these networks represent a significant percentage of internet traffic. Beyond the much discussed copyright infringement issues, P2P networks threaten both corporate and individual security. Our research shows that confidential and potentially damaging documents have made their way onto these networks and continue to do so. The research also shows that criminals trawl P2P networks and opportunistically exploit information that they find.

P2P file sharing represents a growing security threat because of the evolution of these networks. Internet service providers (ISPs), firms, and copyright holders have responded to the rise of P2P both technically (site blocking, traffic filtering and content poisoning[2]) and legally. These challenges have prompted P2P developers to create decentralized, encrypted, anonymous networks that are difficult to track, are designed to accommodate large numbers of clients, and are capable of transferring vast amounts of data.

We analyze the P2P security issues, establishing the vulnerabilities these software clients represent. Then we present experimental evidence of the risk through honey-pot experiments that expose both business and personal financial information and track the resulting consequences. This analysis and experimental results clearly show the security risk of P2P file sharing networks.

---

* We are grateful for the assistance of Tiversa Inc and Scott Dynes of the Center for Digital Strategies at the Tuck School. Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent pending technology that, in real-time, monitors global P2P file sharing networks. This work was supported under Award number 2000-DT-CX-K001 from the Office for Domestic Preparedness, Department of Homeland Security. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security.

Peer-to-Peer File Sharing

Peer-to-peer file-sharing networks enable users to "publish" or "share" files – any file from music to video to spreadsheets. P2P networks provide a ready-made sharing infrastructure that is difficult to block and even harder to track, providing cover for espionage and criminal activity. They encourage users to leave their computers on and connected to the internet at all times, running software that heavily uses their network, disk, and processor. Recent legal battles being won by the content industry (RIAA/MPAA) seem to have done little to really reduce file sharing, but have rather pushed users onto new clients and networks that are even harder to track.

Peer-to-peer file sharing came of age during the dot.com boom and the rise of Napster. Between its debut in 1999 and its eventual failure in 2001, Napster enabled tens of millions of users to easily share MP3-formatted song files with each other. However, its success and failure paved the way for many new P2P file-sharing networks such as Gnutella, FastTrack, e-donkey, and Bittorrent, with related software clients such as Limewire, KaZaA, Morpheus, eMule, and BearShare. This next breed of sharing systems has proven far more difficult to control and a much larger security threat.

A number of firms and internet service providers (ISPs) block or throttle traffic associated with P2P systems using a simple, fast approach known as port filtering. In response, P2P clients responded by using ports associated with other services (web traffic, email traffic, etc.) to exchange data. The P2P traffic then blends in with other traffic. Indeed, recent traffic studies suggest that P2P connections are now distributed across all ports with concentrations at a few preferred points[3].

Today P2P traffic levels are still growing, but no single powerhouse application is driving it[4]. The aggregate numbers suggest that usage has more than doubled in the past three years, from less than 4 million to nearly ten million simultaneous users.[5] This does not include Bittorrent traffic, which is one of the most popular P2P applications for video and is more difficult to monitor. It also doesn't include users on private networks. Private networks, sometimes called dark networks (or darknets), are typically accessed through invitations from other users. Such networks, like OinkMe, may include millions of users.

Many users shift from network to network based on features and popularity. For example, the FastTrack network (used by KaZaA) has seen declines over the past three years while others like Gnutella have grown (Figure 1). Semi-successful attempts by content holders to disrupt access, coupled with KaZaA developers' efforts to increase revenue, quickly drove users to other networks, and even fostered the creation of new networks. This suggests low barriers to entry for new file sharing systems and also suggests that P2P networks serve a very mobile, well-informed user base that is willing to explore new alternatives as they arise.

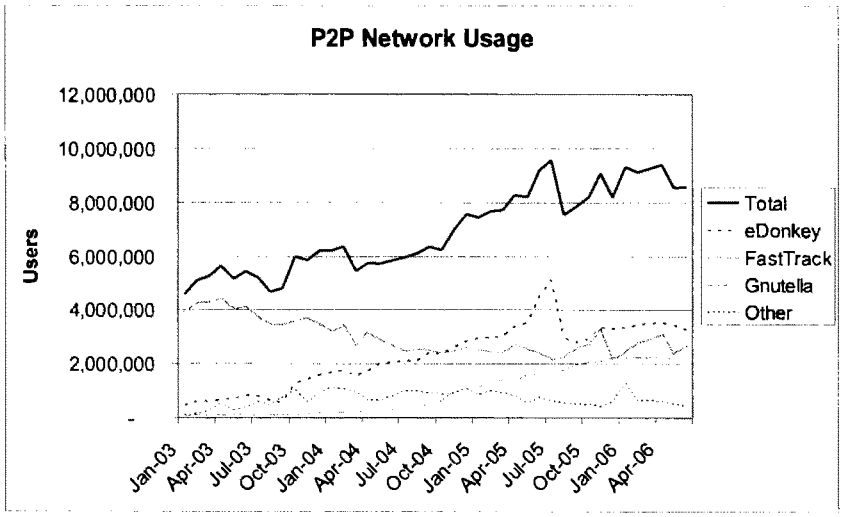


Figure. 1. Slyck.com Peer-to-peer Network Statistics - Simultaneously Connected Users[6]

With the constant introduction of new file sharing systems, one might wonder what is driving the innovation. While there have been some astounding attempts to sell the computational services of the user network, the typical business models of the software client developers are fairly simple, either community-driven open source or advertising supported.

P2P may have once been exclusively for the technologically elite, but today P2P adoption is widespread. One study found that 27% of adult Americans admit to sharing files from their computer with others.[7] Income, race, and sex seem to play little role in determining whether an individual will engage in file sharing.[8] Age is by far the largest signal of an inclination to share: Students are almost twice as likely to share as non-students.

P2P Security - How Does Sensitive Information Get Exposed?

Current P2P clients allow users to share items in a particular folder and often direct users to move files to that folder. In normal operation, a P2P client simply writes files to disk as it downloads them and reads files from disk as it uploads them. There are several routes for confidential data to get on to the network: a user accidentally shares folders containing the information; a user stores music and other data in the same folder that is shared; a user downloads malware that, when executed, exposes files; or the client software has bugs that result in unintentional sharing of file directories. Of course it is not necessary for a worm or virus to expose personal or sensitive documents because many users will unknowingly expose these documents for many reasons:

- *Misplaced Files* – If a file is dropped accidentally into the wrong folder.
- *Confusing Interface Design* – Users may be unaware of what folders are being shared or even that they are sharing files. For example, in a user study, Good and Krekelberg found that the KaZaA interface design contributed to user confusion over what files were being shared[9].
- *Incentives to Share a Large Number of Files* – Certain programs reward users for making files available or uploading more files. Some users may believe they can gain an advantage by sharing their entire hard drives.
- *General Laziness on the Part of the User* – If a user has a folder such as "My Documents" with many media folders inside, they may share My Documents rather than selecting each media folder individually to share, thus exposing all the other types of documents and folders contained within.
- *Wizards designed to determine media folders* – Some sharing clients come with wizards that scan an individual's computer and recommend folders containing media to share. If there is an MP3 or image file in a folder with important documents, that entire folder could be exposed by such a wizard.
- *Unaware or forgetful of what is stored on the computer and where. (especially by other users.)* – Users may simply forget about the letter they wrote to the bank, or the documents they brought home from work. Similarly, teenagers using P2P may not know what their parents keep on the Desktop.
- *Poor Organization Habits* – Certain people may not take the time to organize their files. MP3s, videos, letters, papers, passwords, and family pictures may all be kept in the same folder.

To illustrate the problem, we spent a couple hours searching the Gnutella network for sensitive personal documents; the resulting files we found should be disconcerting to users of P2P networks:

- *Birth Certificate – 45 Results*
- *Passport – 42 Results*
- *Tax Return – 208 Results*
- *FAFSA – 114 Results*

The Free Application for Federal Student Aid (FAFSA) and the U.S. Government's "EFILE" program both encourage individuals to complete forms online. When these forms are complete and full of potentially harmful information, applicants are asked to save a copy for their records. Similarly, those who are worried about credit scores often visit sites such as freecreditreport.com and annualcreditreport.com which, after asking several questions, return the customer a pdf file with their credit history. These types of files leak out onto the P2P networks because of their inherent digital nature.

We downloaded a selection of these files and verified that they were indeed real. We observed one particular individual who was sharing a scanned copy of his

passport. However, he did not only scan his passport, he also decided to scan his driver's license at the same time and include both in the same file. This information made him an easy target for anyone looking to commit identity theft. The passport and driver's license gave us two recent photographs of him, as well as his full name, address, date and place of birth, height, eye color, driver's license number, passport number, and two signatures. Furthermore, we were able to obtain his phone number and aerial photos of his house by using the gathered information in Google and Google Earth. Thieves are likely to download many more files from the individual's computer after finding such a document knowing that they have found much of the needed information to commit fraud.

In many ways, the security risk of P2P clients is similar to Trojan horses, malware, and phishing scams: security breeches that depend on human intervention, abetted by a carelessness or lack of proper security education among users. The remedies are also similar: user education, proper controls on corporate information, site blocking, periodic tests, and P2P network monitoring. We believe that the vast majority of information leaks are the result of accidentally shared data rather than the result of malicious outsiders extracting data from an organization. However, there are many other trends that are driving more security concerns.

Growing Usage and Network Heterogeneity Means More Leaks – Assuming that current usage patterns persist, more and more confidential information will find its way on to these networks. Despite the significant positive network effects associated with using a particular P2P client (the larger the network, the more diverse the content, the greater the reliability, and the greater the speed), P2P networks are far more heterogeneous and faster moving than operating systems. With many networks and clients, users are not likely to grasp the security issues and P2P developers will likely not focus on security.

Set and Forget Increases Losses – Research indicates that P2P clients tend to be "set and forget" applications that run in the background and while the user is not at the computer.[10] This suggests that the user is not carefully tracking the activities of the P2P client, increasing the opportunity for abuse. Further, even benign file sharing programs consume significant processor time and network bandwidth, conditioning the P2P user to tolerate sluggish performance that, for others, might be a first sign that a system has been compromised.

No Borders Result in Global Losses – Geography is largely irrelevant in P2P networks, meaning no particular country or region is safer than another. A computer logging on in Bombay or Brussels becomes part of the same network as a computer in Pittsburgh. As we will show, files certainly migrate globally and threats can come from any corner of the globe.

Digital Wind Spreads Files – A firm that has the unfortunate circumstance of sharing a name with a popular performer or song will experience far more activity. Users looking for a media target may upload unrelated files with similar names thus spreading a file. For example, the group Death Cab for Cutie recently recorded a popular song State Street Residential, which may increase the threat for documents

from State Street Bank. While most takers looking for the song may have no malicious intent for the bank, the business files will be found and spread, increasing the likelihood that they will be found by others. We call this "digital wind." Many factors can drive the spread of files including the file naming conventions. Moreover, second generation P2P networks typically create file indexes using the names of files and metadata associated with them (the MS Word user who created it or the company the software is registered to). For example searching for a live performance from the Wachovia Center in Philadelphia may turn up customers' records of their discussions with the bank (where "Wachovia" is a useful way to separate a bank conversation from a health insurance conversation). It also could snare Wachovia's internal documents because the bank name may appear in the company metadata tag of the file.

Malware - While the overwhelming majority of traffic on P2P networks is entertainment content (games, movies, music, etc.), also lurking on P2P networks are files that pose severe security risks[11,12]. Viruses that exist in email and other programs also have variants that exist in peer-to-peer networks. A particularly severe virus known as Antinny, appeared on the Japanese-based Winny network that led to the disclosure of a large amount of private data including, U.S. military base security codes, and documents belonging to a police investigator involving a major investigation and 1,500 individuals.[13,14]

Experimental Results Illustrating Threat

With a clear understanding of the vulnerability, what about the threat? To illustrate the threat, we ran a set of experiments in conjunction with Tiversa, Inc. In our first experiment, we posted the text of an email message (Figure 2) containing an active VISA (debit) number and AT&T phone card in a music directory that was shared via Limewire. The file was simply named "credit card and phone card numbers.doc" as a user who would title an email subject or file to reflect the message contents. With the help of a Tiversa, we observed both the activity of the file on our client and further tracked the file's movement across the P2P network. The file was quickly taken and retaken by a number of different clients (Figure 3). By the end of a week (1/10-1/17), the VISA card was used and balance depleted. We observed its use through the account's transactions statement posted by VISA on the web. Not knowing the exact balance of the card, the taker(s) used Paypal and Nochex (both processors of on-line payments) to drain funds from the card. It appears that two takers of the card were able to obtain funds as the activity was split into two groups and because one taker used Paypal, which is more US centric, while the other used Nochex, which is UK centric. Within another week the calling card was also depleted. Examining the call records of the card, all of the calls were made from outside of the US to two US area codes - 347 (Bronx, NY) and 253 (Tacoma, WA) clearly illustrating the P2P threat both within and outside of the US. Even more interesting, long after we stopped sharing the file, we observed the file continuing to move to new clients as some of the original takers leaked the file to others (Table 1).

To: "Sara Franklin" <sarakitten12@hotmail.com>
From: "Joe Franklin" <joefranklin197@yahoo.com>
Subject: Grandma sent you stuff

Sara,

Grandma sent you a $25 prepaid visa card and a telephone calling card in the mail for Christmas. She didn't have your address there at school. She said you better call her or else because now you don't have any excuses. Here's the info from the cards:

Visa:

4436-9811-8709-XXXX expiration date is 03/07. That three digit number that some places require is 636.

Phone card:

Here's what the back of the calling card says on how to use it:

TO PLACE A CALL FROM WITHIN THE US:

1. DIAL 1-800-471-1805
2. PRESS 1 FOR ENGLISH
3. ENTER PIN
4. PRESS 1 TO CALL WITHIN THE US PRESS 2 TO CALL ANY OTHER COUNTRY

The pin number is 557-696-XXXX. It has 210 minutes on it.

I know that you'll probably buy something online at bodyworks but if not let me know and I'll drop them in the mail.

XOXOXOXO

Dad

Figure 2. Example of a leaked document.

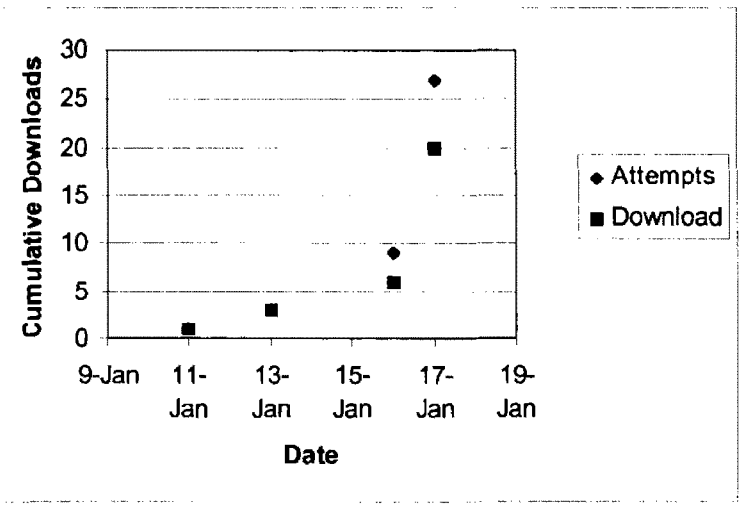


Figure 3. File downloads.

Hanover, NH	1/10	
Little Rock, CA	1/11	
Schenectady, NY	1/13	
Lincoln, NE	1/16	
Portland, ME	1/16	
Lancaster, CA	1/17	Stopped
Portland, ME	1/18	Sharing
Mexico	1/19	
Windsor, Canada	1/19	
UK	1/20	
Burbank, CA	1/21	
Little Rock, CA	1/21	
Singapore	1/22	
Sterling, VA	1/24	
Bakersfield, CA	1/25	
Germany	1/30	
Montreal, Canada	1/31	
Chattanooga, TN	2/1	
New Orleans, LA	2/2	

Table 1. The document kept propagating after we stopped sharing it.

Next we developed an experiment that was more closely focused on the threat to firms. We created and shared three mock business documents. The first was a request for proposal (RFP) for a fictional bank that was looking for IT services to support the integration of a yet-to-be announced merger. Such a document represents strategic business information that could be valuable in many ways, including the possibility of exploiting the information in stock trades. The second was simply as a (publicly available) press release from a major bank announcing the completion of a merger. It would again represent business information that the takers might think valuable. The last was a draft of a fictional patent application for a new nanotechnology. This intellectual property is far more specialized, requiring a more sophisticated thief who could sell it to someone who could, in turn, exploit its value. Again, we placed the files in a music directory that was shared over a seven day period via Limewire. With the help of a Tiversa, our objective was to see both the file movement and the actions of those who took the file. We hypothesized that professional thieves who took the document would be careful not to share it while amateurs might take the documents and reshare.

Over the week, the two banking documents were taken twelve times – eight for the major bank document and four for the fictional bank. The patent application was not taken during the week. We also observed that some of the takers immediately hid the document after taking it – saving it into a directory that was not shared. Others continued to share the documents leading to another six secondary disclosures.

Again, our experiment illustrated the risk of disclosure. Obviously, in this experiment, the risk appears much higher for financial documents than specific intellectual property like our patent application. While some of the takes may have taken the documents hoping to commit identity theft with personal consumer information, it appears likely that others were looking for business related documents. Whatever their motives, these business documents were taken and retaken. They also were taken by purposeful individuals who were quickly hiding their finds.

Conclusion

The popularity of peer-to-peer (P2P) file sharing has created many new security risks for individuals and organizations. In this paper, we have presented an analysis of the security vulnerability in P2P networks and provided accompanying evidence of the threat. There is little doubt that P2P presents a real security risk to both individuals and organizations. Certainly many individuals have likely been victims of identity theft as a result of their participation in these networks. Ironically, many of those victims may never realize the source of their misfortune. Rather than reducing the problem, we see many of the current trends further increasing the problem. While it is possible to use P2P sharing networks safely, the evolving security threats mean that the best security advice for many users is to avoid these networks altogether. In most cases, firms are well advised to block P2P activity on their networks and devices.

However, P2P sharing can be a very effective mechanism for distributing files and collaborating with other users. We see several approaches to reduce security risk including:

User interface design – As discussed by Good and Krekelberg, interface design has a significant impact on security. Client developers should incorporate features that clearly show users what files are being shared and uploaded along with reducing the ease of sharing (or even blocking) nonmedia files. Visualizing system activity and integrating the client configuration into routine user action as suggested by de Paula et al[15] would certainly improve security. However, as we noted earlier, given the business models of many P2P client developers it is not clear they currently have the incentives to improve the security of their interfaces. Thus users must beware and select appropriate clients. Likewise, firms should consider steps to improve user visibility of security gaps.

User education – Understanding the risks is a key step in reducing exposure. Firms should ensure employees, contractors, suppliers, and customers understand the risks.

File naming and organization – Firms and users should also introduce file naming conventions and policies to reduce the "footprint" of their documents. These types of initiatives reduce the threat of documents being found and spread. Folder organization to segregate files types is also important. For many firms, steps to block P2P participation on firm equipment along with policies for storing data on home machines are often warranted.

In ongoing work, we are examining the implications for financial services firms. With thousands of employees, contractors, suppliers, and customers, spread over many countries, we believe large firms face significant risk from information leakage into P2P networks.

References

[1] S. Zhao, D. Stutzbach, and R. Rejaie. Characterizing Files in the Modern Gnutella Network: A Measurement Study. Proc of In *Multimedia Computing and Networking*, (eds: S.Chandra and C Griwodz), 2006.
[2] N. Christin, A.S. Weigend , J. Chuang, "Content availability, pollution and poisoning in file sharing peer-to-peer networks," *Proceedings of the 6th ACM Conference on Electronic commerce*, 68-77, Vancouver, BC, Canada, June 05-08, 2005.
[3] T. Karagiannis, A. Broido, N. Brownlee, K. Claffy, M. Faloutsos, "File sharing in the Internet: A characterization of P2P traffic in the backbone", Technical Report, UC Riverside, 2003.
[4] T. Karagiannis, A. Broido, M. Faloutsos, and K. Claffy, 2004.Transport Layer Identification of P2P Traffic in *Proceedings of the 4th ACM SIGCOMM conference on Internet Measurement*. Taorima, Siciliy, Italy, 121-134.
[5] Mennecke, T. "Slyck News – P2P Population Continues Climb" June 14, 2006. [Online]. http://www.slyck.com/news.php?story=1220
[6] Slyck.com (P2P Network Statistics Beta) [Online]. http://www.slyck.com/stats.php
[7] Pew Internet Activities and Trends Report – June 05. Survey Question: Ever Share files from your own computer such as music, video, or picture files, or computer games with others online?
[8] Pew Internet Project Data Memo. [Online]. July 2003.
http://www.pewinternet.org/pdfs/PIP_Copyright_Memo.pdf
[9] N.S. Good and A. Krekelberg, "Usability and privacy: a study of Kazaa P2P file-sharing," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, April 05-10, 2003.
[10] A. Gerber, J. Houle, H. Nguyen, M. Roughan, and S. Sen. P2P The Gorilla in the Cable. In *National Cable & Telecommunications Association(NCTA) 2003 National Show*, Chicago, IL,
June 8-11, 2003.
[11] A. Kalafut, A. Acharya, M. Gupta, "A Study of Malware in Peer-to-peer Networks," *Proceedings of the Internet Measurement Conference*, ACM 2006.
[12] S. Shin, J. Jung, H. Balakrishnan, "Malware Prevalence in the KaZaA File-Sharing Network," *Proceedings of the Internet Measurement Conference*, ACM 2006.
[13] M. Ingram, "66,000 Names and Personal Details Leak on P2P" April 29,2006. [Online.] http://www.slyck.com/news.php?story=1169
[14] W32.Antinny.Q – Symantec.com
http://www.symantec.com/security_response/writeup.jsp?docid=2004-053016-5101-99&tabid=2
[15] R. de Paula , X. Ding , P. Dourish , K. Nies , B. Pillet , D. F. Redmiles , J. Ren , J. A. Rode , R. S. Filho, "In the eye of the beholder: a visualization-based approach to information system security," *International Journal of Human-Computer Studies*, 63, 5-24, July 2005.

Chairman WAXMAN. Thank you, Mr. Johnson.
Mr. Gorton.

STATEMENT OF MARK GORTON

Mr. GORTON. I would like to thank the Committee on Oversight and Government Reform for inviting me to speak today. My name is Mark Gorton, and I am the founder and chairman of LimeWire, LLC, the makers of the LimeWare file-sharing program.

LimeWire takes the problem of inadvertent file sharing seriously. We strive to make the LimeWire file-sharing program clear and easy to understand. Warnings about inadvertent file sharing are displayed prominently on the LimeWire Web site. The LimeWire program contains a number of features designed to prevent inadvertent file sharing. In the library tab, users can see which files are being shared and how many times each file has been uploaded. They can also turn off or on sharing on a file-by-file or folder-by-folder basis. Monitor and logging tabs on the LimeWire client also show which files are being uploaded.

Users are given warnings when they attempt to share folders which are likely to contain sensitive information, such as the My Document folders on Windows machines. A status bar is always present, which shows how many files are being shared, the number of files currently being uploaded, and the current upload bandwidth being used.

At LimeWire we continue to be frustrated that, despite our warnings and precautions, a small fraction of users override the safety default settings that come with the program and end up inadvertently publishing information that they would prefer to keep private.

However, despite all the work that we have done, inadvertent file sharing continues to be a problem, so LimeWire is working on a new generation of user interfaces and tools designed with neophyte users in mind. These interfaces will make it even easier for users to see which files they are sharing and to intuitively understand the controls that are available to them.

I have sent this committee a document entitled, Inadvertent Sharing Precautions and LimeWire, which provides a more comprehensive list of measures that LimeWire takes to prevent accidental file sharing. I also invite you to go to our Web site and download the LimeWire client and see for yourself how easy it is to see which files are being shared with LimeWire.

In addition to the problem of inadvertent file sharing, P2P networks are plagued by child pornography and copyright infringement. The Internet is a new technology which allows for many novel behaviors. Unfortunately, some of these new behaviors are detrimental to society. The regulatory framework that surrounds the Internet has not kept pace with technical advancements, and currently no effective enforcement mechanisms exist to address illegal behavior on P2P networks.

Internet service providers, ISPs, are a unique point of control for every computer on the Internet. Universities frequently function as their own ISPs, and a handful of universities have implemented notice-based warning systems that result in the disconnection of users engaged in illegal behavior who ignore multiple warnings.

These universities have sharply reduced child pornography and copyright infringement on their campus networks.

Similar policies could be mandated for ISPs in the United States; however, these policies are unpopular with telecom and cable companies who would prefer not to have an enforcement relationship with their paying customers. The telecom industry has objected vigorously to previous attempts to involve ISPs in the enforcement process, and it continues to oppose policies that would allow for the establishment of moderate yet effective enforcement mechanisms to combat illegal behavior on the Internet.

The only institution in the United States with the power to mandate the creation of an effective enforcement mechanism to police the Internet is the U.S. Congress. With the leadership of the U.S. Congress, a proper policing mechanism for the Internet can be established and the problems of child pornography and copyright infringement can be greatly reduced.

Thank you.

[The prepared statement of Mr. Gorton follows:]

Testimony of Mark Gorton
Chairman, Lime Wire LLC
before the
Committee on Oversight and Government Reform
U.S. House of Representatives
July 24, 2007

I would like to thank the Committee on Oversight and Government Reform for inviting me to speak today. My name is Mark Gorton, I am the founder and Chairman of Lime Wire LLC, the makers of the LimeWire file sharing program.

LimeWire takes the problem of inadvertent file-sharing seriously. We strive to make the LimeWire file sharing program clear and easy to understand. Warnings about inadvertent file sharing are displayed prominently on the LimeWire website.

The LimeWire program contains a number of features designed to prevent inadvertent file-sharing. In the Library tab, users can see which files are being shared and how many times each file has been uploaded. They can also turn off or on sharing on a file by file or folder by folder basis. The Monitor and logging tabs on the LimeWire client also show which files have been uploaded. Users are given warnings when they attempt to share folders which are likely to contain sensitive information such as the "My Documents" folder on Windows machines. A status bar is always present which shows how many files are being shared, the number of files currently being uploaded, and the current upload bandwidth being used.

At LimeWire we continue to be frustrated that despite our warnings and precautions, a small fraction of users override the safe default setting that come with the program and end up inadvertently publishing information that they would prefer to keep private.

However, despite all the work that we have done, inadvertent file sharing continues to be a problem, so LimeWire is working on a new generation of user interfaces and tools designed with neophyte users in mind. These interfaces will make it even easier for users to see which files they are sharing and to intuitively understand the controls that are available to them.

I have sent to this committee a document entitled, "Inadvertent Sharing Precautions in LimeWire", which provides a more comprehensive list of the measures that LimeWire takes to prevent accidental file sharing. I also invite you to go to our website and download the LimeWire client and see for yourself how easy it is to see which files are being shared with LimeWire.

In an addition to the problem of inadvertent file-sharing, P2P networks are plagued by child pornography and copyright infringement. The Internet is a technology which allows for many novel behaviors. Unfortunately, some of these new behaviors are detrimental to society. The regulatory framework that surrounds the Internet has not kept pace with technical advancements, and currently, no effective enforcement mechanisms exist to address illegal behavior on P2P networks.

Internet Service Providers, ISP's, are a unique point of control for every computer on the Internet. Universities frequently function as their own ISP's, and a handful of universities have implemented notice based warning systems that result in the disconnection of users engaged in illegal behavior who ignore multiple warnings. These universities have sharply reduced child pornography and copyright infringement on their campus networks.

Similar policies could be mandated for all ISP's in the United States. However, these policies are unpopular with the telecom and cable companies who would prefer not have an enforcement relationship with their paying customers. The telecom industry has objected vigorously to previous attempts to involve ISP's in the enforcement process and it continues to oppose policies that would allow for the establishment of moderate, yet effective enforcement mechanisms to combat illegal behavior on the Internet.

The only institution in the United States with the power to mandate the creation of an effective enforcement mechanism to police the Internet is the United States Congress. With the leadership of the US Congress, a proper policing mechanism for the Internet can be established and the problems of child pornography and copyright infringement can be greatly reduced.

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

General Clark.

Mr. BOBACK. With your permission, Mr. Chairman, I would like to speak first prior to General Clark.

Chairman WAXMAN. Certainly, Mr. Boback.

STATEMENT OF ROBERT BOBACK

Mr. BOBACK. Thank you, Mr. Chairman. Good morning, Chairman Waxman, Ranking Member Davis, and distinguished members of the committee. My name is Robert Boback, and I am the chief executive officer of Tiversa, the company that provided some of the information and data for Professor Johnson's study. I wish to extend my most sincere appreciation for inviting us to testify on this important and serious issue facing our country today.

First let me start by saying that I do agree with Mr. Gorton that the peer-to-peer is very powerful, and many members of the committee expressed similar concerns or similar statements, saying that the peer-to-peer is important and powerful technology, one of the most important in recent years for distributing the amount of user-generated content that is being delivered today.

First, let me start with some background on Tiversa to help you understand the problem.

In 2003 Tiversa developed technology that will allow us to position ourselves accordingly throughout the various peer-to-peer networks, including Mr. Gorton's application of LimeWire, through what we would known as the Gnutella network. In doing so, we were able to then view all of the available searches and information that is now on the network, so it is not limited to that of just LimeWire.

In doing so—and this is what is most astounding to most individuals—we are processing 300 million searches per day. For perspective's sake, Google processes 130 million searches per day. This is a massive network with many searches issued worldwide.

If you think of Tiversa's technology in two buckets, our technology allows us to process all of the search requests, but we can also issue search requests in that same vein for available information, so as I testify we will break down the two: what are people looking for, in a sense; and what is out there to be had.

As we were called to testify, I will address the consumer issue and the corporate issue and turn it over to General Clark to address the more serious national security risks associated with the Government issue.

Searches? So what are people looking for? On this slide demonstrated on the side here—and I know it is small to see—in a brief window we actually took a look to see what are people searching for. And this will be submitted to committee members. There are thousands upon thousands of searches issued for credit card and CD numbers, banking information, account log-in password, very specific terms to find confidential, inadvertently disclosed information on these peer-to-peer networks.

And this information is not only limited to that of the financial service industry, as evidenced by the next slide. Medical information and medical identity theft is a rapid riser. This information has a lower security threshold to that of the financial information.

Should someone question you about your medical information or getting a bill paid by the insurance, which most consumers would want, your likelihood to push back against that information or giving that information is much less than should someone ask you for your credit card information.

If you think of a medical identity card or an insurance card, that is very similar to a credit card with a $1 million spending limit. Identity thieves seek these out, and they seek them out on the peer-to-peer.

So in saying that, what disclosures are out there? These individuals issuing these searches, what is there to be found? Federal and State identification, including passports, driver's licenses, Social Security cards, dispute letters with banks, credit card companies, insurance companies, copies of credit reports—Experian, TransUnion, Equifax, individual bank card statements and credit card statements, signed copies of health insurance cards, full copies of tax returns, as Mr. Issa clearly demonstrated for us, extensive electronic records of active user names and passwords for online banking and brokerage accounts, confidential medical histories and records.

For the committee's review, we are going to submit a number of documents that have been redacted to show this. One individual, as we find thousands of them, sharing their entire life, per se, of information, including their children's Social Security numbers, date of birth, all of their account log-ins and passwords. This individual put them on an Excel spreadsheet in an effort to organize their life and, unfortunately, lost this information.

Another example is a doctor who performed a neuropsychological examination on a pediatric patient, a 9-year old fourth grader, and then disclosed that information as he had a peer-to-peer client on his system, disclosing the entire confidential results of this pediatric patient with very sensitive information.

One thing that is interesting to point out with this doctor is that it is not the person that disclosed the information that is affected. In that case, the doctor disclosed on the patient; therefore, an obvious HIPAA violation. However, it is the extended enterprise. We are now in a wall-less society such that corporations can have the best policies and procedures and hardware measures to try to prevent this; however, in an out-sourced world we share confidential information with attorneys, with this committee, with auditing firms, with out-source partners, and they have to also have the same policies, procedures, and safeguard measures, and that is just not happening.

The searchable corporate documents are as prevalent as consumer-related documents. They can be highly targeted and very specific or general. The larger and better known the company and its brand, the more searches that will happen.

It is important to note that existing security measures do not address this problem. That is an important fact. The current firewalls, anti-virus, the encryption services, the intrusion detection, the intrusion protection, it is not addressing this problem or we wouldn't see the prevalence that we are seeing.

Some of the corporate documents that we have found—press releases of publicly traded companies in markup found prior to their

release, a clear SEC violation; patent work up in markup; network systems related to documents, including administrative passwords and user IDs to private corporate networks; clinical drug trials before FDA approval; countless legal documents involving ongoing litigation, business contracts, nondisclosure agreements, and term sheets; human resources; accounting. It is extensive, it is enterprise-wide, and it affects all levels of corporations, as we have had examples. We can provide thousands of examples of each.

One specific example is an out-sourced telecom provider which shared the entire wide area network of one of the largest, most recognized investment banks in the world. This information could be used by terrorists, by hackers across the world to loop—and what I mean by loop is they can reconfigure router configurations such that that wide area network would not function properly. This would significantly impact a greater than $50 billion company based in the United States here.

Fortune 50 board minutes have been released, to where a confidential board minutes talking about compliance issues have been released on this very network.

The entire 4X trading platform of a very large international bank has also been released.

More importantly, where it starts to hit to Government issues, there was a large Government outsource provider that did security threats on various U.S. cities on the transit authorities for those cities. In that report they were given cart blanche access to the security measures of these various cities. Then they released the report inadvertently on the peer-to-peer. This information gives very precise information on where the bombs should be placed to have the maximum damage, where are the vulnerabilities in this city that could impact our national security. A city hired this company in an effort to decrease the risk facing that city, and, unfortunately, it increased it several-fold, as individuals are able to access that information, which is an important point.

In seeing the searches, we can tell you that people are accessing this information from outside the United States. It has been our research that this information does head to Pakistan. It does head to Africa. It does head to Eastern Europe. There are individuals outside the United States that are grabbing this information.

In closing, briefly on the screen we want to show you this is our technology running in real time, so as the system will bring up searches, these are people that are actually searching for and acquiring information. I know it is small and you can't read it, but we are going to provide a larger examples to the Members. This is information that is currently, right now, in real time, being disclosed. Thousands of it, as you can see. This is inadvertently disclosed and sought-after information on these peer-to-peer.

This is the new threat to information security. Just as 4 years ago we didn't understand phishing, we didn't understand virus, we do now.

I commend this committee for the opportunity to present this today.

Thank you, sir.

[The prepared statement of Mr. Boback follows:]

Robert Boback
Chief Executive Officer
Tiversa, Inc.

Testimony Before the House Committee on Oversight and Government Reform

July 24, 2007

Good morning Chairman Waxman, Ranking Member Davis and distinguished members of the committee.

My name is Robert Boback and I am Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides information technology and investigation services that help protect organizations, government agencies and individual consumers from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

I wish to extend our most sincere appreciation for inviting us to testify on this very important issue today. And I also want to applaud the Chairman for calling this important hearing and this committee's previous legislation and work on this topic.

While the Internet is a true boon to our society and economy, there are critical personal privacy and national security issues that need to be addressed seriously, urgently and with the immediate intent to find solutions.

These privacy and security threats are caused by the inadvertent misuse of P2P file sharing software, which Tiversa estimates has been installed on over 450 million computers worldwide. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the world wide web, it is not without inherent risks.

P2P technology provides an efficient way for people to share files with each other. Essentially, the technology uses the muscle power of the computers that it connects and allows people to share files directly with each other. When files are shared directly between two P2P users, this is called decentralized file sharing. This means the files do not go through any central computer server in the middle of the exchange.

P2P has gained both popularity and notoriety for the file sharing of entertainment content among its users. Yet, regardless of where one stands on P2P activity, it's unquestioned that P2P usage is rapidly growing and becoming generally accepted as the most efficient way to distribute large pieces of digital content to consumers.

Indeed, with the explosive increase in digital content including online video and user generated digital content, P2P file sharing is being embraced by many legitimate, well-known businesses to distribute and share television shows and full-length movies to consumers in a manner that protects the copyright and privacy of the content.

Therefore, P2P file sharing is becoming as much of a critical and integral part of the Internet's infrastructure as Web browsers are today. As a result, we must consider the privacy and security issues around it accordingly while allowing for legitimate uses of the technology.

Inadvertent file sharing happens when computer users mistakenly share more files than they intend. For example, they may only want to share their music files or a large academic report, but instead open all files on their computer's hard drive to access by other users on the P2P network. This typically occurs by a user error in either installing and/or using the software.

The result of inadvertent file sharing is hundreds of thousands of sensitive, confidential, and classified files are exposed and made available to the universe of P2P users each day.

Today, we would like to provide the committee with concrete examples that show the extent of how inadvertent P2P file sharing can negatively affect consumers, corporations, government entities and, indeed, our national security. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how users on P2P file sharing networks actively search for inadvertently shared sensitive information, and offer our thoughts on actions to address this problem.

Despite the tools that P2P networks are putting into their software to avoid the inadvertent file sharing of private or classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC has issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act, co-sponsored by Chairman Waxman, Ranking Member Davis and several members of this committee highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as Carnegie Mellon University's Computer Emergency Response Team (CERT) and

the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's *ST05-007-Risks of File-Sharing Technology - Exposure of Sensitive or Personal Information* clearly states:

> "By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

Additionally, many of the most popular P2P tools prominently display similar warnings to their users.

Regardless, the problem persists, and our opinion is that it's getting worse. Here is why we hold this opinion.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can round-up all the previously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a portion of a P2P file sharing network, Tiversa can see the whole. It is our belief that no other system has this capability. We have the unique ability to observe activity across P2P networks, to see what inadvertent file sharing is taking place, and to see how P2P users are seeking this information, and where the information goes once it is shared.

Tiversa can monitor, on average, at least 300 million total P2P requests per day. We can investigate more fully to determine the intent of those requests. Our systems have the ability to record the searches for files made on P2P networks, as well as the ability to access the files available to users of P2P networks who issue these searches.

Users on a P2P networks must "ask" the network for a file before they can download them. For example, they may request "Frank Sinatra, I Did It My Way." That search request is then broadcasted to all connected users for a response that says in effect - "I have that song". At this point, the searcher can initiate a download request from their choice of users who possess that file.

Substitute the Sinatra search for "classified troop movements" and you begin to understand the problem. Or, if someone searches for "ABC Bank August Statement", we can deem their intent was to obtain bank statements.

For example, Tiversa set its algorithms to record P2P search strings that matched the term "Credit Card" and separately the term "Medical." Illustrated below is a limited set of English language examples taken from the millions of similar search strings that Tiversa observes each day:

Credit Card

▪ d&b credit card info	▪ credit card pin numbers
▪ corporate credit card log	▪ credit card with cv2 numbers
▪ credit card merch copy sr	▪ credit card statements
▪ davids credit card numbers	▪ credit card comm sept private
▪ credit card charge ctm costa	▪ credit card authorisation july
▪ credit card gateway ubc	▪ credit card app pdf
▪ 2007 batch of credit cards	▪ athens mba credit card payment
▪ cash credit card checks	▪ cathys visa credit card go on
▪ confidential credit card app	▪ credit card with acc
▪ credit card processing	▪ credit card statements

Medical

▪ dear medical insurance my	▪ child medical exam
▪ letter re medical bills 10th	▪ billing medical august
▪ denial of medical insurance	▪ digital files medical trans
▪ medical passwords	▪ authorizationform medical
▪ hospital records	▪ caulfield general medical
▪ comprehensive medical	▪ medical coding and billing
▪ medical release	▪ medicine medical passwords
▪ classified medical records	▪ isilo medical
▪ electronic medical record	▪ doctors office medical exam
▪ ltr medical maternity Portland	▪ medical abuse records

There are literally thousands of search strings that we can use to illustrate the millions of individual searches targeting sensitive information available on file sharing networks. One has to ask the question, "Why are P2P users searching for these files on a network typically used to share music and movies?" What are these users looking for? What will they do with the information once they find it?

We would now like to describe how consumers, businesses and government entities are victims of this problem by showing and describing actual examples of sensitive, confidential, and classified files inadvertently disclosed by these entities.

Individuals at Risk
P2P is a highly efficient way for a potential identity thief to gather an individual's private, privileged information that can then be used to commit ID theft, other forms of fraud, or put the individual's personal safety at risk. Yet, very few individuals are aware of this problem, let alone how to protect their information. There have been significant public awareness efforts aimed at educating consumers about phishing scams and other malicious activities. There has been very little effort made to protect consumers from inadvertently sharing information through P2P networks. Virus checking and firewalls, commonly highlighted as the solution, are not fully effective at solving inadvertent file sharing problem.

Examples of readily available documents Tiversa has been able to find on P2P file sharing networks include:

- Federal and State identification including passports, drivers licenses, and social security cards
- Dispute letters with banks, credit card companies, or insurance companies revealing account numbers, credit card numbers, insurance ID numbers and social security numbers
- Copies of individual credit check reports (e.g. Equifax Reports)
- Copies of individual bank and credit card statements
- Signed copies of health insurance cards
- Full copies of federal, state, and local tax returns
- Extensive electronic records of active usernames / ID's for online account access
- Wills and trust documents
- Mortgage and credit applications
- Life insurance applications
- Confidential medical history and records including psychiatric records
- Employment applications
- Family photographs and movies revealing children, addresses, and other personal information
- Student loan / aid applications and documents

Redacted examples that protect the privacy of individual document owners have been provided to the Committee.

In essence, whatever an individual stores on his/her computer electronically can be inadvertently shared. The impact of sharing these files not only hurts individual consumers directly, but also impacts the financial institutions, insurance firms, and government agencies who must incur the costs of fraud and investigations into wrong-doing. In these cases, consumers may hold these institutions responsible, when they themselves are exposing their own information. The lack of a mechanism to trace back to the source of the disclosure is often the issue in these cases. Fraud occurs, but consumers, corporations, and government organizations often do not know the root cause.

Corporate Breaches

Corporate inadvertent file sharing includes any entity that is not a governmental organization or an individual. No organization, regardless of its size or industry is immune from this problem. This ranges from the world's largest multi-national corporations across the financial services, insurance, defense, pharmaceutical, professional services and healthcare industries to small medical, accounting and law practices. Equally, no organizational function is immune to inadvertent file sharing. Tiversa has found files disclosed by and affecting human resources, finance, compliance, legal, research and development, sales, marketing, public relations, and the executive office.

With the increasing virtualization of corporate entities and the greater use of outsourcing, the concept of the *Extended Enterprise* has become critical to Tiversa's clients. This means that any entity entrusted with the corporations sensitive or confidential information can become a disclosure point on P2P file sharing networks. These entities include at home or virtual employees, contractors, suppliers, attorneys, consultants, accountants, or partners. These entities are almost always outside of the corporate perimeter and, therefore, outside of the direct control and enforcement of the corporation. How many times have you e-mailed a file home on which to work? Sent a confidential file to your lawyer or accountant? Inadvertent sharing over P2P file sharing networks is perfectly designed to exploit the *Extended Enterprise*. Our examples will show this.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings would put these corporations at risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information. In fact, many times we will see P2P users searching for specific file titles on a corporation. A recent example shows P2P users searching for a foreign exchange system design document for a major financial institution more than 40 times over a three week period. Tiversa knows this document is available since we obtained it as part of our work for a client.

The larger and better known a company and its brand, the greater the risks associated with searches for these corporations.

Tiversa has many examples of corporate information disclosures. Obviously, many are extremely sensitive and would put these corporations at significant risk if they were shared in a public domain. We are happy to share illustrative information with the committee in a secure environment if specific examples are needed.

The following, however, represents examples and situations that we have encountered illustrating the risk facing corporations today.

The first example illustrates a number of points relating to corporate disclosures clearly. Tiversa has discovered a third party attorney whose clients are the world's largest pharmaceutical manufacturers disclosing 436 sensitive and confidential files related those clients. The information covers, in part, pending litigation. One document, dated April 2007, is labeled "confidential" and "by hand" and addressed to Chairman Waxman with a carbon copy to Ranking Member Davis. It appears to address questions regarding drug trials of this pharmaceutical company. This is a case of an attorney who has exposed multiple pharmaceutical companies outside of their network – a clear example of extended enterprise risk.

A second case involves the exposure of the recent board minutes of one of the world's largest financial services organizations, and was disclosed by an executive assistant to one of the executive team members. This disclosure was originally found by a private investigator and reported to the corporation.

A third case involves the disclosure of the entire foreign exchange trading back-bone for one of the world's largest multi-national financial firms. These files were among hundreds of confidential internal computer design and security files. As we stated earlier, P2P users were searching for these by name.

A forth case illustrates how a contractor can expose a corporation. Tiversa observed P2P searches involving a contractor to one of our clients. Files exposed include the entire launch plan and expected growth targets for this diversified financial institution's entry into Europe. In addition, Tiversa observed these files in the possession of a P2P user in Nigeria. In this instance, a subcontractor to the initial contractor exposed our client's confidential information.

A fifth case again illustrates how a supplier can expose a corporation. Tiversa recovered the wide-area network and disaster recovery plan for a major banking institution exposed by the company to which the bank's entire trading network was outsourced.

Tiversa can provide literally hundreds of case examples like those illustrated above. In addition, we have found:

- Press releases in mark-up before their public release covering material, non-public information
- Patent related files before submission to the patent and trademark office
- Drug trial test records before FDA approval
- Legal documents including business contracts, non-disclosure agreements, term sheets, etc.
- Human resources related documents including employee reviews, executive recruiter post-interview write-ups, confidential termination and pending litigation documents, etc.
- Accounting related documents including audit reports, corporate tax records, payrolls, invoices, etc.

- Information systems related documents including administrative user ID / passwords to corporate systems, network diagrams, router access codes, functional specifications, disaster recovery plans

Highly select redacted examples that protect the privacy of individual document owners and any other sensitive information have been provided to the committee.

Given the media exposure that "lost laptops" and information disclosures on non-P2P networks has received, P2P inadvertent file sharing represents a significant brand, operational, legal, and regulatory risk to corporations. For example, a recent P2P sourced breach affecting 17,000 current and former Pfizer employees' personal information illustrates the impact of the inadvertent sharing of sensitive information on P2P file sharing networks. Any one of the examples provided to the committee could result in a similar problem for its respective corporation.

Classified Government Data Exposed
Inadvertent P2P file sharing affects all levels and branches of government, law enforcement, and intelligence agencies. For our testimony today, Tiversa will focus on how inadvertent file sharing affects federal government agencies and law enforcement.

As with corporations, government inadvertent file sharing may originate with the agencies themselves, contractors to these agencies, soldiers or agents in the field. The same "extended enterprise" exposure problem facing corporations faces the government.

In addition, Tiversa regularly sees P2P searches for government related information including classified information and searches that could assist law enforcement.

In 2003, Chairman Waxman, Ranking Member Davis and many members of this committee co-sponsored the Government Network Security Act. It was designed to quite simply: "require Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by peer-to-peer file sharing."

In a press release announcing the Act, Ranking Member Davis was quoted saying, "Few people recognize these risks. Using these programs is similar to giving a complete stranger access to your personal file cabinet."
Unfortunately, while the bill passed the House, it stalled in the Senate. Now, four years later, there are hundreds, if not thousands, of examples of federal government classified documents publicly available on P2P networks at this very moment.

A stark example is the discovery of 34 classified documents available and found by Tiversa on P2P networks. At least one of these classified examples was

related to a government contractor. At least one of the classified documents is the secret property of the United Kingdom, which shows the inadvertent release of such sensitive data is unquestionably global in nature.

Prior to our testimony today, Tiversa provided secret classified documents we located to General Wesley Clark, an equity holding member of Tiversa's advisory board. He has since furnished these documents to the Chairman of the National Intelligence Advisory Board for investigation. This information could, and most likely does, pose significant risks to our interests domestically and abroad. Unfortunately, this is not an isolated incident.

Inadvertently shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

1. A document illustrating over 100 individual soldier's names and social security numbers
2. Physical Threat Assessments for multiple cities such as Philadelphia, St. Louis, and Miami
3. A government contractor exposing an air force base physical security attack assessment
4. A document titled *"NSA Security Handbook"*
5. A detailed report from a well known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks
6. Numerous Department of Defense Directives (DoDD's) on various Information Security topics – all signed by various Assistant and Deputy Secretaries of State
7. Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g. retina scanner equipment audits, penetration detection software/equipment reviews)
8. Numerous "Field Security Operations" documents including router checklist procedures, "Network Infrastructure Security Checklist", etc.
9. Numerous presentations for Armed Forces leadership on various Information Security topics including how to profile "hackers" and potential internal information leakers
10. Large numbers of army documents marked "For Official Use Only"

A case example illustrates the risks clearly. On July 17, 2007, Tiversa found a defense contractor employee disclosing 1,900 individual files from one IP address on P2P file sharing networks. This contractor supports 34 "Joint and Army agencies", including the Department of Defense at the Pentagon, Defense Intelligence Agency, National Security Agency, US Air Force, Army, Navy and the National Imagery and Mapping Agency. This person was disclosing a wide array of files including music, personal information, resumes, photos, etc. Alarmingly, this individual was also disclosing 534 files with extremely sensitive, privileged information regarding the US Government generally, and the Department of

Defense and various US Armed Forces specifically. The types of information disclosed included:

- The entire Pentagon secret backbone network infrastructure diagram including server/IP addresses
- Password change scripts for Pentagon secret network servers
- Department of Defense employees contact information (including cell and home phone numbers)
- Secure Sockets Layer (SSL) instructions and certificates allowing access to the disclosing contractors' IT systems
- A contract issued by the "Army Contracting Agency" at the Pentagon that authorizes expenditures in excess of $1.5 million with the disclosing contractor
- Numerous policies/procedures regarding the Pentagon's IT infrastructure as well as its threat response activities (including a "Draft Strategic Plan" for 2007 – 2011)
- A letter from a "Deputy Director for Management" at the "Executive Office of the President's Office of Management and Budget" which explicitly talks about some of the risks associated with P2P file sharing networks.

Ironically, it appears that the individual disclosing this information could be a member of a computer incidence response team and could hold top secret clearance – certainly not an uninformed computer user.

The risks posed by this disclosure source are widespread. For one, the disclosed information could be used directly to penetrate the Pentagon's secure IT environment in an effort to access highly classified information. Secondly, the information could be used indirectly against the disclosure source for blackmail, coercion, kidnapping, etc.

Outside of the alarming nature of this instance, this case clearly illustrates a number of key points:

- Extended Enterprise Risks – these disclosures appear to have happened *outside* of the Pentagon's network where traditional perimeter IT approaches and policies are not effective.

- One Source / Many Exposures – one source, in this case, adversely affected multiple government agencies. This exposure is worse than a lost laptop since P2P users have open access to the information on the computer without the knowledge of the owner. Anyone who knows what to look for can obtain this information and share it.

- Risk of "Open Windows" – whatever new files are now added to this individual's computer will then become available to the P2P user community. Despite the fact that sensitive files may or may not be

present on an employee or suppliers computer today, the very existence of P2P file sharing software can expose whatever files are added in the future.

Redacted examples that protect the privacy of the respective government agencies and affected individuals have been provided to the Committee with the exception of classified information which, as noted earlier, was provided to the Chairman of the National Intelligence Advisory Board by General Wesley Clark.

Law Enforcement Related Examples

Citizens expect our government to protect its own classified and confidential information, but to also enforce laws governing illegal uses and exploitation of information. Examples of this include enforcing copyright and licensing laws and export control laws. One example we wish to highlight to the committee is the extensive use of P2P Networks for searching and sharing child pornography. To illustrate the extent of this trafficking of this information, Tiversa collected searches that P2P users were issuing for known child pornography terms. This example is provided to the committee as a separate exhibit.

Live Demonstration

While the examples collected represent various periods of time, a glimpse into what is available *live* on P2P networks dramatically illustrates the extent of exposure for the categories of examples highlighted above. We will now show user issued searches and available files that match a select list of file probing terms.

Evidence of Wrong-doing

Tiversa has shown the committee live views of P2P user issued searches and available sensitive, inadvertently shared files. We have illustrated that P2P users are actively searching for sensitive, confidential, and classified information. We have shown sensitive, confidential, and classified files are present on P2P networks across individual consumer, corporate, and government sources. What happens to these files once they are found, downloaded, replicated, or used? Is there evidence of fraud or wrong doing?

Fraud Test

Tiversa, in conjunction with Dartmouth's Center for Digital Strategies, conducted a test to show that once a file with actionable financial information is inadvertently disclosed on a P2P network, individuals will use it for an ill-gotten financial gain.

Tiversa and Dartmouth purchased a VISA cash card and an AT&T calling card and incorporated the cash card numbers and phone card numbers instructions on how to use these into a letter. An electronic copy of the letter was put on a

Dartmouth test computer and shared using LimeWire file sharing software. Tiversa tracked the spread of the letter globally across P2P file sharing networks, from the point of initial compromise from the original source computer to its sharing and subsequent re-sharing(s). Tiversa and Dartmouth then tracked the real-time use of the cash card and calling card. The VISA cash card was depleted within a week. Even after the original source computer was shut off, the file continued to be shared by others users on P2P file sharing networks.

Professor Eric Johnson from Dartmouth will explain this test in more detail in later testimony to this committee.

Corporate Information Test

A similar Dartmouth experiment was conducted with documents related to a fictitious company placed on a Dartmouth test computer and shared using LimeWire file sharing software. Tiversa then tracked the spread of these files from the original source computer across P2P networks clearly indicating that there was significant "demand" for these "corporate" files.

The Root of the Problem

Why is there such a pervasive and massive amount of sensitive, classified, and confidential information available on peer-to-peer file sharing networks? Corporations and government agencies have installed technologies designed to block access to P2P networks and instituted policies that prohibit employees from using P2P networks or taking or e-mailing information to their homes. Consumers have installed virus checking and firewalls, which is typically the recommended course of action by the world's major security software providers.

Tiversa's focus has been working with corporations, government agencies, and consumers to mitigate P2P disclosures and risks. Based on our experience, we believe the reason so much information is present is driven by these factors:

1. A lack of awareness to the pervasiveness and magnitude of sensitive and classified information present on P2P networks. One cannot "fix" a problem that one is unaware of, no matter how much it currently may affect an organization.

2. Overextended information security functions and budgets that prioritize recent "fires" or compliance with legislation and industry mandates. Prioritizing something to which there is little awareness is often not done because it is difficult to gain the attention of senior management and procure budgets and resources.

3. Organizations have "too narrow" a view of their network perimeter. Whose responsibility is it to protect information once it leaves the corporate perimeter? Does a consumer or the US government care

whether a corporation or a supplier to that corporation entrusted with sensitive information disclosed files on P2P File Sharing Networks once the damage is done? The overwhelming evidence shows that a substantial amount of P2P inadvertent file sharing breaches come from an organization's *Extended Enterprise* outside of its network perimeter. Many organizations today focus solely on protecting their network perimeters when their business is becoming more virtual and outsourcing is taking hold. Sensitive, confidential, and classified information follows these new business operations.

Finding Solutions

We would like to provide the committee our initial recommendations on how consumers, corporations, and government entities can mitigate this problem.

The committee should take steps to:

- Create broader and more focused awareness of the dangers of inadvertent P2P file sharing.
- Require continuous auditing of P2P file sharing networks themselves for sensitive, confidential, and classified information disclosures.
- Encourage organizations to adopt policies and to take steps to address their *Extended Enterprise.*

Consumers:

For consumers, Tiversa has a number of recommended actions

- Consumers first need to become aware of this problem. While government warnings already exist, we feel the private sector can play a highly effective role in addressing this issue and in creating awareness. Banks, credit card companies, and healthcare insurance organizations can lead this effort since they are most impacted by P2P originated fraud. They are trusted by their customers and have existing communication channels available. Previous efforts to address phishing serve as a useful model.
- Consumers should consider putting their highly sensitive information on a separate PC or device disconnected from the Internet.
- Consumers should continuously audit P2P networks to ensure that unwanted files are not exposed. If they find personal or sensitive information available, they should be equipped with the knowledge of what actions to immediately take.

Corporate

For corporations, Tiversa has a number of recommended actions:

- Those tasked with managing security risks inside of an organization must be aware of the pervasiveness and magnitude of inadvertent P2P file sharing, and how it affects them. These individuals need to educate senior leadership – especially those in privacy, legal, and compliance – to the risks they face.

- Corporations need to understand their disclosed information exposure by auditing, as fully as possible by a neutral third party, the type and magnitude of their information on P2P file sharing networks.

- Corporations need to continuously monitor for new exposure points on P2P networks, and to judge the effectiveness of their policies and remedial actions.

- Corporations need to identify disclosure sources across their Extended Enterprises that expose them to inadvertent file sharing risks. This includes employees operating outside of the perimeter, suppliers and contractors, agents, and partners.

- Corporations should re-evaluate "four-wall" perimeter approaches to information security and update their policies to address information disclosure by third parties and the general lack of control once information exits an organization. This may include, for instance, requiring contractors, suppliers, attorneys, and accountants to indemnify the organization for peer-to-peer originated information disclosures.

Government

- The government should take the lead in creating greater awareness at corporations and throughout the public on the dangers associated with P2P file sharing.

- The government should immediately and continuously identify the full exposure and global spread of classified information to shut down these disclosure sources.

- The government should conduct a comprehensive audit of P2P file sharing network information disclosures – not just focused on the agencies themselves, but on also on contractors and non-agency sources.

- P2P information exposure risk should be emphasized in the Federal Information Security Management Act Report Card.

- The government should require their contractors to certify that they and their extended enterprises have fully addressed inadvertent file sharing disclosure risk.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, or classified information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of the technology in the future.

Thank you for the opportunity to testify here today.

Chairman WAXMAN. Thank you, Mr. Boback.
General Clark.

STATEMENT OF GENERAL WESLEY K. CLARK

General CLARK. Good morning, Mr. Chairman and Ranking Member Davis, distinguished members of the committee. It is an honor to come before you today to talk about a topic that is critical to our national security and to the safety and privacy of our Nation's citizens and companies. I want to commend Congressman Waxman and Congressman Davis and members of the committee for both bringing this issue back to light and for the work this committee has done previously to try to highlight the risk.

I want to just disclose now that I am an advisor to Tiversa, and in that role I do have a small equity stake in Tiversa. But my engagement here has just opened my eyes to activities that I think, if you saw the scope of the risk, I think you would agree that it is just totally unacceptable. The American people would be outraged if they were aware of what is inadvertently shared by Government agencies on P2P networks. They would demand solutions.

Now, Bob Boback has just explained what is out there on the corporate side. I have submitted some material for the record. Let me just summarize quickly what we found.

As I was preparing for the testimony, I asked Mr. Boback to search for anything marked classified secret, or secret no-foreign. So he pulled up over 200 classified documents in a few hours running his search engine. These documents were everything from insums of what is going on in Iraq to contractor data on radio frequency information to defeat improvised explosive devices. This material was all secret, it was all legitimate.

I called the chairman of the National Intelligence Advisory Board, who worked for Admiral McConnell, and shipped the information to him. He looked at it. He called NSA. NSA has it. They are now very seized with the problem, I think. But I think that the work of this committee has been a great assist in getting the agencies to look at this, because previously there have been contacts but we never have sort of engaged.

As the chairman of the Advisory Committee told me when he looked at the documents, he said, my goodness, they are in full color. Yes, they are the complete documents. They are not faxed copies, they are not smudged. They are just as fresh as if they were printed off on the computer printer of the organization.

Even more alarming, I got a call from Bob Boback on Wednesday night that he had found on the peer-to-peer net the entire Pentagon's secret backbone network infrastructure diagram, including the server and IP addresses, with password transcripts for Pentagon's secret network servers, the Department of Defense employees' contact information, secure sockets layer instructions, and certificates allowing access to the disclosing contractors' IT systems, and ironically, a letter from OMB which explicitly talks about the risks associated with P2P file-sharing networks.

So I called the Office of the Secretary of Defense. I got the right people involved. They had some meetings on it this. It turns out that a woman with top secret clearance working for a contractor on her home computer, she did have LimeWire, and somehow, I guess,

she had taken some material home to work on it, and so all this was out there.

This material was not, strictly speaking, secret. It was, I think, labeled FOUO. But it was certainly information that would be sort of a hacker's dream.

What we found at Tiversa was that many people were queued up to download this information. This looked so interesting that they wanted it. So we don't know how long it had been out there. There is no way of knowing that. But we called the company an obviously we got it stopped as soon as we found out about it.

But these two examples illustrate the risks that are out there. Peer-to-peer file sharing is a wonderful tool. It is going to be a continuing part of the economy. It is a way that successfully moves large volumes of data, and that is not going to go away, but it has to be regulated and people have to be warned about the risks, and especially our Government agencies—our National Security Agency, DOD, people that run the Sipranet—have to take the appropriate precautions, because we can't have this kind of information bleeding out over the peer-to-peer network.

Thank you, Mr. Chairman.

Chairman WAXMAN. Thank you very much, General Clark.

Let me start off the questioning. It is really stunning to see what you can get on a real-time basis, the kind of information that is being viewed even during the time we are holding this hearing. But I want to go into this issue, General Clark, about classified national security secrets.

You described that you were able to find the entire Pentagon secret backbone network infrastructure diagram using P2P networks available to millions of users. They also could find this. You have also said you have found other types of classified information such as—and this is not a complete list of what you reported to find: one, a document with individual soldiers' names and Social Security numbers; two, physical threat assessments for multiple cities such as Philadelphia, St. Louis, and Miami; three, a document entitled NSA Security Handbook; four, numerous DOD directives on information security; five, DOD security system audits; six, numerous field security operations documents; and seven, numerous presentations for armed forces leadership on information security tactics, including how to profile hackers and potential internal information leakers.

From a national security perspective, how significant is information you were able to find? You indicated that this was from one person who had taken material home to use and to work from home, but they weren't classified but they were secret. Would this kind of information jeopardize our national security if it fell into the wrong hands?

General CLARK. Of course it would, Mr. Chairman. It is very significant information, and the kinds of information that you list are simply what we found. We put the straw in the water. But we could have put the straw in the water and asked for something else. We didn't ask for top secret. We didn't ask for code word or SCI. This morning we found a document that shows the status of people receiving security clearances for SCI.

So there are all kinds of materials out there that is leaking out inadvertently. This is a major channel of communication, and we don't want to shut it down, but people just don't understand the risks when they put this information onto a computer that it is broadcast all over the world and it is being taken.

So we need a real program that sorts through this that observes it and watches for these kinds of violations and shuts it down immediately. We shut down this woman's computer instantly as soon as I called the CEO and told him what was on it, but there is no guarantee that there wasn't something equally damaging on another employee's computer that we just hadn't programmed a search for.

Chairman WAXMAN. These are not Government employees directly, but more the contractors that might be using a P2P network?

General CLARK. Right. These are contractors who work in the Pentagon. Most of our agencies have a mixture of Government, Civil Service, or Schedule C appointees working, plus they augment with contractors.

Chairman WAXMAN. Yes. Now, you indicated you promptly turned these documents over to officials in the intelligence community. Can you specify where you sent these documents?

General CLARK. They were sent to the chairman of Admiral McConnell's National Intelligence Advisory Board.

Chairman WAXMAN. And what was their reaction? Were they aware of this risk to national security?

General CLARK. They were aware of it in general, but they were not aware in specific, and they weren't aware, for example, of how to monitor it.

Again, I am not in this network now. I am a civilian and I am just in business, but my impression was—I have dealt with classified information all my life, and normally when you have a breach it is a pretty simple, clear-cut thing. You can pretty much trace it back to somebody making a mistake, carrying a document home, leaving a briefcase somewhere. Somehow it gets lost, turned in by somebody, and you can do a damage assessment on it.

In this case, when the documents are presented, they are going to have to go to very elaborate measures to find out where the documents came from and who has actually viewed or downloaded these documents. It can be done, but they don't have the procedures in place to do it, so we are talking about opening up a new area of national security for document protection here.

Chairman WAXMAN. So until we do something along those lines, it is an ongoing national security threat.

General CLARK. Right. What businesses are doing is they are having people screen the peer-to-peer space for their documents, and then it can be traced back normally to the source of that document, and then they can get the computer shut down or make the correction. And if it is done on a routine basis and it is up there all the time, hopefully the document doesn't leak very far.

Apparently, we don't have that system in place yet in the U.S. Government, so we don't know what is really out there that is inadvertently leaked out in the peer-to-peer.

Chairman WAXMAN. And that is something the Government should do, not the P2P network?

General CLARK. I don't think you can totally control it without observing it, so I don't think you can simply tell LimeWire and the other companies, change your software so this never happens again. I think you have to have an active defensive monitoring program for Government documents on the net, just like investment banks are starting to add, or law firms, because there are just so many opportunities for this material to get out there that if you wait for the lawsuit you have waited too long.

Chairman WAXMAN. Thank you very much.

Mr. Davis.

Mr. DAVIS OF VIRGINIA. Let me ask, my first question is: we are focused really on privacy protections, proprietary information, secret information leaking out. But conceivably, if the wrong people got in through peer-to-peer into Government files, could it lead to a cyber Pearl Harbor? General Clark, do you have any thought on that?

General CLARK. This material obviously poses risks, because there are opportunities here for hacking, for covert entry, for inserting programs inside routers and servers and other things, all of which are very damaging.

Now, we can't tell you at this moment who took the information on the secure Internet. We can do some detective work on it and we may find it, but at any given point a computer, an innocent computer, supposedly, let's say in Ghana, could have downloaded this information, printed it, and themselves then had it carried as a document, so you would lose the trail at that point.

Mr. DAVIS OF VIRGINIA. Mr. Mintz, let me ask you, could conceivably the wrong people get inside the files at your Department? Could they take control? Is there a way that they could do that?

Mr. MINTZ. Well, certainly if people got access to information, password information or something like that, it would be possible for them to get in. Typically, within our own network we are able to stop this kind of activity fairly quickly. The problem, however, is the release of information that would go out would be the greater problem, I think, for us. They'd be able to get access to information we don't want them to have.

Mr. DAVIS OF VIRGINIA. Well, let me ask you this, if you know. FISMA guides agency information security postures. In the context of Federal agencies, should we address these issues then under FISMA?

Mr. MINTZ. The issue of the peer-to-peer?

Mr. DAVIS OF VIRGINIA. Yes.

Mr. MINTZ. Peer-to-peer, in fact, is a requirement of the FISMA report. There is a part of it that we have to respond to what we are doing with peer-to-peer activity. It certainly should be an important part of FISMA.

What we found here also, I think, beyond just the technologies I mentioned, there are two issues that I think we have to look at. One is what do we do in terms of training to make sure that people are paying attention to these issues, because often the use is home computers, not just the use in the system.

And the second is to emphasize the need to audit. That is, we do a lot of times, I think, what I call policy on the shelf. We put together a lot of the policies, but what is it we do to make sure that the policies are actually being followed and paid attention to? So we needed some kind of an auditing process to go back and check to see that.

Mr. DAVIS OF VIRGINIA. Let me ask Mr. Johnson and Mr. Boback, what portion of the volume on file-sharing programs is basically music and video sharing?

Mr. JOHNSON. In terms of just the sheer size of the files, video content makes up a huge fraction of what is moving out there, video and other media.

Mr. DAVIS OF VIRGINIA. Any ballpark?

Mr. JOHNSON. Documents are just a tiny fraction, because they are so small, but there are many of them, but a document is so small compared to a music file or a video file.

Mr. BOBACK. Sir, in our research we found that MP3s are actually 38 percent of the information that we have found. We are not talking just document size, as Professor Johnson mentioned, kind of skews the data, but we are also talking just in the number. So MP3s are 38 percent, m-PEGS, which are movies, are another 19 percent in our research. But, again, this is irrelevant of the size.

Mr. DAVIS OF VIRGINIA. Right.

Mr. BOBACK. Just the number.

Mr. DAVIS OF VIRGINIA. How much of this activity comes from overseas actors? Any evidence of any state-sponsored activity in these areas, seeking classified or proprietary information from file-sharing networks?

Mr. BOBACK. We have found information, classified information, from multiple foreign governments. What we can testify to is that there are multiple foreign entities that are actively using the peer-to-peer to issue what we would say are illicit searches. If someone were to issue a search for, as General Clark mentioned, Sipranet, and that search originated—which one just recently happened—out of Ghana, West Africa, that should be an area of concern to the U.S. Government.

As Professor Johnson testified, that is a Sipranet search being issued on a file-based network most notably known for movies and music. Why is that search being issued from Africa?

As to who issued that search, we can target back to an actual IP address, but, unfortunately, I cannot, without further investigation, get to an individual.

Mr. DAVIS OF VIRGINIA. Thank you.

Chairman WAXMAN. Thank you, Mr. Davis. Your time has expired.

Mr. Cummings.

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

I want to go back to something Mr. Waxman said to you, General Clark, about the threat to our national security. As a member of the Armed Services Committee and as chairman of the Coast Guard Subcommittee, we go into a lot of classified briefings. I look at what we go through. You have to sign the documents, you have to swear that they will never mumble one syllable. And then to find out that this kind of information is out there is frightening.

When you talk about, for example, the schematic of a city and the threat level, and then we think about this report that just came out about Al Qaeda trying to do things in this country, the idea that, in the hands right now of somebody who wants to do some harm, they have the necessary information to effectively—and this is some serious stuff. In the past we have heard about them taking pictures of the World Trade Center and things like this.

What we are saying here, if I understand you correctly, it is quite possible that they actually have the information to be most effective and efficient in bringing hell to this country.

So I guess what I am thinking about, General Clark, you said something, and the chairman took you a little farther down the road. I want to bring you back. It is one thing to find out who got the information. It is one thing to find out who is searching for it. It is another thing to know what is already out there.

See, that is what bothers me. I mean, it sounds like, Mr. Boback, you all want to work with the Government and try to figure out how we can address these issues, but a lot of stuff is out there and it seems to me that this is something that would call for the utmost urgency or we may find ourselves sadly in a worse situation than 9/11 because now they may have the kind of information that they could do a whole lot of harm.

Again, from the national intelligence estimate report, they talked about how Al Qaeda is trying to find all kinds of ways that we might least expect to bring massive harm to our country. I just want you to comment on that. And what can you all do?

I mean, if I am looking at this on C–SPAN, I am asking the question, all right, I have heard all of that. Now, what can we do to make a difference? What can the companies do?

And the other thing that we have to keep in mind is not everybody is sophisticated in all of this computer language as you all are. So I am just wondering can you just help me with that, or anybody else.

General CLARK. Well, first of all, Congressman, I think your statement of the urgency of the problem is accurate. I think it is an urgent problem. We do not know what is already out there.

In the case of the information on the city vulnerability, of course, we immediately contacted the contractor and the city and so forth. They denied the problem. They don't understand what has been leaked.

So the first thing we need are some pretty hard-nosed policies about businesses and Government contractors that simply prevent people from doing Government work on computers that have anything to do with the P2P network and have LimeWire or any of the other file-sharing information on it. Even when people are sophisticated and understand LimeWire and are sophisticated with computers, they can still make a mistake and all that material could be gone in an instant.

The woman who had the Sipranet backbone was an experienced woman in IT infrastructure. That was her specialty in the Department of Defense. Yet, she had inadvertently broadcast it.

So I do think that it is an urgent problem. I think that strong policies can help. I think a dedicated search effort needs to be run on some of the key sensitive items or sensitive terms. Tiversa is in

discussions with the Department of Defense and National Security Agency now to try to start doing it. But the horse is out of the barn, and unless we have some specific key words that we want to follow, it is almost impossible to know what could be out there. Anybody who wrote a draft of a secret document at home, brought it into the office on a hard drive, loaded the hard drive in, prepared it in the office, took it back and worked on it at home in the hard drive, and his daughter uploads the music-sharing program, that document could be out on the Internet.

So there is just no way of knowing everything that is out there right now. What we do need is, as soon as possible, an active monitoring program, and we need a greater awareness and the right policies in place in our Government agencies.

Mr. BOBACK. Mr. Cummings, I think you are spot on on the process that you suggested. First, we do need to assess what information has been disclosed across the board using specific terms that are provided by the various agencies of information that they are interested in protecting. We also need to know where did that information go, who has it, and what are their intentions.

If I may, early on in Tiversa's history we actually provided information. We saw an individual searching for pictures of the President's daughter, not that specific. Then they issued a same search that said pictures of Air Force I. Again, not that impactful. Then they issued a very specific search that said active White House security force, which obviously prompted our concern and said what is this person looking for. We file shared with the individual to say, what other files do you have? Let's download some of the files that they have actively already downloaded. The person had, I believe it was 47 files of sniper, sniper training, sniper tactics, avoiding police investigations, extensive training in sniper tactics.

We immediately alerted the U.S. Secret Service. The Secret Service actually showed up at my doorstep 6:30 in the morning to retrieve this information, and we were able to locate the individual. When the Secret Service found this information that individual was 55 miles away from the Crawford Ranch. Criminals are using this information today. We need to find what is out there. We need to find it right now.

Chairman WAXMAN. The gentleman's time has expired.

Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman.

I know we have piled on pretty good on all the things that can happen, and I am just going to pile on a little more quickly and then ask a couple of questions.

I think it is humorous that I have in front of me Charles Fuller's Alternate Pistol Qualification Course. This is a Tradoc document, Wes. He got 132, 33 hits out of 40, so he is pretty fair. That could be humorous.

Now, a little like that other document, I have Mike's credit cards and accounts, including all the passwords. I can't even redact this and turn it in for the record, because all you would have is staples followed by everything redacted. A MasterCard, AMX. Everything redacted. It is exactly that. It is everything that you want to keep secret. I don't know whether it was Mike that messed up, or Mike's son or daughter, but it happened.

This one I am not going to turn in for the record, but I will be contacting the 101st Airborne Division Air Assault, because I have 20—and I could have had 200—records of orders. Clearly, this was not an individual. This was an asset that either had directly or indirectly permanent change of station and other orders, each one with Social Security number, name, rank, and date on it. I guess the kids don't actually come in on Saturday into the commanding officers' office and download LimeWire, but maybe somebody did it.

There is an elephant in the room, and I figure we have all missed him, so, Mr. Gorton, I want to talk to you for a moment.

You know, we have been talking about you and we haven't given you a chance in the Q&A, so I am going to give you that chance. Last year we held hearings on steroids and we put Major League baseball players where you all are. You are all handsome, but you don't quite—except for you, actually. Nobody else up there looks like a current baseball player. At the end of it all, professional baseball banned steroids and made it very harsh to use them.

We are here today talking about the defaults on your software—essentially, just hit enter, enter, enter—making all these things happen, or be able to happen. Do you feel any obligation today that you should change your defaults to secure, secure, secure as a result of what you are hearing here today?

Mr. GORTON. I think right now the defaults are secure. So if you just go hit enter, enter, enter using LimeWire you don't share any files and there is no information that would be on your computer that would be made public to anybody.

Now, I think what you have here is a situation where people override the safe defaults and end up disclosing things that they didn't mean to disclose, and clearly that happens more than it should.

I had no idea that there was the amount of classified information out there or that there are people who are actively looking for that and looking for credit card information.

Mr. ISSA. Now that you are aware of it, the first question I am going to ask briefly, because I will run out of time pretty quickly, is, are you prepared here today to say you are going to make significant changes in the software to help prevent this in the future?

Mr. GORTON. Absolutely. And we have some in the works right now.

It seems like, as far as I can see, there are two big categories of things that we can do. One of them addresses how people share directories and folders. I think probably a lot of the information that gets out there now is because people accidentally share directories that they wouldn't mean to share.

We have warnings in the program that currently warn people when they try and share directories that they shouldn't be sharing. Clearly, those warnings are not enough, at least in a handful of cases.

Mr. ISSA. Let me ask you a final question, and others may answer it also. We did not heavily weight today's panel with lawyers, but many of us on this panel up on the dais also serve on Judiciary. Would it surprise you if you have a string of lawsuits for inherent defect in your product if people like Charlie Mueller of Missouri—I will say no more—finds out that he has lost his IRS filings

and finds he has been damaged? Would it surprise you that you would be potentially not dismissible in tens of thousands or hundreds of thousands of venues around the country for your software, even inadvertently, but in their opinion being defective, you know, causing these releases? Would that surprise you?

Mr. GORTON. LimeWire has always tried to make the program clear and easy to understand for users. I think it works for the vast majority of users. There is clearly a minority who make mistakes using the program, and those mistakes can have consequences more serious than I ever imagined. So we want to work to fix that. I mean, I am not a lawyer and I honestly can't tell you the legal answer to the question you asked.

Mr. ISSA. Well, I will tell you, and then I will return the balance of the time, but I would not be surprised that, not only on the part we are not talking about here today, which is all of the proprietary music and video that is being downloaded by people who may not have been properly warned by your software that they were violating copyright laws in essentially publishing this, but also in these people who feel they have been damaged.

I would hope today that you are sincere in what you are telling us, that very quickly you are going to make each and every change and encourage your industry to, because with what we got in a quick scan it is not anecdotal. This is not once in a while. This is happening, I am going to guess, more often than not by your users.

I yield back and thank the chairman.

Thank you, Mr. Issa.

Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman.

I thank all of the witnesses for testifying here today. I think it is apparent to someone like myself, who is not all that computer savvy, that this is a problem that can affect every type of computer. It is important to families who could disclose financial information and other personal matters, families, businesses, and goes right on down the line. So is this a matter of people just carelessly using their computers, or does it go to even more sophisticated people who are experienced on this who have also been affected by it? Mr. Boback.

Mr. BOBACK. Thank you for the question, sir. It is experienced users. It is not just careless users; however, careless users do play a role. It is also important to note that it is not only LimeWire, that Tiversa has evaluated over 200 applications. LimeWire is just one of over 200, most of which are not U.S.-based and will not follow U.S. law. So I commend Mr. Gorton for coming forth today and doing that. However, the problem is widespread across the network. Again, it is not just the inexperienced user.

Mr. TIERNEY. Mr. Gorton, do you share that perspective?

Mr. GORTON. I have to say I am probably a little less informed on this issue, in some ways, than Mr. Boback, because he is searching the network looking for this stuff. He probably has a better grasp on that.

I think I have always felt that it was inexperienced users who didn't know what they were doing; however, when you see documents coming from people who specialize in computer security about military documents, it really makes you think twice.

My first job after grad school was working at Martin Marietta, where I worked with classified information. We had very tight protocols as to which computers you could use information on and who was allowed to use those computers. The fact that classified documents are ending up on home computers I think is a little disturbing and that is sort of a separate point. It is surprising to me that professionals in this field would do that sort of stuff.

Mr. TIERNEY. I am going to ask a question. I would ask each member of the panel to answer briefly, if possible, from right to left. Can we legislate policies that will positively impact this situation? Or is there something different that Government agencies should do to protect at least the Government information? And how do consumers protect themselves?

Maybe, Mr. Sydnor, we will start with you and move right along.

Mr. SYDNOR. Can this problem be legislated away? Probably not. As Mr. Boback indicated, there are peer-to-peer applications that have developed overseas. They are available over the Internet. Some of the developers are beyond the reach of U.S. law.

Could legislation be part of a solution? Certainly. One of the problems that we documented in our report, the trouble with them is a lot of them were identified very, very clearly, spelled out specifically in the 2002 study that led to this committee's 2003 hearing, and those lessons have not been learned.

Some of the problems that still exist in the programs are exactly the problems that are documented in that study. Self-regulation certainly had a chance to work and has not been entirely effective.

As far as how consumers can protect themselves, I believe Mr. Boback might be able to speak to that. In doing the study, we tried to look and think about, if you wanted to keep these programs off your home computer, what would you do. The short of it is we really did not think there were great answers that would be particularly accessible to a normal home computer user.

So, for example, I do understand that this is a serious risk. Is there anything I can do at the moment to keep somebody from signing one of these on one of my computers? Not very effectively. If it try to use very lock-down settings on the firewall, it will not prove to be practical on a day-to-day basis.

Mr. TIERNEY. I'd like to jump to Mr. Boback. I am sorry to interrupt, but I will skip all the others after saying I was going to ask everybody, but since you were mentioned, Mr. Boback, what do you think about that? What is a consumer to do?

Mr. BOBACK. As we recognized this problem several years back, we started to extend our services that we provide to the largest corporations in the country. We wanted to try to develop a product that would protect consumers from this inadvertent issue. So we actually just launched a product that we call File Detector. What File Detector does is it causes an ink stamp of the drive, itself. In layman's terms, it causes a marker to be put in each individual file such that the user now cannot be duped. And when I say duped, I mean that with respect to Mr. Gorton. They cannot be tricked or an executable cannot be acted upon that computer that will allow a shared folder to be shared.

So we constantly monitor the network, but if I can access your My Documents file, for example, if I can access that file that I put

in there without seeing any other information that the individual has, then that system is now subject to inadvertent file sharing, so we are now offering that product, as well. We just started to offer that to consumers. It is an extension of our product to corporations.

If I may, legislatively, the legislation should be enacted to protect this Government information, particularly on Government computers, particularly the classified information. That information can be scanned. We can provide it globally. Other systems can also look at this information, but we see the puzzle in its entirety rather than looking at a piece, which is why most corporations don't understand this problem. They make assessments and audits looking at one piece of a one thousand piece puzzle. We have the entire puzzle put together and can make very accurate assessments associated with it.

Mr. TIERNEY. I yield back, Mr. Chairman.

Chairman WAXMAN. Thank you, Mr. Tierney.

Mr. Cooper.

Mr. COOPER. Thank you, Mr. Chairman.

The title of this hearing is Inadvertent File Sharing. It is important to remember that intentional file sharing is probably the backbone of this entire industry. In representing Nashville, TN, I probably have more victims of this theft of property than the representative of any other District, with the possible exception of the Los Angeles or New York areas.

Mr. Gorton, you strike me as one of the most naive chairman or CEOs I have ever run across. As Mr. Sydnor pointed out, most of these problems were disclosed and available years ago. The FTC has brought some significant enforcement actions and succeeded, and yet—and I hope you don't have a family, because if you do some of your own personal information may have already been in danger, although you probably have taken appropriate defensive measures yourself, since you must be a software expert.

But it strikes me as an odd situation where you essentially are in the business of making and distributing skeleton keys, and Mr. Boback will help everybody buy new locks, and then, with your business plan of remaining one step ahead of the law, then you will probably make and distribute burglar tools, and then Mr. Boback or someone else will further improve the locks. So we are going back and forth.

You call for regulation, saying that Congress is the only entity with the power to step in here. I think it has already been established that there are hundreds of companies from outside U.S. borders that we do not have legal jurisdiction over, so it is going to take more than congressional enforcement, new laws, to try to solve this problem.

If I were you—and obviously I am not—I would feel more than a shade of guilt at this point for having made the laptop a dangerous weapon against the security of the United States. The 9/11 Commission reported that the central failure was a failure of imagination. Mr. Gorton, you, in particular, seem to lack imagination for how your company and its product can be deliberately misused by evildoers against this country.

Imagine someone downloading the material necessary to go after the President of the United States's daughters. You just didn't know.

Members of this committee, as Mr. Issa has already pointed out, have been able to download, themselves, unbelievable information, and you didn't know.

Well, I hope you care, because this is an abuse. The Internet is a shining, wonderful technology, and to have this pollution be so easily available—and remember, the business plan of many companies is to promote illegal copyright infringement. Today we are just talking about inadvertent use of peripheral problems.

So it is such a shame that we are not using the productive minds of this country to have cleaner, better uses of this fantastic thing. I appreciate your bravery in being willing to testify today, but, as Mr. Issa pointed out, I would think you would be the target of multiple suits at this point, as you helped produce the skeleton keys, the enabling software, to do a lot of damage, including to the security of this Nation.

I would be delighted, with my time remaining, to give you a response.

Mr. GORTON. Well, I guess there are several points you made there.

First of all, I absolutely want to do everything in my power to fight inadvertent file sharing. I am sorry to say that I didn't realize the scope of the problem. You say I lack imagination. Perhaps that is true. But this sort of series of events, I didn't have the imagination to imagine that computer security experts from the Government would be publishing their information publicly. But I do want to combat the problem and I do want to be part of the solution.

As to the copyright infringement that you pointed out, copyright infringement is clearly a problem on peer-to-peer networks. The solution that I am advocating, which involves regulating the ISPs, is one that cannot be circumvented by foreign software makers, because every computer in the United States is connected to a domestic ISP. There is no such thing as a fly by-night ISP. They are all very large companies with large capital investments and wires in the ground and things like that. They are all subject to U.S. regulation.

If it was the policy of the United States that those ISPs could not keep connected to their network computers engaged in illegal activity, then I think you would see that consumer behavior would change rather rapidly, because I think P2P is a great technology, and I am pleased a number of people here have said that. But clearly we have a way to go before the good parts of the technology stand alone without the bad parts standing so tall next to them.

I want to come here, because I have thought a lot about this problem. Clearly, there have been previous solutions before. There has been action in the courts, and we have certainly had talks with media companies and things like that. Generally, in my talks with people who are performances engaged in this topic, I have found them not to have a sense that this is a solvable problem. Generally, most of the people I have met sort of feel like this is a hopeless problem, and it is not a hopeless problem. It can be solved. I would be happy to talk to anyone about that.

I think I have laid out the bare bones of my ideas already.

Chairman WAXMAN. Thank you, Mr. Cooper.

Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman.

This hearing has been particularly disturbing to me. I am not in the computer field. I have used computers a long time. I am now thankful that, although I have been involved in the media and entertainment industries, I am a dinosaur and I have not engaged in P2P file sharing, and so I am thanking my lucky starts that I simply haven't had the time to put myself at that kind of risk.

Mr. Boback, would you comment on the suggestion that regulation of ISPs is the way to solve the problem we have been facing today?

Mr. BOBACK. We looked at that as a solution as we found this early on, as well. One of the problems with implementing an ISP solution is that the amazing amount of traffic that has to go through these systems, if you were to put a hardware device at the ISP, that would create a choke point and information would have to be analyzed at the ISP. It would, in turn, slow down usage across the network, slow down.

The reason why Mr. Gorton testified that users don't want that is because users want increased speed. They don't want decreased speed. They don't want the pictures to slowly load back to dial-up.

Solving at the ISP is not—we want to solve it at data at rest, not data in transition, trying to catch it as it passes by on a freeway and snatch it off. We want to find it where it is at rest and keep it at rest, where it should be.

Mr. HODES. Ms. Engle, in 2005 the FTC staff concluded that P2P file sharing, like many other consumer technologies, is a "neutral technology which risks result largely from how individuals use the technology rather than being inherent in the technology, itself." I suppose, based on what we have heard today, compared to a time bomb, you are right. It is a neutral technology.

Does what you have heard today change your view about the inherent risks in P2P networks? And does it give rise for you to an you thoughts about what you ought to be doing to help cure the issues we are discussing today?

Ms. ENGLE. It is certainly true that P2P technology causes these substantial risks about sensitive data getting out. We have certainly seen that there is a lot that individuals and businesses and the Government can to do better secure their data.

We have all heard about lost or stolen laptops, for example, that have left very widespread breaches. That having been said, the PTO report raises some very difficult, serious questions about the design of the technology which has not been previously brought to our attention, and we are looking at it very closely to see whether further FTC involvement in this area is appropriate.

Mr. HODES. Thank you.

Mr. Mintz, because you are the CIO at a Government agency, I want to direct the next question to you. It sounds to me—and from some of the other hearings that I have been part of, for instance, I'm part of the Subcommittee on Information of this full committee—that Government agency protocols may not be adequate at least to begin to address the problems we have been facing today.

Do you think that current Government agency protocols which are designed to prevent inadvertent P2P file sharing are in place? Do they need to be beefed up? If that is so, what is the touchstone? Where is the central place to go to make sure that, throughout the Federal Government, we are dealing with this at our agencies? Or is it a matter of legislation from Congress?

Mr. MINTZ. I would say that the place that I would look in terms that the biggest issue is—I think Congressman Davis talked about this—the FISMA report and making sure that this review process looks at this technology.

In terms of policy, we have what we need. I am not saying we do it right, but we, in fact, have peer-to-peer policy in place. We have as policy you are not supposed to use it on any computer that has Government information on it.

One of the challenges we have, particularly with people working at home so much, is that people don't always pay attention to it. So the question is: what is the kind of oversight that we have to put in place? And perhaps the oversight on us to make sure that we are really pushing the policy as opposed to just putting it on a piece of paper. But we have enough authority right now to take care of the network, in terms of our own networks and the employee use.

Mr. HODES. Thank you. I see my time has expired. Thank you, Mr. Chairman.

Chairman WAXMAN. Thank you, Mr. Hodes.

Mr. Welch.

Mr. WELCH. Thank you, Mr. Chairman.

Mr. Boback, the sensitive national security information that you mentioned, General Clark testified to, that was picked up off of LimeWire?

Mr. BOBACK. That was picked up off of multiple peer-to-peer applications, one of which was LimeWire, yes.

Mr. WELCH. OK. Mr. Gorton, do you have any knowledge about how much usage of LimeWire involves people getting sensitive national security information?

Mr. GORTON. No. Most of what I know about that I have learned in this room today.

Mr. WELCH. How many subscribers do you have?

Mr. GORTON. There are, on a monthly basis, about 50 million users of LimeWire.

Mr. WELCH. And what is the purpose for which most subscribers go to your site?

Mr. GORTON. To share files.

Mr. WELCH. Well, I know that, but the nature of the files.

Mr. GORTON. Most of them are media files.

Mr. WELCH. They are what?

Mr. GORTON. Media files.

Mr. WELCH. Media as in music?

Mr. GORTON. Music and video.

Mr. WELCH. And what percentage of your subscribers would be getting music files?

Mr. GORTON. I don't have those numbers. I mean, the ones that Mr. Boback had earlier sound approximately right to me.

Mr. WELCH. Wait a minute. How long have you been in business?

Mr. GORTON. LimeWire was started in 2000.

Mr. WELCH. And I assume that you do analytical work to determine how your business plan is working?

Mr. GORTON. No. I mean, we don't do any analysis of what goes on on the network. We make a piece of software and we distribute it. So I have a general idea of what goes on on the network because I read the papers and I talk to people, but we don't have any analytical——

Mr. WELCH. It is not relevant to you why more people might be coming onto your system or less, depending on how your system is operating?

Mr. GORTON. I mean, we make a great effort to make the LimeWire program easy to use and clear to understand so that our users have a positive experience.

Mr. WELCH. But I was looking for an answer to the question.

Mr. GORTON. And what was the question?

Mr. WELCH. The question is: how many of your subscribers go on there for music?

Mr. GORTON. I mean, like I said, I don't know specifically, but, you know, he said 38 percent of the files were MP3s. That sounds plausible to me.

Mr. WELCH. We have some data here that says in January 2005 your market share was about 21 percent. This is people looking to get music downloads. Does that sound about right?

Mr. GORTON. That is 21 percent of what?

Mr. WELCH. Households.

Mr. GORTON. So 21 percent, that could be correct. Yes, that sounds——

Mr. WELCH. And it is now up to about 75 percent.

Mr. GORTON. That sounds a bit high. I mean, 75 percent of households?

Mr. WELCH. That are looking for music downloads, get their music downloads through LimeWire.

Mr. GORTON. I mean, LimeWire is the most popular file-sharing application in America.

Mr. WELCH. Music file sharing?

Mr. GORTON. Well, all types of file sharing. Music is a large use among that.

Mr. WELCH. Let's get to the point here. I mean, the main reason people go to LimeWire is to get music.

Mr. GORTON. Certainly one of the biggest, yes. They also get videos.

Mr. WELCH. Is this a complicated question? Do they go there for music or——

Mr. GORTON. Yes, they go there for music.

Mr. WELCH [continuing]. National security data?

Mr. GORTON. Hopefully not for——

Mr. WELCH. What is so hard about this question? Is it national security or is it music?

Mr. GORTON. The only thing that competes with music is video.

Mr. WELCH. All right. Are you familiar with the Grokster decision?

Mr. GORTON. Yes.

Mr. WELCH. June 2005.

Mr. GORTON. Yes.

Mr. WELCH. And you, I am sure, are aware that you went from about 22 percent, 23 percent, to 75 percent of market share after that, correct?

Mr. GORTON. It actually happened before the decision.

Mr. WELCH. Started to go a little bit before. And do you know what happened? Some of your competitors are Imesh, BearShare, Kazaa, correct?

Mr. GORTON. Yes, or used to be.

Mr. WELCH. All right. And, subsequent to the Grokster decision, they installed filters in their system, correct?

Mr. GORTON. Yes.

Mr. WELCH. Making it impossible or very difficult for individuals who are seeking to get music, infringing without respecting the copyright, to do so, correct?

Mr. GORTON. Yes.

Mr. WELCH. And have you installed the same type of filters at LimeWire?

Mr. GORTON. Yes. At LimeWire we have built a filter that allows copyright holders to flag specific files as——

Mr. WELCH. I am going to ask you a favor.

Mr. GORTON. OK.

Mr. WELCH. I am going to ask you to answer the question I asked——

Mr. GORTON. Yes, we have a filter.

Mr. WELCH [continuing]. Not the question that you would like me to ask.

Mr. GORTON. Yes, we have the filter.

Mr. WELCH. It is a little bit more. You have offered, if I understood your answer, to permit an individual, if I go on to LimeWire, to opt into the filter, correct?

Mr. GORTON. Yes.

Mr. WELCH. And your competitors, they have installed a filter at the site; yes or no?

Mr. GORTON. When you say site, I take it, I mean, the file-sharing programs are not Web sites, so——

Mr. WELCH. They have a filter, so if I ask for a particular song it will be blocked when I go to BearShare or Imesh or Kazaa.

Mr. GORTON. The functioning of the LimeWire filter is substantially similar to that of other file-sharing companies.

Mr. WELCH. But it is elective. I, the user, have to say I want that filter?

Mr. GORTON. Yes.

Mr. WELCH. But the other competitors, after the Grokster decision, they have installed it so it is not an election, right?

Mr. GORTON. Yes.

Mr. WELCH. All right. And that is a modest difference. If I am a person who wants to get music in violation of a copyright, and I am offered the opportunity to not get it when I go seeking it, most of the time I will probably ignore the offer that you have given me.

Chairman WAXMAN. Mr. Welch, your time has expired.

Mr. WELCH. Mr. Chairman, I thank you. I just find that there is an interesting inter-connection between teenage music and national security.

Chairman WAXMAN. Thank you.

Mr. Yarmuth.

Mr. YARMUTH. Thank you, Mr. Chairman.

It occurs to me, Mr. Chairman, that after today's hearing we may have found an alternative to subpoenas in trying to get information from the administration that we haven't been able to get. [Laughter.]

Mr. Sydnor, the PTO report design is long and detailed and very technical. I would like to cut through some of that and ask you a very simple question: do you think that users that download P2P software applications are being tricked into sharing files that they would not ordinarily share?

Mr. SYDNOR. Yes. They are inadvertently sharing files they do not intend to share. In the report we attempt to explain why, although the user does not intend that result, that result may have been intended by others. That is not a question we purport to be able to answer based on the publicly available data that we were able to review.

But the short answer is yes, people are making catastrophic mistakes with these programs. Although we have focused today on perhaps the most high-profile incidents, it is all too important to note, as was just discussed, a lot of the files that are traded over these networks are copyrighted. If people are inadvertently sharing copyrighted files, they are violating the law and they are setting themselves up for an enforcement lawsuit.

That is also a very important part of the problem, and people who do not want to be distributors of pirated goods on these networks should be able to make that choice and have it be very easy, and right now it is simply not.

Mr. YARMUTH. Maybe the answer is obvious, but explain the benefits of tricking users in this way.

Mr. SYDNOR. Well, that was the question that sort of prompted us as we began working on the report, because it was just stunning to see that, after this committee's 2003 hearing, features that really are incredibly easy to misuse—you can go to an interface and use programs that looks like you are doing nothing except choosing a place to store files, like you are using the Save As button in Microsoft Word, and you end up sharing recursively all the folders on your computer. Very easy to make a catastrophic mistake.

The problems were very well documented. This committee called additional attention to them. Yet, they persisted.

That type of feature we found in four out of five programs that we looked at after this committee's hearing, after usability and privacy, and that led to the question why would anyone continue to do this.

In trying to think about why someone might do this if they knew or really should have known that this was going to cause problems, why would you keep doing this?

The only thing that we could see is that if people make mistakes with these—we call them share folder features—what they tend to do is they are trying to store files in a place that will be easy to find. They pick either root directory C or My Documents folder or maybe My Music. You pick any of those three. You pick your root directory, you share the whole hard drive. You pick My Documents,

you will share all the data files you care about. You pick MyMusic, you will share all your entire collection of audio files that you may have ripped from lawfully purchased CDs.

In each case, though, in addition to all your personal data, you will also share My Music. The access, as Mr. Gorton mentioned, to media files, there is also a My Media folder, subfolder of My Documents. That is driving traffic on these networks. That seemed to us to be a possible explanation for why this conduct continues. It would have catastrophic consequence for users, but it would also put more infringing files on the network.

Thank you.

Mr. YARMUTH. Thanks.

Mr. Gorton, do you share Mr. Sydnor's analysis? Do you have another perspective?

Mr. GORTON. Yes. I think my perspective is maybe a little bit more benign. I don't think there are sinister motives behind this. I mean, I can certainly speak for ourselves. I mean, we have been trying to build a program that is easy for consumers to use that allows them to share files.

In the case of the root directories, the C directory, and the My Documents directory, LimeWire pops up a warning that says, you know, be careful, you could share confidential information, when they try and share those folders. So we recognize that this is a problem. We try and warn consumers.

Clearly, some people are not paying attention to our warnings, and we need to do a better job of making it very, very, very difficult for users to accidentally share files. But I think there is a difference in opinion that probably has more to do with motive than the result.

Chairman WAXMAN. The gentleman's time is expired.

Mr. SYDNOR. If I could clarify one point?

Chairman WAXMAN. Yes.

Mr. SYDNOR. It is not accurate to say that if users share a sensitive file like My Documents or documents and settings that they will share all the files of all the users of the network, that they will get a warning indicating that they are doing something that could be dangerous. There are three different interfaces in LimeWire that can share folders.

One of those, the most obvious, is, of course, the sharing interface. If the users happens to be in that interface and they happen to try to share a folder like documents and settings, they will receive a warning saying, this folder may contain sensitive information, do you want to share this folder? If they are in one of the other interfaces, they won't receive any warning. They won't receive that warning. So from the LimeWire library you can share documents and settings. You won't get a warning of any kind.

The warning that they get doesn't provide them critical information, because it says, do you want to share this folder? I can look in My Documents and settings, and there is a documents and settings folder on my computer, there is no sensitive information in it. No sensitive files. But what I am not being told is I am not going to share just this folder; I am going to share all of the folders that are subfolders of it. This is a problem that was documented

in the usability and privacy study that this committee highlighted in its 2003 hearing, and it is still going on.

Chairman WAXMAN. Thank you, Mr. Yarmuth.

Ms. Watson.

Ms. WATSON. I want to thank you, Mr. Chairman, and all the witnesses. I know that as we create more and more higher technology, there is always a way to use that technology in a cynical way.

I represent Hollywood, and we also have here in Congress a Protection of Intellectual Property Caucus, because, as you know, our creative works are every day taken and duplicated around the world. I am just fascinated when I go into a foreign country how our products are sold for such little money and the profit never gets back to the creators.

So as we develop this technology so that peers can share with each other and it can be done quickly—you know, we are in a hurry in this country, and it is spreading around the globe. We want information immediately. We create holes and glitches. We saw the results of the computer codes where 19 million veterans' Social Security numbers were stolen. We saw 2.2 million active duty military personnel information that was part of this data exposed; 1.1 million active duty military personnel had their names, Social Security numbers, and birth dates in this data base, and that was some way taken.

So we have some real, real holes and glitches and problems that we must address. We have held hearings, and there is technology that can protect or can trace the artful products that are being duplicated illegally, but I throw this question out to all of you. You just might want to answer in a 20 or 30 second clip.

What do you know that we can do to protect this most sensitive data, to protect intellectual property? And what can we do for the future? Is the technology there to guarantee that the businesses in my District can protect their property so the creators then can enjoy the benefits of their work and so that those who are in the military, General Clark, can feel secure that their most vital information is protected? So can you just go down the line and tell me what you see needs to be done, starting with Attorney Sydnor.

Mr. SYDNOR. Thank you, Representative Watson. What can be done? Certainly I know that the content industries are working hard to find technological ways to both protect their content and exploit the opportunities that the Internet provides. Potentially, it could be a wonderful tool for both content creators and users of content.

As someone who is more of a user than a creator, I think one of the important aspects of all that will be that we need to make sure that, as content is distributed over the Internet, it gets to consumers in ways that they are basically safe to use. That is a big part of this whole problem is, you know, right now, you know, it certainly is tragic to see, with the peer-to-peer file-sharing networks, really the first time copyright enforcement against end users. Hopefully, by more action by some of the middle, those sort of situations can be a thing of the past, I would hope.

Ms. WATSON. Thank you.

Ms. Engle.

Ms. ENGLE. Well, I am definitely not a technology expert and can't really offer views——

Ms. WATSON. But what do you think we need to do?

Ms. ENGLE. Well, I think the kind of attention that this hearing is putting on this issue is extremely important. The more consumers and businesses and especially Government agencies know about this problem, the more they can take steps internally to prevent further breaches.

On the side of intellectual property protection, setting aside for data security, I think we have seen the industry innovate on its own to make legal methods of downloading more available, and it is helping in that area.

Ms. WATSON. Thank you.

Mr. Mintz.

Mr. MINTZ. I can't speak in terms of the consumer industry so much. In terms of the Government information, as I have said, I think the biggest focus we have is making sure that the policies and the technologies we have in place right now are followed and protected, and to become more aware of the fact that there is a lot of this kind of software, particularly in terms of the home use. I think the publicity, even the attention the committee puts on this, is very helpful. It has brought a lot more attention to the Department for these kinds of issues.

I think you are faced with a big challenge, as a number of other members of the panel have talked about. A lot of this activity is international in scope, so the question is what do you do about that, also.

Mr. JOHNSON. Education is the key right now. I am working with financial firms. They have been quite successful in educating consumers about phishing, and this is a case very similar to that.

But one of the things I think that has to be thought of over and over again is that in this program case, when information is leaked it is out there, and the digital wind will carry it everywhere. It is very hard to get it back. It is a very different kind of concept than what we are used to, a physical piece of paper that we can go grab and bring back and put in the filing cabinet. Once that information is out there, it is going to be blown around and spread, and very, very hard to control.

Mr. GORTON. I think there are two separate issues that you are talking about here. One is the release of classified information with inadvertent file sharing. Certainly LimeWire can be part of the solution by improving the functioning of our program. I also think companies like Tiversa can be part of this solution by providing technologies which allow notice and monitoring of the networks.

On the front of copyright infringement, as I mentioned before, I think the ISPs need to be part of the solution. There are proven technologies out there that work. The USC and UCLA have policies in place, these warning systems that result in the disconnection of students' computers who continue to engage in copyright infringement. Those universities have succeeded in suppressing the problems of copyright infringement on their campuses, and I think we can use that successful model. That can be rolled out across the country so that it is not just a handful of universities that have

successfully dealt with these problems, but can be the entire country and all the ISPs.

General CLARK. As far as classified information is concerned, I think the Government is aware of the right policies; that is, to keep file-sharing applications off Government computers and to separate the Government and personal computers. I don't think these policies are always enforced appropriately, and until now there is a lack of the ability to monitor through the peer-to-peer space to determine whether there are violations.

What we detected with Tiversa's software is we have now got the capacity to monitor, and we can, to protect these from violations. So I think that, in addition to the separating Government and personal, preventing file-sharing applications, that you have to do some defensive monitoring of the peer-to-peer space so that you know what is out there, you know if you had had any compromises of information. You can do the investigations and followup work to seal off that leak of information and to prevent it from happening again.

Mr. BOBACK. And I echo the other speeches about the education being a first step. I also echo General Clark's thoughts as to the auditing of Government classified information.

As far as the intellectual property issue for the media industry, that is something—I mean, my personal belief is that the media industry should look to work with the peer-to-peer to actually use that as a distribution method to find a way, as there are so many users, as Mr. Gorton has testified to. Its users are on the peer-to-peer. It would be more appropriate for them to figure out business models that act in conjunction with the peer-to-peer, rather than trying to just eliminate the peer-to-peer as a threat.

I believe that legislation in the Supreme Court, while attempting to do just that, has not succeeded, and the peer-to-peer has spread offshore. But if the media industry were to look to protect their content by including that as a distribution channel, very similarly to iTunes, looking to distribute in alternative methods, the peer-to-peer is a—I once read that there are over 14,000 movies made in Hollywood in your District each year, and less than 100 of those movies actually are profitable. The other 13,900 movies will never see the inside of a movie theater. It is not financially viable for them to distribute it in any other method. They can distribute this information, full-length videos, on the peer-to-peer. These artists could arrange, it is some work, no doubt. There are business models that need to start to look to distribute this information.

Tiversa's original work was looking in that very angle until we found the massive security issues that existed and we said, you know, as U.S. citizens we need to address this issue before a functional, viable distribution method could be found for the media industry.

I think that there is incredible opportunity for your District, particularly, to be able to distribute that additional 13,900 movies that are made each and every year and actually reap some revenue from that as the user demand goes up. There are 50 million, as Mr. Gorton testified to, users every month that are starving for content. They want this content. They have no access to it.

One of our clients——

Chairman WAXMAN. Mr. Boback, we are going to have to move on.

Mr. BOBACK. I'm sorry.

Chairman WAXMAN. Thank you, Ms. Watson.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

My questions are directed at Mr. Mintz. Mr. Mintz, in your testimony you described an inadvertent disclosure that occurred at the Transportation Department. A diligent, well-meaning employee was working on a home computer. Unbeknownst to her, a teenager sharing the family computer downloaded the LimeWire P2P file-sharing program. Next thing, the Government employee's work documents are all over the Internet and the employee is being called by a reporter.

To confirm your statement here today, DOT has completed its forensic analysis of the employee's computer and no sensitive documents were compromised; is that correct?

Mr. MINTZ. Sensitive in the sense of classified, no. There was personally identifiable information. There was one piece of personal identifiable information from the Department of Defense, her own, and there was a small amount but there was some personally identifiable information from her previous job of approximately, I believe, six or seven people. That was available. We don't know if it was released, but it was available and it was sharable. Other than that, there was nothing. There were no classified documents.

Mr. CLAY. And that sensitive information——

Mr. MINTZ. No.

Mr. CLAY [continuing]. Has not shown up anywhere else?

Mr. MINTZ. No.

Mr. CLAY. OK. This example also illustrates the potential conflict between encouraging and promoting telework and the flexible workplace and data security that was exposed. Mr. Mintz, how do you balance the tension between telework and data security?

Mr. MINTZ. This is a big challenge. As a number of people here have said, the average person that is going to be using this is not necessarily computer literate or knowledgeable that we want to make use of, so one of the things we are doing is we are increasing the education process. We have already had a security leak. And we also have online training. We are increasing the training for that. Then the other activity we are doing is we are going to be moving more from desktop computers where the standard computer is a desktop computer that would always stay on a Government site, to a laptop computer, which is a Government-owned computer where we have encrypted it and we control the contents.

So for those people who are actively involved in telework, they will be using Government-owned equipment. That will be done over a period of time.

Mr. CLAY. And you think that will be more secure than what is used now?

Mr. MINTZ. It will help. The reality is that at the end of the day you are always dependent on the procedures that people follow. A user could always work around any security environment. But we think it will make it more secure.

Mr. CLAY. In this case, Mr. Mintz, it appears that very few, if any, measures were taken to protect the employee's computer or the work product she produced. She is working from her home computer, which was shared with other members of her family over her own Internet connection; is that accurate?

Mr. MINTZ. Yes.

Mr. CLAY. And was this in compliance with DOT telework requirements?

Mr. MINTZ. Yes. The telework requirements were that she was not to keep personally identifiable information on a non-Government-owned computer, and, except for her own, at least from the Department of Defense, she did not.

She did make a mistake. We talk about that. When she left her previous employment, chances are she should have deleted that information. We have added that as a process at the Department, to remind people to do that.

Mr. CLAY. Does the Department need to revise its telework program?

Mr. MINTZ. We are going to have to enhance, at a minimum, the training, and we are going to have to give increased advice to employees as to how they set up their own personal computer. And, as I have said, we have to do a better job of auditing the process to make sure that people are reminded of the responsibilities. Just putting the policy in place is clearly not sufficient.

We have set up a Tele-Work Committee led by the sponsorship of the Deputy Secretary to look at these issues. The IT CIO has a representative on there. My office has a representative on it. We are very active in looking at those policies, but we are going to have to re-look at all of them.

Mr. CLAY. Thank you for your responses.

Mr. Chairman, I yield back.

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

I want to thank the members of this panel, as well, for your presentations to us. I think it has been a very useful, helpful, constructive hearing, and I appreciate the Members asking so many probing questions.

Clearly, this issue merits further review and closer analysis. Although most agree P2P technology has great potential in its present form, it appears to come with significant risks. We need to figure out if there is a way we can protect national, corporate, and individual security without hindering lawful innovation in this area. That is a challenge for all of us and we need to work together.

That concludes our business today. The hearing stands adjourned. Thank you.

[Whereupon, at 12:15 p.m., the committee was adjourned.]

[Additional information submmitted for the hearing record follows:]

WRITTEN STATEMENT OF

MR. SAFWAT FAHMY,

CEO AND FOUNDER, SAFEMEDIA CORPORATION

FOR THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

"INADVERTENT FILESHARING OVER PEER-TO-PEER NETWORKS"

JULY 24, 2007, 10:00 A.M.

ROOM 2154, RAYBURN HOUSE OFFICE BUILDING

Chairman Waxman, Ranking Member Davis, distinguished Members of the Committee, I want to commend you and your committee for calling this important hearing on "Inadvertent File Sharing on P2P Networks" and your dedication and persistence in educating consumers on the privacy and security risks posed by "contaminated" P2P networks.

My name is Safwat Fahmy, and I am the CEO and Founder of SafeMedia Corporation. Prior to founding SafeMedia, I spent more than 30 years in computer architecture design and software product development. I founded and served as the Chairman of the Board for WIZNET, a business to business ("B2B") e-Commerce content firm, have developed GIS systems for federal and local governments and IBM's IPCS/MAPICS.

SafeMedia's mission is to provide an effective, cost-efficient and easily implemented solution for preventing illegal transfers of copyrighted digital material and personal information via "contaminated" peer-to-peer networks. We have developed a technological solution prevents the invasion of consumer privacy by contaminated P2P applications and restores and preserves copyright holders' asset value.

There have been numerous hearings in the United States Congress to examine the uses of P2P technology – many of these hearings have focused on the use of P2P networks to illegally transfer music and movies – an activity which is especially prevalent on college campuses – and some have focused on the benefits of P2P technology generally. Candidly, as a technologist in the field of computer architecture design, I have been disheartened by the lack of understanding and smokescreen of misinformation about how "contaminated" P2P networks operate.
Mr. Chairman, I applaud you and your committee for taking a hard look at how the redistribution and search features of many popular P2P file sharing networks pose serious privacy and security threats to consumers, students, businesses and the Government.

Other witnesses will testify on the recent report issued by the United States Patent and Trademark Office on Inadvertent File-Sharing and the Dartmouth Study on the exposure of financial institutions to privacy and security breaches from P2P. I will focus on how P2P networks operate, the features and characteristics of "contaminated" P2P networks and explain how the technology developed by my company to address illegal sharing of copyrighted materials on P2P networks will help to protect consumers, students and businesses from the serious privacy and security risks that this committee is examining today.

In layman's terms, very simply, Peer to Peer networking (P2P) allows individual users to transfer files directly to each other without going through a central server. In the traditional Client/Server model, the client sends requests to the server and the server responds to these requests and acts on them. This is how the popular downloading service "iTunes" operates and this is how "MySpace" and "YouTube" work as well. In contrast, with P2P networks, each computer serves as a peer and functions as a client with a layer of server functionality – the individual peers communicate and exchange files directly.

Historically, P2P networks were developed to overcome limitations on bandwidth and processing/storage so arguably there were some benefits to using P2P networking as opposed to the client-server model. While a Client-Server network is unquestionably more secure and reliable, all information has to go through a central server, therefore the volume of files that could be handled was limited by the capacity of the server. With P2P networks, all clients provide resources, including bandwidth, storage space, and computing power. Thus, as nodes (individual peers) arrive and demand on the system increases, the total capacity of the system also increases. In contrast, client-server architecture has a finite set of servers so adding more clients could mean slower data transfer for all users. But frankly, the historic reasons for developing P2P networks do not exist in today's world: limitations on bandwidth and processing storage are easily remedied by clustering many low cost servers and the deployment of wideband fiber to deliver even more powerful performance than P2P networks.

P2P technology is clearly a usable, freely available tool for research and education and at SafeMedia we support the lawful use of uncontaminated P2P networks. The legal and innovative uses of P2P technology highlight the importance of being able to differentiate between legitimate uses of P2P and "contaminated" P2P networks.

Let me explain what I mean by a ***contaminated*** network.

One of the defining characteristics of contaminated networks is that users rarely ever know that they are sharing the files on their computer with other users of the network. P2P software, in order to work and survive, requires that most users share files. If no users shared files to be downloaded, then the network would be pointless. So, the developers of the software create a directory on the user's computer "shared" with the entire network most often without their knowledge at the time of installation.

In addition, a P2P network is only valuable to users if it has a large selection of files available to download, so developers automatically add upload capabilities to the client software so that everything a user has downloaded is now available for other users on the network to download. Without this mechanism, P2P clients would provide no value to those seeking files and would not expand and grow.[1]

From a technical perspective, a contaminated (Illegal) P2P network is a "***virtual***" network with the following characteristics:

1. Consists of many public peers who have distributed content.
2. Allows all peers to be active nodes on the network.
3. Use the peer-owned network to pass 'free riding' traffic to other peers on the contaminated network.
4. Allows uploads as well as downloads to and from other peers.
5. Has no ability to control the content on the network or what content peers upload or download.

It is no secret that in order to avoid liability for the creation and distribution of a network that allows users to illegally transfer copyrighted material, most popular filesharing networks have no accountability of ownership, contents or participants.

[1] This is why current filesharing programs are horrible at locating rare files. Since distributors of filesharing programs have decentralized their networks in response to litigation, users can only search a small fraction of the entire network and consequently, only popular files – those that are widely shared by many users – can be reliably located. Thus, the garage band that wants to get its music out to the public could not reliably use a file-sharing program to distribute its songs – since no one is likely to download a song that they can't find and don't know that it exists!

Contaminated networks use the features described in the USPTO report to induce their users to upload and download files: a default "redistribution" feature that causes users of the program to upload all files that they download, a "recursive sharing" feature that causes the program to share not only the file stored in the folder selected to store downloaded files, but also all files stored in any of its subfolders, a "partial-uninstall" feature that prevents users from completely uninstalling the program without leaving behind files that might affect subsequently installed versions of the program, and "coerced sharing" features that disallow downloads if the user reduces or attempts to stop uploads.

The Report exhaustively examines how these features have been designed and deployed since 2003, well after legal actions were being initiated against users and after the industry adopted a voluntary "code of conduct" agreeing not to engage in such practices. This example and others like it demonstrate why the U.S. Patent and Trademark Office said, "They [file sharing programs] pose a real and documented threat to the security of personal, corporate, and government data."

With my background of 35 years in the technology industry, I became acutely aware of the serious privacy and security risks posed by some P2P file sharing networks and the significant economic losses that were being sustained through illegal file sharing on contaminated P2P networks. I also recognized that technology could serve as an important part of the solution. In October of 2003, I founded SafeMedia to be a good corporate citizen and contribute to the advancement of this country. I understood that any technological solution had to distinguish between P2P networks that utilize seemingly inadvertent and anonymous file-sharing and services such as BitTorrent which require identification and consent of peers prior to the sharing of files.

I also knew that attempting to distinguish between infringing and non-infringing files would be fruitless – because many of the contaminated P2P networks use encryption and because any technology that simply blocks files or data will fail to address the dangers to consumers and businesses outlined in the USPTO study and the Dartmouth study. The only way to protect consumers and businesses is to prevent contaminated networks from freely accessing users' computers. The simple truth is that discriminating between legal and illegal content on popular P2P file sharing programs does nothing to protect consumers from the insidious features of these programs that were the focus of the USPTO report. These networks, by their features and design are "contaminated".

At SafeMedia, we have developed patent pending business solutions combining P2P Disaggregator technology (P2PD) and a Digital Internet Distribution Solution (DIDS) that prevents contaminated P2P networks from indiscriminately accessing users' computers.

P2PD is based on a new paradigm in system architecture encapsulating the total functionality of many advanced technologies on a chip, and deploying multi/hyper processing architecture created specifically for network operations, resulting in far higher, scalable processing capacity than the network bandwidth it serves. It utilizes the following technologies:

- ***Adaptive Fingerprinting and DNA markers***: The P2PD library of all P2P clients and protocols is the world's largest and most current library of fingerprints and DNA markers and is updated every 3 hours. P2PD looks for fingerprints and DNA markers in outgoing and incoming packets and, depending upon identity strength, employs many levels of analysis. In the few cases where fingerprints alone are insufficient, P2PD actually combines DNA marker evidence from multiple packets using stored evidence history.

- ***Adaptive network patterns***: Not all protocols can be easily identified with a single set of packets. As such, P2PD is set to monitor packet flows and adapt its technique based on what it has already seen and what it sees now. This extensible system utilizes "Experience Libraries". P2PD looks for patterns of certain identifiable characteristics of network events and determines if the packets are from contaminated network or not. Contaminated packets are dropped and non-contaminated packets continue on their way.
- ***Intelligent libraries:*** SafeMedia's experience libraries are knowledge-based, created from the actual operations of the subnet, and include specific logic markers in addition to the derived adaptive network pattern analyses.
- ***Remote update and self-healing***: All maintenance actions-updates, integrity checks, sanity validations, system housekeeping, and self-defense are remotely performed through SafeMedia's servers with no delay in network operation.
- ***No Invasion of User Privacy***: P2PD detection does not invade user privacy, does not record and track user IP's, does not decrypt any traffic, and allows the execution of all current security techniques (Tunneling, SSH, etc.).
- ***Accuracy:*** P2PD is fully effective at forensically discriminating between contaminated and non-contaminated P2P traffic with no false positives (i.e., identifying another protocol as the targeted protocol) whether encrypted or not.
- ***Speed***: P2PD operates at network speed with little or no latency.

Mr. Chairman, distinguished members of the Committee, the issues you are examining today are vital to the future of a secure internet where the value of digital media is protected to allow our economy to grow and expand in the global marketplace and to protect consumers, students, businesses and government from identity theft and security breaches. SafeMedia has the only technological solution available to address these issues.

In closing, I would like to share a recent "case study".

Last week, we hired a new executive assistant for SafeMedia's President Pasquale Giordano. During the course of the interview, we explained what our technology does and how it works. She said her 13 year old son had installed LimeWire on their home computer. Mr. Giordano explained the dangers of P2P and to prove the point told her she should go home and type in "tax return" to see what she came up with. The next day, she returned to the office with a copy of a tax return from Rosemary Wyatt – a resident of London, UK. She is now in the process of testing our home use product – Clouseau – to protect herself and her son from the contaminated P2P network that had been installed on her computer.

In the final analysis, a user whose identity has been stolen or a business that has had a serious data breach really doesn't care whether contaminated P2P networks were deliberately designed to deceive or inadvertently caused the release of private and sensitive information - the result is the same. The simple fact is that the most popular P2P services cannot thrive without "cooperation" from users sharing their files. If that cooperation cannot be obtained willingly, as the report's analysis shows, it will be obtained through "technological features" that "induce" users to "share."

As an experienced computer technologist, I would never recommend that Congress mandate the adoption of a *particular* technology to address the vital issues you are examining today. However, I do believe that the only way to protect individuals, companies and the U.S. economy from the dangers of contaminated P2P including identity theft is for Congress to act decisively on recommending that technical solutions be adopted that eliminate the threat of contaminated P2P. And of course, such solutions would best be achieved without putting any additional burdens on individuals using the internet. At SafeMedia, we believe we have such a

solution and I am confident that, in time, the marketplace will show that we have the best technological solution.

I am thankful for the opportunity to serve this Committee and would appreciate the opportunity to answer any questions or to provide any technical assistance or analysis that may be helpful to the Committee.

July 18, 2007

The Honorable Henry A. Waxman
The Honorable Tom Davis
United States House of Representatives
Rayburn House Office Building
Washington, DC 20515

Dear Congressmen Waxman and Davis:

The Distributed Computing Industry Association (www.DCIA.info) is a one-hundred Member-company non-profit trade organization focused on the commercial development of peer-to-peer (P2P) file-sharing technologies.

We commend you for your leadership in conducting a Hearing scheduled for July 24th to explore potential privacy and security concerns associated with the use of P2P file-sharing programs, and greatly appreciate the opportunity to comment on this important issue.

The DCIA has taken several steps to address such matters since our inception in 2003 and continues to seek further advances. We have worked closely with the Federal Trade Commission (FTC) on this and related issues. We have also provided witnesses and testimony for previous Congressional Hearings that in part addressed this subject.

We were particularly impressed with your report entitled "File-Sharing Programs and Peer-to-Peer Networks: Privacy and Security Risks." The DCIA is also familiar with the March 2007 Patent and Trademark Office (PTO) report and the more recent correspondence between the Committee and two leading US-based P2P software developers and distributors regarding consumer disclosures, default settings, recursive sharing, un-installation procedures, etc.

As we suggested to the PTO in March, please allow us to offer the Committee the DCIA's professional assistance in accelerating adoption of technological advances and related business practices to further protect P2P users against inadvertent sharing of private data.

In our view, because of both the technical complexity and relatively fast-moving innovation in this area, a federally mandated and closely monitored private sector initiative, rather than even the best intentioned legislative measure, will produce the most beneficial effect to the public and to government agencies whose sensitive and confidential information must be protected as a matter of national security.

We currently conduct several working groups tackling a number of issues, including consumer security concerns, such as the inadvertent sharing of files. These working groups can extend beyond our Membership as needed to ensure that the output of their work is widely adopted on a voluntary basis across the distributed computing industry.

The DCIA is willing to create a new working group or to charge an existing one with responding to the concerns that the PTO report has uncovered as may be more precisely delineated during your upcoming Hearing. We look forward to working with the Committee in a productive manner on these issues in a way that will significantly benefit all of your constituencies.

We will contact your offices to follow-up after the Hearing. Thank you very much for your continued interest in our developing industry.

Respectfully,

Martin C. Lafferty
CEO, DCIA

CC: Committee on Oversight & Government Reform
The Honorable Tom Lantos
The Honorable Edolphus Towns
The Honorable Paul E. Kanjorski
The Honorable Carolyn B. Maloney,
The Honorable Elijah E. Cummings
The Honorable Dennis J. Kucinich
The Honorable Danny K. Davis
The Honorable John F. Tierney
The Honorable Wm. Lacy Clay
The Honorable Diane E. Watson
The Honorable Stephen F. Lynch
The Honorable Brian Higgins
The Honorable John A. Yarmuth
The Honorable Bruce L. Braley
The Honorable Eleanor Holmes Norton
The Honorable Betty McCollum
The Honorable Jim Cooper
The Honorable Chris Van Hollen
The Honorable Paul W. Hodes
The Honorable Christopher S. Murphy
The Honorable John P. Sarbanes
The Honorable Peter Welch
The Honorable Dan Burton
The Honorable Christopher Shays
The Honorable John M. McHugh
The Honorable John L. Mica
The Honorable Mark E. Souder
The Honorable Todd Russell Platts
The Honorable Chris Cannon
The Honorable John J. Duncan
The Honorable Michael R. Turner
The Honorable Darrell E. Issa
The Honorable Kenny Marchant
The Honorable Lynn A. Westmoreland
The Honorable Patrick T. McHenry
The Honorable Virginia Foxx
The Honorable Brian P. Bilbray
The Honorable Bill Sali

Distributed Computing Industry Association
2838 Cox Neck Road
Suite 200
Chester, MD 21619
410-476-7965
www.dcia.info