Preliminary Transcript

STENOGRAPHIC MINUTES
Unrevised and Unedited
Not for Quotation or
Duplication

HEARING ON INADVERTENT FILE SHARING

OVER PEER-TO-PEER NETWORKS

Tuesday, July 24, 2007

House of Representatives,

Committee on Oversight and

Government Reform,

Washington, D.C.

"This is a preliminary transcript of a Committee Hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statements within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record."

Committee Hearings

of the

U.S. HOUSE OF REPRESENTATIVES

U.S. HOUSE OF REPRESENTATIVES

OFFICE OF THE CLERK
Office of Official Reporters

Court Reporting Services, Inc.

HGO205000

HEARING ON INADVERTENT FILE SHARING
OVER PEER-TO-PEER NETWORKS
Tuesday, July 24, 2007
House of Representatives,
Committee on Oversight and
Government Reform,
Washington, D.C.

The committee met, pursuant to call, at 10:00 a.m. in room 2154, Rayburn House Office Building, the Honorable 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, Staff Assistant; Will Ragland, Staff Assistant; 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 four 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, the 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.

[Prepared statement of Mr. Waxman follows:]

********** INSERT **********

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. You 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 four 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.

[Prepared statement of Mr. Davis of Virginia follows:]

********** INSERT **********

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 five 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.

[Prepared statement of Mr. Hodes follows:]

********** INSERT **********

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.

[Prepared statement of Mr. Cannon follows:]

********** INSERT **********

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

Mr. Cooper?

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

Chairman WAXMAN. Mr. Walsh?

Mr. WALSH. 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.

[Prepared statement of Mr. Issa follows:]

********** INSERT **********

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 United States 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 United States 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.

And 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 of 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 hand.

[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 five 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 one 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; 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 determined 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. I'd share those, too. 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 United States 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.

[Prepared statement of Mr. Sydnor follows:]

********** INSERT **********

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 websites. 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 websites, 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 three years, we have periodically reviewed the risk disclosures provided on major P2P software websites and found that these disclosures have steadily improved. We also reviewed P2P websites to determine if they were a source of spyware.

In the fall of 2005 we downloaded the ten 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 ten programs, two 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 website MP3DownloadCity.com for making allegedly deceptive claims that it was 100 percent legal for consumers to use the file-sharing programs 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 website 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 website over 1.3 million times.

In addition, the FTC's general Internet education website, 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.

[Prepared statement of Ms. Engle follows:]

********** INSERT **********

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 tele-work, 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 tele-work 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.

[Prepared statement of Mr. Mintz follows:]

********** INSERT **********

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 Sysco Systems, we founded the Thought Leadership Roundtable on Digital Strategies to bring CIOs together to talk about 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, 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 U.S. into two U.S. area codes in The Bronx and Tacoma. This illustrates the threat both within and outside the U.S.

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 two-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 database, 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 associate 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.

[Prepared statement of Mr. Johnson follows:]

********** INSERT **********

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 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. 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 website 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 United States 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.

[Prepared statement of Mr. Gorton follows:]

********** INSERT **********

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 Iversa, 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 new tele-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 license, 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 nine 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 four 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.

[Prepared statement of Mr. Boback follows:]

********** INSERT **********

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 in-sums 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.

[Prepared statement of General Clark follows:]

********** INSERT **********

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, members' 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 material 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 United States 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 got to sign the documents, you have got to swear them 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 got 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 got 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 United States 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 they were 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 got 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 apparently 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, Tennessee, 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 to day?

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. Okay. 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.--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 of 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. Okay.

Mr. WELCH. I am going to ask you to answer the question I asked--

Mr. GORTON. Yes, we have a filter.

Mr. WELCH.--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 websites, 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. YARMUTH. 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 database, 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 a peoples 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 go that 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 follow-up 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.--has not shown up anywhere else?

Mr. MINTZ. No.

Mr. CLAY. Okay. This example also illustrates the potential conflict between encouraging and promoting tele-work and the flexible workplace and data security that was exposed. Mr. Mintz, how do you balance the tension between tele-work 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 tele-work, 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 tele-work requirements?

Mr. MINTZ. Yes. The tele-work 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 tele-work 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 represent 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.]

****
CONTENTS
****

****

INDEX OF INSERTS

****

********** INSERT **********

PAGE 52