AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

INADVERTENT FILE SHARING OVER PEER-TO-PEER NETWORKS: HOW IT ENDANGERS CITIZENS AND JEOPARDIZES NATIONAL SECURITY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JULY 29, 2009

Serial No. 111–25

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

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

U.S. GOVERNMENT PRINTING OFFICE

54–009 PDF WASHINGTON : 2009

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

CONTENTS

	Page
Hearing held on July 29, 2009	1
Statement of:	
Boback, Robert, chief executive officer, Tiversa, Inc.; Mark Gorton, chairman, the Lime Group; and Tom Sydnor, senior fellow and director, Center for the Study of Digital Property, the Progress and Freedom Foundation	10
Boback, Robert	10
Gorton, Mark	26
Sydnor, Tom	50
Letters, statements, etc., submitted for the record by:	
Boback, Robert, chief executive officer, Tiversa, Inc., prepared statement of	17
Connolly, Hon. Gerald E., a Representative in Congress from the State of Virginia, prepared statement of	91
Gorton, Mark, chairman, the Lime Group, prepared statement of	29
Issa, Hon. Darrell E., a Representative in Congress from the State of California:	
July 28, 2009, screenshots in HTML format	72
Prepared statement of	8
Sydnor, Tom, senior fellow and director, Center for the Study of Digital Property, the Progress and Freedom Foundation, prepared statement of	53
Towns, Chairman Edolphus, a Representative in Congress from the State of New York, prepared statement of	3

INADVERTENT FILE SHARING OVER PEER-TO-PEER NETWORKS: HOW IT ENDANGERS CITIZENS AND JEOPARDIZES NATIONAL SECURITY

WEDNESDAY, JULY 29, 2009

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

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

Present: Representatives Towns, Issa, Maloney, Cummings, Kucinich, Tierney, Watson, Connolly, Norton, Cuellar, Hodes, Welch, Foster, Duncan, and Bilbray.

Staff present: John Arlington, chief counsel, investigations; Linda Good, deputy chief clerk; Neema Guliani, investigative counsel; Adam Hodge, deputy press secretary; Carla Hultberg, chief clerk; Marc Johnson and Ophelia Rivas, assistant clerks; Phyllis Love and Alex Wolf, professional staff members; Mike McCarthy, deputy staff director; Jesse McCollum, senior advisor; Amy Miller, special assistant; Steven Rangel, senior counsel; Julie Rones, counsel, full committee, health; Ron Stroman, staff director; Lawrence Brady, minority staff director; John Cuaderes, minority deputy staff director; Jennifer Safavian, minority chief counsel for oversight and investigations; Frederick Hill, minority director of communications; Dan Blankenburg, minority director of outreach and senior advisor; Adam Fromm, minority chief clerk and Member liaison; Kurt Bardella, minority press secretary; Stephen Castor, minority senior counsel; and Mark Marin and John Ohly, minority professional staff members.

Chairman TOWNS. The committee will come to order. Good morning and thank you all for being here.

Imagine for a moment that you had special software on your computer that exposed many of the files on your hard drive to searches by other people. Any time your computer is connected to the Internet, other computer users with similar software can simply search your hard drive and copy unprotected files. Unfortunately, that is the sad reality for many unsuspecting computer users.

Peer-to-peer file sharing software like LimeWire works in just that way. Most people who use peer-to-peer software do it to download music and movies over the Internet. Most people who use

it are totally unaware that they may expose some of the most private files on their computers to being downloaded by others.

Nine years ago this committee first held a hearing that revealed that Government, commercial, and private information was being stolen by peer-to-peer file sharing networks without knowledge of the users. In response to congressional pressure, the file sharing software industry agreed to regulate itself, implementing a code of conduct to address inadvertent file sharing. The efforts failed.

Two years ago at our July 24, 2007 hearing, LimeWire's CEO Mark Gorton expressed surprise that sensitive personal information was available through LimeWire. He pledged to address the problem. That effort failed.

Over the last year alone, there have been several reports of major security and privacy breaches involving LimeWire. Information about avionics for the President's Marine One helicopter and financial information belonging to Supreme Court Justice Stephen Breyer were leaked on LimeWire. LimeWire does not deny those reports but claims that recent changes to the software prevent inadvertent file sharing.

To investigate LimeWire's assertion, the committee staff downloaded and explored LimeWire's software. The staff found copyrighted music and movies, Federal tax returns, Government files, medical records, and many other sensitive documents on the LimeWire network. Security experts from Tiversa found major problems. Specific examples of recent LimeWire leaks ranged from appalling to shocking.

The Social Security numbers and family information for every Master Sergeant in the Army have been found on LimeWire. The medical records of some 24,000 patients of a Texas hospital were inadvertently released. Most of the files are still available on LimeWire. FBI files, including civilian photographs of an alleged mafia hit man, were leaked while he was on trial and before he was convicted. We were astonished to discover that a security breach involving the Secret Service resulted in the leak of a file on LimeWire containing a safe house location for the First Family.

As far as I am concerned, the days of self regulation should be over for the file sharing industry. In the last administration, the Federal Trade Commission took a see-no-evil, hear-no-evil approach to file sharing software industry. I hope the new administration is revisiting that approach. I hope to work with them on how to better protect the privacy of consumers.

Today I look forward to hearing from our witnesses on the impact of peer-to-peer file sharing, and particularly how LimeWire proposes to help remedy the problems caused by its software.

I now yield 5 minutes to the ranking member, Congressman Darrell Issa of California.

[The prepared statement of Chairman Edolphus Towns follows:]

HOUSE COMMITTEE ON
OVERSIGHT & GOVERNMENT REFORM

CHAIRMAN EDOLPHUS TOWNS

OPENING STATEMENT

HEARING

"Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security."

July 29, 2009

Good morning and thank you for being here.

Imagine for a moment that you had special software on your computer that exposed many of the files on your hard drive to searches by other people. At any time your computer is connected to the Internet, other computer users with similar software could simply search your hard drive and copy unprotected files. Unfortunately, that is the sad reality for many unsuspecting computer users.

Peer-to-peer (P2P) file sharing software like LimeWire works in just that way. Most people who use P2P software do it to download music and movies over the Internet. And most people who use it are totally unaware that they may expose some of the most private files on their computers to being downloaded by others.

Nine years ago, this Committee first held a hearing that revealed that government, commercial, and private information was being stolen over P2P file sharing networks, unbeknownst to the users. In response to Congressional

pressure, the file sharing software industry agreed to regulate itself, implementing a Code of Conduct to address inadvertent file sharing.

That effort failed.

Two years ago, at our July 24, 2007, hearing, LimeWire's CEO Mark Gorton expressed surprise that sensitive personal information was available through LimeWire. He pledged to address this problem.

That effort failed, too.

Over the last year alone, there have been several reports of major security and privacy breaches involving LimeWire. Information about electronics for the President's "Marine One" helicopter and financial information belonging to Supreme Court Justice Stephen Breyer were leaked onto LimeWire.

LimeWire does not deny those reports, but claims that recent changes to the software prevent inadvertent file sharing.

To investigate LimeWire's assertions, the Committee staff downloaded and explored LimeWire software. The staff found copyrighted music and movies, Federal tax returns, government files, medical records, and many other sensitive documents on the LimeWire network.

Security experts from Tiversa found major problems. Specific examples of recent LimeWire leaks range from appalling to shocking:

- The Social Security numbers and family information for every master sergeant in the Army had been found on LimeWire.

- The medical records of some 24,000 patients of a Texas hospital were inadvertently released and most of the files are still available on LimeWire.

- FBI files, including surveillance photos of an alleged Mafia hit man, were leaked while he was on trial and before he was convicted.

We were astonished to discover that a security breach involving the Secret Service resulted in the leak of a file on LimeWire containing a safe house location for the First Family.

As far as I am concerned, the days of self-regulation should be over for the file-sharing industry. In the last Administration, the Federal Trade Commission took a see-no-evil, hear-no-evil approach to the file sharing software industry. I hope the new Administration is revisiting that approach and I hope to work with them on how to better protect the privacy of consumers.

Today, I look forward to hearing from our witnesses on the impacts of P2P file-sharing, and in particular, how LimeWire proposes to help remedy the problems caused by its software.

Mr. ISSA. Thank you, Mr. Chairman. I think, as both of us are saying in various ways, today is clearly déjà vu all over again.

Two years ago in July 2007, this committee brought to light in a vivid but altogether too easy to demonstrate demonstration that, by design or at least with knowledge and allowance, unwitting sharing of personal information over this peer-to-peer network was not just going on but was well known and going on in a rampant way. I remember all too well the details of the documents, including Social Security numbers, of a soldier and his colleagues with the 101st Airborne. Those Social Security numbers were there for everyone along with name, rank, date and place of birth, and anything and everything one would need to capture his identity and those of his colleagues.

It is very clear that little has changed. In preparation for this hearing we noted that there was a brand new version, a version that at least went part of the way toward protecting the inadvertent loss of documents. But I say part of the way because, as you can imagine, in the world of the Internet we assume that you are protected unless you give up those protections. That is not true of this software.

This software required essentially that for copyrighted works you opt into protecting the software rather than having to knowingly make copyrighted software available. You don't simply check and never again have to worry about your copy or someone else's copyrighted software being available to everyone.

The committee's jurisdiction and the committee's primary interest today are contained on this disk and could be contained on thousands like it. These are zip files of names, addresses, Social Security numbers, and income tax returns from California once again showing that today, loading the current software—I should more accurately say yesterday—my staff, never having worked it before and with a brand new computer, downloaded the latest software and went sight seeing to find exactly what you might find. An engineer who only made about $37,000 took a standard deduction. In fact, his information, all of it, is available.

Mr. Chairman, identity theft should be at the heart of our concern. I am personally on the Judiciary Committee and am concerned about the copyrighted software, about the hundreds of thousands and hundreds of millions of dollars that are being stolen through peer-to-peer transaction. But I think that when we look at the most important thing for the American people is to close once and for all in no uncertain terms the loophole that allows people's individual and sensitive information, company information, and employee information to be inadvertently and thoroughly disbursed in a way that leads without a doubt to PayPal registration, to MasterCard registration, and to the ruining of credit and lives.

Mr. Chairman, there is no question that we have come not far enough in 2 years. I know that this hearing will shed more light on it. But I will tell you that this disk, Mr. Chairman, to me represents a referral to the AG and a referral to California's Attorney General if we cannot be satisfied in no uncertain terms that we have reached the end of this kind of activity. Otherwise, as we say too often on this committee but appropriately here, if you condone, allow, and induce this to happen, you are guilty of cooperation and

participation in every criminal act that flows from the discovery of that information.

Mr. Chairman, I ask unanimous consent to have the rest of my opening statement placed in the record. I yield back the balance of my time.

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

EDOLPHUS TOWNS, NEW YORK
CHAIRMAN

DARRELL E. ISSA, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

Majority (202) 225-5051
Minority (202) 225-5074

Statement of Rep. Darrell Issa, Ranking Republican Member
Committee on Oversight and Government Reform
"Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security"
July 27, 2009

Thank you, Chairman Towns, for holding this hearing.

I must admit to a feeling of déjà vu. Almost exactly two years ago, this Committee held a hearing nearly identical to today's. The hearing took place in this room. Its title was also "Inadvertent File Sharing Over Peer-to-Peer Networks." Our three witnesses were among those who testified that day. And the issues we addressed in July 2007 – the unwitting sharing of personal information over peer-to-peer networks that can wreak havoc on American's lives and endanger national security – are the same as those we will hear about today.

There may be only one difference: as the use of these file sharing programs has grown – one recent report says that 200 million computers worldwide have at least one file sharing program installed – so too have the problems related to inadvertent file sharing.

According to one of the witnesses here today, P2P network searches for financial, accounting, and medical records have risen nearly 60% since September 2008. During a live demonstration on *The Today Show* earlier this year, a search of P2P networks turned up 250,000 individual tax returns in minutes. Last July, it was reported in the *Washington Post* that Supreme Court Justice Stephen Breyer and 2,000 other individuals had their social security numbers and dates of birth released to the world due to an investment company employee using the LimeWire file sharing program.

In preparation for this hearing, I asked one of my staff to conduct an experiment. This staffer had never used a P2P file sharing program. He took a laptop computer, brought it home, and downloaded the latest version of LimeWire. After installing and running the program, he typed in a search for "tax return." In less than a minute, he found and downloaded to the laptop's hard drive a .pdf copy of the 2007 tax return for an

individual from Houston, Texas. My staff now knows the following about this man: his full name; his street address and apartment number; his social security number; the fact that he is single without children; the fact that he is an engineer, made about $37,000 in 2007, and took the standard deduction on his tax return. Again, all of this took less than a minute to locate and download.

There are legitimate and beneficial uses of file sharing. As the size of files increases and the demand for bandwidth expands, P2P file sharing programs can help move huge amounts of data cheaply and efficiently among any number of users. There are also legitimate arguments to be made for personal and institutional responsibility – individuals, companies, and governments with sensitive data on their hard drives and networks should do all that is possible to ensure the security of that information by developing protocols that will not allow the use of P2P programs on those computers or otherwise ensure their safe use.

But the problems associated with P2P file sharing programs continue to plague us. In addition to the financial chaos that can ensue for anyone whose social security number, date of birth, or other personally identifying information is released over the networks, there are legitimate concerns about national security There have been multiple reports of anti-terrorist security plans for a number of cities and transportation systems being accidentally, and unknowingly, shared over P2P networks, plans which could be used by terrorists in any country in the world to better coordinate the very attacks those plans were drafted to combat. Committee staff has heard from one of our witnesses today about a spreadsheet widely available on a P2P network that includes the names, social security numbers, home addresses, and names and ages of the children of military Special Forces units.

Mr. Chairman, we heard from Mark Gorton, LimeWire's Chairman, at our 2007 hearing. At that time, Mr. Gorton expressed surprise at the widespread availability of personally identifying information and other sensitive data available on P2P networks, and that so many users were actively searching for it. I asked Mr. Gorton, as a result of becoming more aware of the issue, if he was committed to making significant changes in the software to help prevent the problem in the future. Mr. Gorton replied, "Absolutely."

LimeWire is by no means the only P2P software program; there are hundreds. However, LimeWire remains the largest and most used, with more than 183 million downloads of its various versions according to one report. I am very interested to hear today from Mr. Gorton and our other witnesses about the current state of inadvertent file sharing on P2P networks and LimeWire's attempts to fulfill its promise to this Committee to improve its software's safe use.

Thank you again, Mr. Chairman. I look forward to hearing today's testimony.

Chairman TOWNS. Without objection, so ordered.

It is the longstanding policy that we swear in all of our witnesses. Will you please stand and raise your right hands?

[Witnesses sworn.]

Chairman TOWNS. You may be seated. Let the record reflect that the witnesses answered in the affirmative.

Mr. Robert Boback is the Chief Executive Officer of Tiversa, Inc. Mr. Boback will conduct a demonstration of the dangerous uses and activities of LimeWire that Tiversa has uncovered through monitoring technology and work with the Federal Bureau of Investigation.

Let me welcome you, Mr. Boback. We are now prepared to hear your testimony.

STATEMENTS OF ROBERT BOBACK, CHIEF EXECUTIVE OFFICER, TIVERSA, INC.; MARK GORTON, CHAIRMAN, THE LIME GROUP; AND TOM SYDNOR, SENIOR FELLOW AND DIRECTOR, CENTER FOR THE STUDY OF DIGITAL PROPERTY, THE PROGRESS AND FREEDOM FOUNDATION

STATEMENT OF ROBERT BOBACK

Mr. BOBACK. Thank you, Chairman Towns, Ranking Member Issa, and distinguished members of this committee for the opportunity to testify here today. As the chairman mentioned, my name is Robert Boback and I am the CEO of Tiversa.

What we are about to show you is information that is current. This is all within the last few months, disclosures that have not been publicly released, so this information you most likely haven't seen prior.

As Ranking Member Issa points out, identity theft is going to be at the core of this. You will see that, despite the regulations around identity theft, the FTC has not addressed this fully. In fact, peer-to-peer is not even mentioned on the identity theft Web site of the FTC for the 9 million victims. You will find that this is where identity theft is occurring. This is the harvest ground.

This is why your consumers will say they do not know where or how identity theft happened. We are going to show you a demonstration of just that fact. It affects every district. There are millions and million of individuals that are affected.

If we could start through the demonstration, we are going to highlight this in a number of issues. The first one, of course, is the national security implication, of which there are many. What we are starting here, these are just excerpts from some of the files. They have been redacted. These are all military troops, hundreds of thousands of troops' Social Security numbers, different rosters, different information from around the world with their next of kin, their children's names, their Social Security numbers, and their dates of birth, as Ranking Member Issa pointed out. Again, it goes on and on and on. These are all current. They are still all available, by the way, on the peer-to-peer.

If we could go on to the next one, as pointed out in the opening statement of the chairman, this is the safe house route for the U.S. Secret Service when they have to evacuate the First Lady in this case. This is found on the peer-to-peer. This is the location. I don't

know how much the U.S. Government spends in preparing a safe house location but I presume it is pretty expensive. All of that is lost based on this information being disclosed.

Now the safe house has to be moved. The locations have to be moved. We of course redacted all of this in order to protect what is left of the security of this. Some of the other information is the motorcade route.

The next one, Sam? As you can see, this was a breach just as of yesterday. We found this yesterday but you can see the date, July 5, 2009. This is the entirety of the U.S. nuclear information, all of our facilities, everything. This is from the United States. This is from the President with the President's information listed on here, every nuclear facility and all the secure, highly confidential information. As you can read on the top, it says "highly confidential, safeguard sensitive." This is every nuclear agency, every facility.

The problem is that we found this in France, in four locations in France, not in the United States. Other countries know how to access this information and they are accessing this information. This was, you can see the date.

If we push on to the next slide, this was the cover letter on it, right from the President of the United States with Barack Obama's signature at the end, with his writing at the end. This is not even subject to a FOIA request. You couldn't get this information on a Freedom of Information Act. You can, however, access it on the peer-to-peer in free open text. It just doesn't make sense.

Switching over to another issue, again, identity theft, medical identity theft is hugely on the rise. People understand that they are looking for credit card information. I get that. But I don't look at my explanation of benefits from my insurance provider like I look at my credit card statement. I will tell you that you should because the identity thieves will. A medical insurance card is like a Visa card with a million dollar spending limit. They will buy online drugs, OxyContin, Viagra, and by the time you go to the doctor next time, all of a sudden the doctor has you listed as an OxyContin addict when you have never taken it in your life. This is the problem.

This information has come out of a hospital, as you mentioned, in a southern State. Individuals will say, "I don't even use peer-to-peer; I have never downloaded a thing so I am safe, right?" Well, have you ever been to the emergency room? You just might not be safe. That is exactly what happened to these 20-some-thousand individuals. All they did was go to the doctor. They provided their information—as they should—to their facility for the insurance billing. At the billing company someone was listening to music while they were typing in their data entries and what ended up happening is that 24,000 victims are affected.

In this specific case we informed the company. This actually was the only one that occurred over a year ago. It occurred over a year ago and through our client, which was a large insurance carrier, we told the hospital that this was disclosed. Unfortunately, they said it is not their problem. It is not their problem. They don't want to go out publicly and say that they disclosed 24,000 individuals.

That there is a House bill, H.R. 2221. H.R. 2221 provides for a national breach notification. It is long overdue. Forty-one of the 50 States have breach notification laws and they vary in their severity. This hospital is a clear case. The State of Texas does have a breach notification law and this hospital is in direct violation of it. They have known about this for over a year. They haven't even told these victims that they are victims, so these people have been the victims of identity theft.

The hospital was clearly negligent for handling this information in the way that they have but this is what you see. This is the pattern. No one wants to say, gosh, I had a data breach and it is my responsibility to address it. So there needs to be legislation in order to force companies to do the right thing. You would hope that they would do it without the pressing.

Back up one, Sam, please. This is a Midwest-based HIV clinic with people's most sensitive information. These are AIDS victims, 184 patients, who are now victims of identity theft. The clinic released their information and has not addressed it. This information is still out there.

This is everything you need as an identity thief. Why would you ever dive in a dumpster, which the FTC calls out as the No. 1 reason where people get it? I can get 184 just from this one file and thousands from the other files.

As we continue on, we have a major pharmaceutical company, information on all of their research. It has everyone and where they are going.

It affects even the most robust security measures, which is what we are seeing. All of these companies have firewalls, anti-virus, intrusion detection, intrusion prevention, and encryption. Yet where is the security? There isn't any. They don't address it because the awareness isn't there. They say they don't allow downloading of peer-to-peer or that is a recording industry problem. No. In fact, it is their problem. Companies need to do this. Just as when anti-virus started out, it was unheard of at the beginning and then it evolved. That is how security and technology evolves.

This information is out. If you have ever gone to a doctor, your complete patient records, everything, your soap notes, if you will, are all out there as well. Continuing on, there is behavioral health information, again, all with Social Security numbers. Everything we are showing you is a Social Security number in here.

Continue on. This is one. If you have ever gone to the drug store and were buying Sudafed, you are required to give your driver's license information because they keep track of that for methamphetamine labs. The problem, though, remains that you now gave your driver's license information to buy Sudafed because you had a cold and now you could be the victim of identity theft around the Nation because that information may or may not have been secured. If it is not secured, as this one wasn't, you are now exposed. You are exposed forever. They may not even tell you when they find out. There is a serious issue.

Then, moving on from there, here is an interesting example for corporations nationwide. This is an enormous organization that all of you have heard of. Unfortunately, we can't give the name in an open environment because this is a publicly traded company that

is very well known in the Fortune 500. This individual is an M&A executive, the mergers and acquisitions executive that handles all of the M&A activity for the organization.

In doing that, they were using peer-to-peer and exposed a file called a PST file. A PST file is your archive of your emails. It is you. Imagine someone being able to open up your Outlook and read every email that you sent, open every attachment, and also open your calendar to see what conference calls you have, the dialing numbers, and the pass codes. That, in fact, is what happened in this case.

I am sure that the SEC would have an interest in looking at companies that do this and have this information. Not only are the emails on there but they also have the attachments of every acquisition that this company is going to make and the ranges of which they are willing to pay for these. As the next slide will show, it also has the financial information all the way listed through the third quarter, as you can see, third quarter 2009.

Now, if you were an investor, there is market manipulation that could happen from here because you know the internal financials of what the company is going to do for the next 3 months or 6 months. I know what the stock is going to do because I see your financials. This information has to be protected. Again, they use state-of-the-art protection and spend millions of dollars on their security, yet this is still a problem.

Going forward, there are other financial institutions with thousands, 5,000 entries of client information, of exposures on mortgage information. Here on the next file there are 12,000 credit card numbers. Again, this is identity theft.

Continuing on, as the chairman mentioned, these are photos, and we have redacted the photos to protect this, the organized crime case that we were talking about. These are their surveillance photos of an organized crime. This is a murder trial. These photos were disclosed while the trial was in process. There was no conviction before this. Who disclosed them, we still haven't investigated yet. But this was just found. Literally, the individual in the photos here is actually behind bars now on a life sentence. But this was disclosed while he was on trial.

On the right hand side, Sam, could you jump up one? Obviously, in an organized crime case you don't want to disclose the Government witness list for obvious reasons. As you can see on the right hand side, we blurred it out so that you can't see the names, that is the entire confidential Government witness list in an organized crime case. Many of these people are in the Witness Protection Program. There is their information. This is not what you want to have out there.

The next slide as we continue on, as Ranking Member Issa mentioned, there are tax returns from all over Brooklyn, Arizona, Massachusetts, Maryland, and Vermont. We could have gone on through all 50 States and had thousands of them from any 1 of these 50 States. This is where identity theft is happening. It is not out there; this is where it is happening. If you have been the victim of identity theft and you didn't lose your purse or wallet, think peer-to-peer because that is where it happened.

As we go on, Sam, we are going to show a video. We are not on that one yet. We are going to do the tax return video. I want to show you using LimeWire. Tiversa has technology that allows us to see the entire network. We are going to use LimeWire. We did a LimeWire video here just to show you how easy it is for individuals to gain access to tax return information.

Using LimeWire Pro here, we typed in "tax return." There are five connections that you are connected to. We use this because people say you have fancy technology and that is the only reason you can gain access to this. No, it is not. He typed in "tax return." There are only five connections so it is not even widely connected. As you can see, it is small on the screen, there are just hundreds of tax returns coming in. This is not using our technology. So, as you can see, it is this simple. This is in real time so you could click on any of those tax returns. That function used was a "browse host" function. Again, this software is still out there.

Download the tax return and literally within minutes, as you are going to see here, it is downloading a couple of tax returns. We are going to show you just how easy this is as this loads in. Here they are coming in at the bottom there. As we click on those, you are going to see that this individual used H&R Block. It is not a problem with H&R Block. That is just who they used. They saved a copy of it.

That person used TurboTax. As you can see, there is their Social Security number. There are their children's Social Security numbers. It is that simple. Why would you ever dumpster dive? It is right there. That is not our technology; that is theirs. It is that information.

Sam, switching to information concentrator, we will show you that individuals do this. We call them information concentrators or identity thieves. This individual right here is an individual in Arizona. If you could see all the files that they have, this individual does exactly what I just showed you. He is collecting tax return files to sell them on the black market. We are working with the FBI to address this right now.

This is an investigation here. This individual has 1,800 files, if you can see with how small that is. He is just scrolling through all of those tax returns. All of those victims are identity theft victims. They are all going to be victims of identity theft if they haven't been already.

Many have already been victims of identity theft. But my Social Security number has been my Social Security number for 38 years and it will continue to be. So if someone has mine maybe they will wait a year or 2 years. Then they will do a thing like file my tax return for me. Yes, that is right. That is the new identity theft. I will file your tax return for you in January.

In January, I will steal your return because no amount of monitoring, nothing is going to stop me. I will take the return. The U.S. Government, the Treasury pays that money. In working with the IRS, they told us that is $20 billion a year in cost to the U.S. Treasury, $20 billion a year of individuals filing someone else's tax return and stealing the refund. This is what is going down and this is how it is happening. This is how they gain access to the information.

Again, just to close it all up, I am showing the Eagle Vision, our software. I am going to show you our software running here. It actually hits even closer to home as a parent of three daughters. These are, we can't even show this all because of the nature of it. This is our software running live right now. Every one of those little blips along the bottom there, those red little blips on the screen, every one of those is an individual that is either a child predator or child pornographer.

That is happening live right now, taking information, child pornography. That is only child pornography. Here is a 4-year old, a 5-year old. You can see the searches as they go by. These are individual searches happening right now. This is live right this second. All of those little red blips, every one of those was a child pornographer. This is felony possession, 5 years. You can't even possess it but they are not afraid on peer-to-peer because they know security can't catch them. So this is what is happening.

Behind that, Sam, flip to the screen. This individual, we had to black it but this is a famous NASCAR driver. He is very well known. That is why I didn't want to show his face. That is an innocent picture of him with his son. There is nothing wrong with this. We found this picture in an investigation with the FBI in the hands of a child pornographer.

Here is what they do. They take your picture which you may have on your computer and they will take it off of your computer. They will put that innocent little boy, the son of the NASCAR driver, in amongst the pictures of indecent pictures. What it will do is it will make law enforcement think that it is that person. They will only show midsections of the indecent pictures but once they show a face, obviously law enforcement is going to deduce that is the face of the victim. And in an effort to try to find the victim, it actually turns you the wrong direction.

Imagine if this NASCAR driver were a potential victim in a sexually explicit case. It could ruin his career and he didn't do anything wrong. His daughter downloaded a peer-to-peer client, had it on her system, and she had a picture of her dad and her brother. That is nothing bad, but this is what happens.

In closing, I would like to say that clearly there is a problem. There are a number of recommendations. Obviously a number of Government agencies are disclosing information across the board. Why are they not monitoring for this information? This would be like a bank shutting off the security cameras and saying the vault is safe enough so I don't need to worry about watching it. It doesn't make sense. All Government agencies should monitor for this information. You can't disclose this. We can't be the victim.

These military individuals were disclosed by the military. You can't have that. We saw the press that it got when the body armor wasn't approved. Imagine these troops fighting. They are trying to stay off of an IED. They don't want to check their credit. They are not doing that. They are coming home and they are being victims of identity theft. We can't have that happen.

There is legislation with H.R. 2221 that should be out there to give the FTC power to do this. As of now, they don't have the extensive power that they need. The DSS, the Defense Security Service, should look for the defense contractors that are disclosing infor-

mation. The SEC should look and the FTC should also be engaged in changing their Web site to do that.

I apologize. I know I was over time. Sir, I will yield back.

[The prepared statement of Mr. Boback follows:]

Testimony before the House Committee on Oversight and Government Reform

Robert Boback, CEO, Tiversa, Inc.

July 29, 2009

TIVERSA

Good morning Chairman Towns, Ranking Member Issa and Distinguished Members of the Committee.

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

P2P file-sharing continues to be a major security risk and privacy issue. Today, I will provide a brief background on P2P networks, highlight the risks of inadvertent file sharing, provide examples of P2P file disclosures and the impact on consumers, businesses, government, the military and national security, and share our observations and recommendations.

Background: Peer-to-Peer Networks

The Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

P2P networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The P2P networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

P2P networks are growing and dynamic. Since 2005, P2P networks have grown at the rate of over 20% (CAGR). Today, worldwide P2P networks may have over 20 million users at any point in time. P2P networks are ever-changing as users join and exit constantly. The number of P2P programs or "clients" has grown to over 225, with many having multiple versions in use. Additionally, many of the programs are open source and, accordingly, subject to modification as users see fit. P2P networks are a worldwide phenomenon with users across wide ranges of ages, educational backgrounds and incomes.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

1 – Planned file sharing – its intended use.
2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

Inadvertent File Disclosure

P2P networks continue to grow in size and popularity due to the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this unintentional sharing that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may want to share only their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads P2P software program on his/her parents' computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

"Intentional software developer deception" occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software programs that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

"Malicious code dissemination" occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code ("worms") in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user's computer who may have never intended to install a P2P file sharing program. This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim's computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs typically do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, foreign intelligence organizations and terrorists worldwide.

Despite the tools that P2P network developers are incorporating into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today's existing safeguards, such as data loss prevention, firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

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

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

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the "Inadvertent Sharing via P2P Networks," during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

Today, we will provide the Committee with concrete examples that show the extent of the security problems that exist on the P2P networks and the implications of sharing this type of information. During our testimony, we will provide the Committee with examples that illustrate the types of sensitive information available on P2P networks, provide examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers and government agencies in previous hearings, the problem remains. In fact, we will also demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Tiversa and its Technology

Beginning in 2003, Tiversa developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been designed, developed and implemented in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, more than the number of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Tiversa uses this technology to provide P2P security and intelligence services to businesses, consumers and law enforcement agencies. The following examples demonstrate how inadvertent breaches affect individual consumers, businesses, government, military and national security and are based on our unique perspective on P2P networks.

Examples: Inadvertent Disclosures on P2P

Consumers

Financial Fraud – From analysis of P2P searches, listed below is a small sampling of actual searches issued on P2P networks during a brief research window in March 2009. The term *credit card* was used as the filter criteria for the period.

- *2007 credit card numbers*
- *2008 batch of credit cards*
- *2008 credit card numbers*
- *a&l credit card*
- *aa credit card application*
- *abbey credit cards*
- *abbey national credit card*
- *ad credit card authorization*
- *april credit card information*
- *athens mba credit card payment*
- *atw 4m credit card application*
- *austins credit card info*
- *auth card credit*
- *authorization credit card*
- *authorization for credit card*
- *authorize net credit card*
- *bank and credit card informati*
- *bank credit card*
- *bank credit card information*
- *bank credits cards passwords*
- *bank numbers on credit cards*
- *bank of america credit cards*
- *bank of scotland credit card*
- *bank staffs credit cards only*
- *barnabys credit card personal*
- *bibby chase credit card*

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January of this year for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases in which accountants and tax offices, themselves, inadvertently disclosed client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately $35 each. This is up from approximately $8-$10 only a few short years ago. One plausible explanation for the rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSNs. This is a very important point. Our search data shows that thieves in fact employ a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her legitimate tax return, it will automatically be rejected by the IRS as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims leaving the initial victim to address the problem with the IRS. This is very costly and time consuming for both the victim and the IRS.

Stolen SSNs are also used by illegal aliens to gain employment in the United States. This crime has far reaching implications as well as placing a tremendous tax burden on the victim.

Medical Fraud – Medical information is also being targeted on P2P networks with alarming and increasing regularity. Listed below are some terms issued over the same period regarding medical information.

- *letter for medical bills*
- *letter for medical bills dr*
- *letter for medical bills etmc*
- *letter re medical bills 10th*
- *ltr client medical report*
- *ltr hjh rosimah medical*
- *ltr medical body4life*
- *ltr medical maternity portland*
- *ltr medical misc portland*
- *ltr orange medical head center*
- *ltr to valley medical*
- *lytec medical billing*
- *medical investigation*
- *medical journals password medical .txt*
- *medical abuce records*
- *medical abuse*
- *medical abuse records*
- *medical algoritms*
- *medical authorization*
- *medical authorization form*
- *medical authorization*
- *medical benefits*
- *medical benefits plan chart*
- *medical biliing*
- *medical biling*
- *medical bill*
- *medical biller resume*
- *medical billig software*
- *medical billing*
- *medical billing windows*

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, the thief would immediately have access to significant financial resources (in many cases medical insurance policies have limits set at $1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which can be quickly sold for cash. This is a very difficult crime to detect as many consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company, prolonging the criminal activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for valid medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

User-issued P2P searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. For the years of 2006 and 2007, the average annual rise in the search totaled just over 10%.

Child Predation – As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can be even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos

and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program and have been seeking to work more extensively with other law enforcement and prosecutorial organizations.

Tiversa has used its ability to locate available files and track individual's P2P network searches to document cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Sources of the Breach – Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

In research involving over 30,000 consumers, Tiversa found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the 60 day research period (2/25-4/26/09), Tiversa downloaded 3,908,060 files that had been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. It is important to note that these files were only downloaded with general industry terms and client filters running. Many more exist on the network in a given period of time.

Corporations and businesses

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of specific search strings in this testimony would put these corporations at further risk. General search terms include company names in combination with "confidential," "executive," "payroll" and other terms clearly designed to identify files containing important or personal information. The Committee should note that the searches of this nature are every bit as aggressive and more specific than those for credit cards and medical information – the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Corporate information disclosed on P2P networks includes breached PII and personal health information (the basis for much of the personal information used in identity theft described above), intellectual property, strategic documents and business plans. We have identified disclosures of legal documents, performance reviews, Board minutes, merger and acquisition plans, plant physical security plans, network diagrams, user ID's and passwords. Specific examples of inadvertent disclosures are described below.

One Supplier affects Thousands – In one instance, we identified one small company with fewer than 12 employees that provides third party billing services to hospitals. An inadvertent disclosure on patients from three different hospitals by this company exposed personal health information (patient names, SSNs, diagnosis codes, physician names, and other information) involving:

- 20,245 Patients
- 266 Physicians
- 4,029 Employer Organizations
- 335 Insurance Providers

It is easy to see the criminal value of the information exposed in this single breach and the potential impact to a broad range of individuals, professionals and organizations.

Corporate secrets revealed – In another instance, Tiversa discovered the PST file of a high-ranking officer involved in the merger and acquisition area of a Fortune 100 company. The entire Microsoft Outlook information of this officer was exposed to the public:

- Entire calendar
- Schedule of conference calls with dial-in numbers and passcodes
- Business and personal contacts including names, e-mails, addresses, phone numbers, etc.
- Over 12,000 e-mails to and from the individual
- Over 400 e-mail attachments (documents, PowerPoints, spreadsheets, etc.) including:
  - Regional sales information
  - M&A business integration updates
  - Strategic business alliances
  - Revenues through acquisitions

In the wrong hands, this information could be used for individual profit from trading on "insider information" not formally reported by the company, or on a much larger scale to manipulate and undermine the credibility of the capital markets.

Government, the Military and National Security

This risk also extends to the military and to overall national security.

Troop PII exposed – Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of more than 200,000 of our troops.

Classified information searched for...and found – P2P networks also pose a national security risk. In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Searches are directed at identifying and obtaining sensitive information on matters of security using terms such as:

- Classified
- Military classified
- Military confidential
- Top secret
- US Marines classified
- Restricted

Examples of information breaches emanating from P2P networks and known to the public are described below.

In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the *Wall Street Journal* printed a front cover story reporting that former Pentagon officials had indicated that spies had downloaded plans for the $300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

Recommendations

For several years, Tiversa's focus has been working with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

FTC – On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

SEC – Awareness should extend to corporations and government agencies as well. Corporations regularly breach personal information of individuals (employees, customers, etc.). With consumers increasingly being asked to provide PII to employers, banks, accountants, doctors, hospitals, and government agencies, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Corporations also disclose non-public information that could be used for individual profit or to manipulate or undermine the markets. P2P risks and vulnerabilities that lead to these disclosures should be addressed in the application of current laws (Sarbanes-Oxley, Gramm-Leach-Bliley, etc.).

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary from state to state and, in our experience, are seldom respected or followed by organizations. In some cases, companies that seek to do the right thing are unfamiliar with the various laws that may apply to their situation or have difficulty in complying with the applicable laws.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. In this regard, we believe that P2P risks and vulnerabilities should be addressed in the application of current laws, and we support HR 2221 – the Data Accountability and Trust Act. This proposed legislation requires the establishment and implementation of policies and procedures for information security practices and includes notification and remediation provisions in instances of breach.

The breach laws will also need to be enforced. Many disclosing companies disregard the current state laws, if any, to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel & National Security Disclosures

DOD – The safety and identity of our men and women in uniform of Congress should be vigorously protected. Measures should be taken to safeguard personal information, and to monitor, detect and remediate any disclosures. For soldiers who have had their information disclosed, comprehensive identity theft protection services should be provided to prevent and guard against the use of the breached information.

DSS – P2P networks should be continuously monitored globally for the presence of any classified or confidential information disclosed by defense contractors or subcontractors that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it) – Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask! Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service – Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

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

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

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

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

Thank you for the opportunity to testify today.

TIVERSA.

144 Emeryville Drive
Suite 300
Cranberry Township
Pennsylvania 16066

(724) 940-9030 *office*
(724) 940-9033 *fax*
www.tiversa.com

Chairman TOWNS. Thank you very much, Mr. Boback.

Mr. Gorton is the chairman of Lime Group and founder of the world's most popular peer-to-peer software called LimeWire. Mr. Gorton, I will give you 10 minutes to respond.

STATEMENT OF MARK GORTON

Mr. GORTON. Thank you, Chairman Towns and Ranking Member Issa. My name is Mark Gorton and I am the founder and chairman of LimeWire, LLC.

I am happy to be able to report that since the July 24, 2003 hearing on inadvertent file sharing, LimeWire has made great progress in addressing inadvertent file sharing. With the most recent versions of the LimeWire application, the problem of inadvertent file sharing for current LimeWire users has been eliminated. The LimeWire team has put a huge amount of effort into resolving this problem. We have redesigned and re-engineered the entire user interface for the application. This has been a large task and our efforts have proved worthwhile.

The current version of LimeWire does not share any documents by default. In order for a LimeWire user to change their default settings to enable document sharing, they have to click nine times and disregard three warnings. Even then, if a user shares a folder, LimeWire will not share the documents in that folder.

In LimeWire 5 there are no shared folders, meaning that if a user elects to share a folder, they are only electing to share the contents of that folder at that particular time. Nothing will be shared that a user adds to that folder at a later point in time. All LimeWire versions 5 and above automatically unshare documents that a user may have shared using an earlier version of LimeWire 4.

I am confident that with the recent versions of LimeWire all sharing is intentional sharing. From the vast improvements that LimeWire has made on the front of inadvertent file sharing, I hope that the members of this committee can see that LimeWire is sincere and dedicated to working with this committee. In addition to this committee, LimeWire has successfully worked with the FBI, the New York State Attorney General's Office, and the FTC on a range of issues surrounding P2P file sharing.

Unfortunately, the popular perception of LimeWire regarding inadvertent file sharing fails to match LimeWire's excellent record in addressing these problems. A good part of this misperception is due to the highly inaccurate and misleading report produced by Tom Sydnor of the Progress and Freedom Foundation. Mr. Sydnor's report is deceptive and filled with factual errors and misleading statements. The number of issues with Mr. Sydnor's report is too large for me to cover in my summary statement so, for the benefit of this committee, I have submitted a detailed critique of Mr. Sydnor's report in my written statement.

It is probably worth me going a little bit into the technical details of how file sharing networks work so that people can understand the relationship of LimeWire to the file sharing networks in the world. LimeWire the application speaks a protocol called Gnutella. There are many common Internet protocols. There are the email protocols, the World Wide Web protocols, and FTP proto-

cols. Using these open protocols, many applications that speak these protocols are capable of communicating with each other. So by using LimeWire, you are capable of communicating with dozens of applications that speak compatible protocols.

When you do a search with LimeWire, you are not just talking to other LimeWire programs in the world. You are talking to dozens of other different types of programs, most of which are produced outside of the United States. So it is important to keep in mind that even though you might actually be using LimeWire, the results that you get with LimeWire don't necessarily come from another LimeWire client. It is somewhat analogous to the World Wide Web. You have Internet Explorer, you have Safari, and you have Firefox. Using each of those applications you can access a Web site, but the Web site that is being seen may not have anything to do with those particular applications.

It is certainly true that in the past LimeWire has had issues with inadvertent file sharing. We have worked very hard to address those issues. I would like to point out that while using the recent versions of LimeWire it would have been very difficult for any individual to share any of the documents that Mr. Boback has shown us recently.

I do understand that inadvertent file sharing is a problem in this world. LimeWire is committed to helping address it. But LimeWire is one company in a field where there are hundreds of P2P applications in this world. We are doing our best to set a standard that we hope other file sharing companies can follow. But most of these creators of file sharing applications are not based in the United States. They may not even be corporations. So I think it is important for the committee to understand when they are considering regulations in this regard the somewhat complicated nature of peer-to-peer networks in the world.

In addition to inadvertent file sharing, there are a couple of other issues that I would like to at least cover in my opening statement and potentially in the question period. I would like to point out that LimeWire has been working to build a collaborative relationship with the recording industry. LimeWire has built a store for digital media at store.limewire.com which currently has over 3.5 million MP3s available for purchase. In addition, LimeWire is actively building an advertising solution to allow participating content holders to profit from advertising related to their media.

Many of the very most senior people in the music industry support working constructively with LimeWire but building an industry-wide consensus on a policy change regarding P2P has been a slow and grueling process. After many meetings with record industry executives, I am convinced that the industry recognizes the benefits of embracing P2P in order to stay relevant going forward.

I would also like to take this opportunity to discuss the current regulatory environment surrounding copyright and the Internet. The history of copyright regulation is one where new technologies have created issues for the old regulatory system. Then the new regulatory system was updated to take into account the abilities of these new technologies. The Internet has transformed media distribution and consumption, yet copyright regulation is yet to be updated to account for the new capabilities of digital technologies.

The current lack of practical copyright enforcement mechanisms has put the recording industry in the unfortunate position of being pitted against its customers and technology companies.

As a technologist, I have a good sense of the range of technical possibilities available to regulators as they consider updating regulations surrounding the Internet. The Internet is not un-policeable. With determined targeted regulation, almost any level of control of the Internet is possible. As Mr. Boback has shown, technology can play a role in this. The fact is, using and leveraging technology, law enforcement officials can with one person monitor millions and millions of computers. A lot of the behavior that is currently going on, with a little bit of technology, probably can be remedied fairly quickly. I think law enforcement has been a little bit behind the curve in using technology to police the Internet.

In addition to simply law enforcement, it is also worth keeping in mind on the judiciary side that currently the procedural overhead in dealing with crime that occurs on the Internet is very time consuming and difficult to address. I am sure Mr. Boback can testify to that in terms of what it takes to contact the FBI, to get files taken down, and things like that. It is possible to set up enforcement mechanisms that are nearly automated. If we were to have a proper enforcement regime out there, it would be possible to simply address many of these problems.

I think it is very important to keep in mind the need to address the problems at the root point of control. Every computer on the Internet is connected through an Internet service provider. That is a unique point of control for that single computer. That Internet service provider can cutoff access to the offending computer. I understand that when addressing these issues LimeWire is the superficial interface to all of these problems.

As you are well aware, LimeWire is now the most popular peer-to-peer file sharing application. It hasn't always been that way. There is a list of file sharing applications that have come before LimeWire. Certainly there were Napster, Kazaa, Morpheus, BearShare, and iMesh. There is quite a long list. Most of the regulatory efforts, or perhaps prosecutorial efforts, on the part of the recording industry have focused on file sharing applications.

But those file sharing applications are by no means a unique point of control. Consumers have the ability to switch between them very, very simply. So I think when people are considering regulation, it is very important to consider the effects of that regulation.

Thank you.

[The prepared statement of Mr. Gorton follows:]

STATEMENT BY

Mark Gorton
Chairman, The Lime Group

BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

ON

Inadvertent File Sharing Over Peer-To-Peer Networks: How it Endangers Citizens and Jeopardizes National Security

FIRST SESSION, 111TH CONGRESS
JULY 29, 2009

Not For Publication
Until Released By The
Committee On Oversight And Government Reform
United States House Of Representatives

Dear Chairman Towns, Ranking Member Issa and Member of the Committee:

I would like to thank you for inviting me to speak before the Committee today. My name is Mark Gorton, and I am the founder and Chairman of Lime Wire LLC.

I am happy to report that immediately after the Committee brought the issue of inadvertent file sharing to my attention at the July 24, 2007 hearing on the matter, Lime Wire began the process that culminated in all but eliminating inadvertent file-sharing with the LimeWire application.

Specifically, within weeks of the July 2007 hearing, the Lime Wire team began working with the Distributed Computing Industry Association ("DCIA") to establish an Inadvertent Sharing Protection Working Group (the "ISPG") of leading P2P and other technology companies to address issues associated with inadvertent sharing of personal and sensitive data. Lime Wire, the DCIA and the ISPG have since worked directly with staff at the Federal Trade Commission in an iterative process to formulate and implement the *Voluntary Best Practices For P2P File-Sharing Software Developers to Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data* (the "VBPs"), announced in July 2008. In summary, the VBPs outline seven principle best practices in the areas of: 1) default settings, 2) file-sharing controls, 3) shared-folder configurations, 4) user-error protections, 5) sensitive-file-type restrictions, 6) file-sharing status communications, and 7) developer principles. In so doing, LimeWire, the DCIA, the ISPG and the FTC created a set of best practices that may serve as a guide for not only Lime Wire, but all file-sharing software developers, in addressing the issue.

Within six months after the issuance of the voluntary best practices, Lime Wire, in December 2008, released LimeWire 5, culminating a concerted effort to combat and eliminate inadvertent file sharing in accordance with compliance with these principles. The LimeWire team has put tremendous effort into resolving the issue, completely redesigning and reengineering the entire user interface for the LimeWire application. This has been an enormous task, and our efforts have proved worthwhile. Thanks in part to ongoing feedback from the FTC and DCIA, Lime Wire has since released LimeWire version 5.2.8 taking the inadvertent sharing prevention built into LimeWire 5 and making it stronger and even simpler for the user to control. To mention some of the highlights since the July 2007 hearing -

- LimeWire 5 does not share any Documents by default.[1] In order for a LimeWire user to change their default settings to enable Document sharing, they have to click nine times and disregard three warnings.

- A LimeWire 5.2.8 user *cannot* share or even place into the LimeWire Library their "My Documents" folder, "Documents and Settings" folder, "Desktop" folder, or "C" drive no matter what. And this setting *cannot* be changed.

- If a user shares the contents of a folder, LimeWire 5.2.8 will not share the Documents in that folder even if the default settings have been changed to allow Document sharing.

[1] LimeWire considers 150 file extensions to be Documents that are not shared by default. See pp. 10, infra.

- In LimeWire 5 there are no "shared" folders, meaning that if a user elects to share a folder they are only electing to share the contents of that folder at that *particular* time, nothing will be shared that a user adds to that folder at a later point in time. All LimeWire versions 5 and above automatically *un-share* Documents that a user may have shared using an earlier version of LimeWire 4.

With these changes, I am confident that with LimeWire 5.2.8 any sharing is intentional sharing. For the convenience of the Committee, please find a detailed list of the changes made to the LimeWire application attached to this testimony at **Appendix A**. Lime Wire is proud to have taken a leadership role in the reduction of inadvertent file sharing and, if the Committee desires, Lime Wire is happy to be of assistance with any efforts to ensure that other makers and distributors of P2P software follow suit.

From the vast improvements that Lime Wire has made on the front of inadvertent file sharing, I hope that the members of this Committee can see that Lime Wire is sincere and dedicated to working with this Committee and in addressing serious issues that is brought to our attention. In addition to this Committee, Lime Wire has formed successful working relationships with the Federal Bureau of Investigation, the New York State Attorney General's office, and the FTC on a range of issues surrounding P2P file sharing.

Unfortunately, the popular perception of LimeWire regarding inadvertent file sharing fails to match Lime Wire's excellent record in addressing this problem. A good part of this misperception is due to the distribution of inaccurate and misleading information concerning LimeWire. One recent example is the July 2009 report of Thomas Sydnor of *The Progress & Freedom Foundation* entitled *"Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5."* The numbers of factual discrepancies in Mr. Syndor's report are too many for me to cover in my opening statement but I have attached a thorough illustration to this written testimony as **Appendix B**. As well, since the PFF report, a new version of LimeWire has been released - version 5.2.8, which takes the inadvertent sharing prevention built into LimeWire 5 and improves upon it making it even simpler for the user to control sharing.

In short, contrary to what Mr. Sydnor states, LimeWire 5 does *not* share user-originated files by default. In fact, by default, LimeWire 5 shares no files of any sort for the new LimeWire user.[2] Also contrary to what Mr. Sydnor states, LimeWire 5 does not share "sensitive file types" by default. In fact, by default LimeWire does not permit sharing of Microsoft Word documents, Corel documents, many proprietary tax document extensions, Excel spreadsheets, power point presentations and .pdf file. .Pdfs are file types that are most often associated with scanned personal documents as .pdf is the default file format for most consumer grade scanners. For example, Apple used .pdf as the native metafile format for Mac OS X.

Regarding Mr. Sydnor's comment that "LimeWire 5 will share Documents and Settings and its subfolders", LimeWire 5.2.8 does not permit the sharing of a user's "Documents and Settings" folder, nor a user's "My Documents" folder, "Desktop" folder, or "C" drive. This is true no matter where those folders are located. In fact, LimeWire 5.2.8 does not even permit placing these folders or drives into the

[2] For details regarding the sharing of previously shared files for a previous LimeWire user, see p.12, fn. 5 infra.

LimeWire Library. Further, no matter what folder or file a user attempts to share, if it is a folder that contains Documents or is a Document file, LimeWire 5.2.8 by default will *not* share the Documents in that folder or that Document file. Should the Committee take Mr. Sydnor's report into consideration in this investigation, I implore it to make its own assessment as to its accuracy.

Although Lime Wire has all but solved the problem of inadvertent file sharing for users of the LimeWire application, the global issue of inadvertent file sharing has not been resolved. While the LimeWire software allows its users to access the Gnutella network, LimeWire is not alone in providing access to the this network, much like Google, Yahoo, and Microsoft are not alone in providing access to the internet. To hold LimeWire solely accountable for what is available on the Gnutella network would be akin to holding Google solely accountable for what is available on the internet – both LimeWire and Google provide search and access capabilities to their respective superhighway, but they do not control that superhighway. There are hundreds of P2P applications in the world that are based on the same protocol as LimeWire (i.e., the Gnutella protocol), that allow user access to this same network, and consequently, that contribute to the issue of inadvertent file-sharing on Gnutella. Though a file may be found with the LimeWire application, it simply cannot be determined what P2P application was used to place that file into the Gnutella network. As many of these applications are produced outside of the United States, a US regulatory approach that focuses on software developers will always face an uphill battle with other, non-U.S. P2P developers.

I would also like to take this opportunity to discuss the current legislative and regulatory environment regarding copyright and the Internet. The gap between copyright law and the actions of hundreds of millions of Americans is enormous, and the lack of viable copyright enforcement mechanisms has pitted the recording industry against its customers and technology companies. For its part, Lime Wire has been working to build a relationship of collaboration between P2P and the recording industry. Lime Wire has invested millions of dollars creating the LimeWire Store to help rights holders monetize users at the point of acquisition: located at store.limewire.com, the LimeWire Store currently sells licensed, DRM-free MP3s. Recent distribution deals bring the total number of sound recordings to over 3.5 million, from hundreds of thousands of artists. In addition, Lime Wire is actively building an advertizing solution to allow participating content holders to profit from advertising related to their media.

Many of the very most senior people in the music industry support working constructively with Lime Wire, but building an industry wide consensus on a policy change regarding P2P is a slow, grueling process. After many, many meetings with record industry executives, I am convinced that the industry recognizes the benefits of embracing P2P in order to stay relevant going forward.

The history of copyright regulation is one where new technologies have created issues for the old regulatory system, and then the regulatory system was updated to take into account the abilities of the new technologies. The Internet has transformed media distribution and consumption, yet copyright regulation has yet to be updated to account for the new capabilities of digital technologies.

As a technologist, I have a good sense of the range of technical possibilities available to regulators as they consider updating regulations surrounding the Internet. The Internet is not unpolicable. With determined, targeted regulation, almost any level of control of the Internet is possible.

For anyone interested in learning more about this topic, I highly recommend the recent Harvard Business School paper authored by Felix Oberholzer-Gee and Koleman Strumpf titled "File Sharing and Copyright". More than any publication I have yet seen, this paper does a good job at analyzing the costs and benefits of file sharing to both makers and consumers of creative works.

A new regulatory balance needs to be found, one that allows our country to benefit from the technical innovations of the digital age while at the same time allowing artists to profit from their work. This system needs to provide incentives to the creators of content while limiting rent seeking behavior that exploits the protections given artists at the expense of the general public. If the correct balance is to be found, Congress must be sure to keep the interests of the American public in mind and not just the corporate interests who pay to have their viewpoint well represented.

This legislative reform will be hard work, but if any members of Congress are interested in crafting this legislation, I would be very happy to spent the time to work to find realistic, well balanced solutions to the disconnect between current law and public practice.

Mr. Chairman, Ranking Member Issa, Members of the Committee, thank you for bringing to my attention and allowing me the opportunity to deal with the issue of inadvertent file-sharing and for the opportunity to appear before this Committee today.

APPENDIX A

Since my deposition testimony on July 24, 2007, Lime Wire has made the following changes to the LimeWire software and underlying code to address the Committee's concerns regarding inadvertent file-sharing:

A. In LimeWire 4.13.13, released July 24th, 2007, Lime Wire updated the "sensitive directory check" to include Windows Vista's "Documents and Settings" directory. The "sensitive directory check" is used to warn users when a sensitive directory may be shared.

B. In LimeWire 4.15.0, released November 29, 2007 (the first major release following my testimony):
   i. The first major change was designed to help the user understand what was being shared and to make more clear how to remove things he/she may not want shared. This change introduced a link, always visible on the search screen, that said, "View your ### shared files", where ### was the number of files that were shared. Clicking on it would open up a tab that displayed every single shared file. You could right-click on any file and choose to stop sharing that file.
      1. A link was introduced on the page displaying your shared files that said, "You are sharing ### files. You can configure which files LimeWire shares." Clicking on that link would open up LimeWire's sharing preferences, where the user would have greater control over which folders were shared.
   ii. The second major change was designed to give more control over what file types were shared. This change introduced a new step in LimeWire's set-up that let the user choose which extensions would be shared. Extensions were categorized into "Audio", "Video", "Documents", "Images", "Programs" and "Other". The user could uncheck any category, or any extension within a category, and LimeWire would stop sharing all files that were in that category.
      1. In order to provide even greater control over sensitive file types, certain sensitive file extensions (including but not limited to .doc and .pdf) were marked as "sensitive". An option was added to this page that said, "Do Not Share Sensitive File Types" and was checked by default. Unless the user unchecked this option, LimeWire refused to

allow any sensitive file type from being shared when a directory was shared.

iii. The third major change was designed to warn the user in the event an ordinate number of files where being shared by that user. If LimeWire detected that a large number of files were shared, or a large number of folders were recursively shared, LimeWire displayed a warning telling the user that many files were being shared and giving the user the ability the go to their options menu and change this. These warnings were displayed every time LimeWire started until the user actively chose to either correct the problem or hide the warning.

iv. The fourth major change was designed to reduce confusion over what is shared and what is saved. This was accomplished by splitting the Sharing & Saving directories. Previously, LimeWire would create one directory called "Saved" where downloads would be saved to. Users also frequently elected to "share" this folder. In order to reduce confusion, this was changed so that downloads would be saved to a folder called "Saved" and a separate folder called "Shared" would be shared by default. The "Saved" folder was no longer shared by default.

v. The fifth major change was designed to make sure that all default options were skewed to not sharing sensitive information. This was accomplished by reviewing all prompts where the user was asked whether or not they really wanted to share something. The review focused on defaulting to the negative for any folder or file that was deemed sensitive.

vi. Minor Changes: (1) A bug was fixed so that Windows Vista's "Documents" directory was properly considered a "sensitive directory". (2) A bug was fixed so that if a sensitive directory was shared through recursive sharing, the user was properly warned. (3) The "Cookies" folder was added to the list of folders that cannot be shared.

C. In LimeWire 4.17.6, released March 27th, 2008, Lime Wire made additional changes to make it more clear to users how LimeWire shares and what sorts of information is likely to be sensitive information.

i. When a user chose a new "Save" folder, LimeWire warned them if this folder could contain sensitive information and allowed the user to choose a new location to store downloaded files.

ii. In addition we improved the wording for sharing individual files, extensions that are shared, partial file-sharing & .torrent file-sharing, so that it would be clearer to the user what was being shared.

iii. We audited every possible way a file or folder could become shared and verified that proper warnings are displayed. A few issues were found where the user wasn't properly warned that some files could not be shared, so warnings were added. Prior to this, the folder would still not be shared, but the user was not informed why it was not shared.

D. In LimeWire 5.0, released to the public on December 9th, 2008, LimeWire fundamentally changed the way file-sharing works. Lime Wire started from the ground up and addressed the fundamental problems that led to inadvertent file-sharing.

i. Persistently Shared Folders were removed entirely. A user can drag a folder into LimeWire to share it, but the folder itself is no longer shared. Only the files that were in the folder at the time it was dragged are shared. If a new file gets added to the folder at a later point in time, that new file is **not** shared. Dragging a folder into LimeWire to share it is simply a shortcut for selecting many files and sharing them each individually.

ii. Because shared folders no longer exist, recursive sharing (i.e., automatic sharing of newly added files to a shared folder) also no longer exists. In order to drive this point home, recursive sharing doesn't even happen when a user drags a folder to be shared.

iii. Documents cannot be shared with the P2P network by default. In order to change this, a user must change his/her settings by going to *Tools -> Options -> Security* and clicking *Configure* under the heading "Unsafe Categories", and disregarding the following warning, "We strongly recommend you do not enable these settings". Should a user elect to continue beyond this point, he/she then has to affirmatively "check" a box stating "Allow me to share documents with the P2P Network" and then click "O.K." in disregard for the following warning: "Enabling these settings make you more prone to viruses and accidentally sharing private documents". Even if a user had shared documents in a version of LimeWire prior to LimeWire 5, these documents will be unshared upon the installation of LimeWire 5.

iv. Viruses are typically contained within program files. To address viruses, LimeWire 5.0 completely removed the ability to manage, share, or download any kind of program file. In order to change this setting, the user must go to the same "Unsafe Categories" option with the same warnings as described in 3,E,iii, above.

E. LimeWire 5.2.8 introduced even further protections against inadvertent file-sharing.

i. Language has been changed to address the pertinent actions of sharing in layman's terms. Instead of using "P2P Network", terms like "Public Shared" and "Shared with the world" are consistently used throughout the program. These terms were found, through user testing, to be the clearest expression of the underlying actions and related consequences of sharing files.
ii. For new LimeWire users, the LimeWire Library is no longer populated automatically. Nothing appears in the user's Library unless they put it there.
iii. Additional warnings to users were added if a user tries to share sensitive file types after they disable the default settings preventing them from sharing sensitive file types. Along with this, an "Unshare all" button was added to this warning which, when clicked, not only unshares all sensitive file-types, but also reverts back to the default settings preventing the sharing of sensitive file-types.
iv. Bugs related to inadvertent file-sharing were found and fixed.
v. Additional file extensions were added to the list of "sensitive file types". "Sensitive file-types" that are not shared or shareable by default now number 150.
vi. The list-centered organization of the library was introduced, allowing users to create groups of files for easier, more informed sharing functionality.

APPENDIX B

Re: *The Progress & Freedom Foundation*, "Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5" (Thomas D. Mr. Sydnor II, July 2009)(the "Report").

I would ask that the Committee take note at the outset that the Report inexplicably concerns itself only with LimeWire. Mr. Sydnor does not make it clear, but the LimeWire software application is only one of many software applications that use the Gnutella protocol to allow users to access the Gnutella network. Some of the more popular Gnutella bases peer-to-peer programs include Shareaza, Bearshare, Frostwire, and MP3Rocket. And there are many more, including a great number of counterfeit LimeWire applications and many foreign distributed applications. A P2P user can share documents with any one of these applications, not just LimeWire. For every file type that is found using the LimeWire application, it is impossible to determine whether it originally entered the Gnutella network using the LimeWire application or any of the other Gnutella speaking applications. The Lime Wire team has worked very hard to make the LimeWire application the safest and most secure P2P available. And it has succeeded. To dilute or obfuscate the effort and success of Lime Wire by misattributing to it all things P2P runs a very real risk of leaving unmanaged, rogue and irresponsible P2P companies to flower and create *true* insecurity where LimeWire has created true security.

As a threshold matter, it is important to note that the Report redefines (without making clear that it is in fact a *new* definition) "sensitive file types" to include all Images, Audio and Video. See e.g., the Report, pp. 15-16. It is this new definition of "sensitive file types" that Mr. Sydnor uses throughout the Report. However, this new definition is simply unworkable: it has no basis in the industry; it cannot reconcile itself with the near 1 *trillion* "image" files posted by the public to the internet to date[3]; and it is in contravention of the definition of "sensitive file types" that has been used by the industry and industry players to date. Specifically, the Distributed Computing Industry Association's ("DCIA") Inadvertent Sharing Protection Working Group's ("ISPG") *Voluntary Best Practices* ("VBP") defines "Sensitive Files Types" as: *"file types which are known to be associated with personal or sensitive data, for example, those with file extensions such as .doc or .xls in Windows Office, .pdf in Adobe, or the equivalent in other software programs."* As this is the definition accepted and used by the industry as a whole, this is the definition used by LimeWire in defining what file types will not be shared by default. Mr. Sydnor's confusing and confounding expansion of the definition of "sensitive file types" makes it appear that LimeWire shares "sensitive file-types" by default. To be clear, it does not. [4]

---

[3] TechCrunch, April 7, 2009 (http://www.techcrunch.com/2009/04/07/who-has-the-most-photos-of-them-all-hint-it-is-not-facebook/).

[4] In LimeWire 5.x up to 5.2, allowing Document sharing was accomplished by going to *Tools -> Options -> Security* and clicking *Configure* under the heading "Unsafe Categories", and disregarding the following warning, "We strongly recommend you do not enable these settings". Should a user elect to continue beyond this point, he/she then has to affirmatively "check" a box stating "Allow me to share documents with the P2P Network" and then click "O.K." in disregard for the following warning: "Enabling these settings make you more prone to viruses and accidentally sharing private documents". If a user was running a previous LimeWire 5.x version, AND affirmatively changed the settings as described above to allow document sharing, AND affirmatively elected to share a specific

Included among "sensitive file types" (referred to as "Documents" in the LimeWire application) that are not shared by default in LimeWire 5.x up to LimeWire version 5.2.8 are files with the following extensions: *html, htm, xhtml, mht, mhtml, xml, txt, ans, asc, diz, eml, pdf, ps, eps, epsf, dvi, rtf, wri, doc, mcw, wps, xls, wk1, dif, csv, ppt, tsv,hlp, chm, lit, tex, texi, latex, info, man, wp, wpd, wp5, wk3, wk4, shw, sdd, sdw, sdp, sdc, sxd, sxw, sxp, sxc, abw, kwd.*

Included among "sensitive file types" (referred to as Documents in the LimeWire application and this testimony) that are not shared by default in LimeWire 5.2.8 are files with the following extensions: *123, abw, accdb, accde, accdr, accdt, ans, asc, asp, bdr, chm, css, csv, dat, db, dif, diz, doc, docm, docx, dotm, dotx, dvi, eml, eps, epsf, fm, grv, gsa, gts, hlp, htm, html, idb, idx, iif, info, js, jsp, kfl, kwd, latex, lif, lit, log, man, mcw, mdb, mht, mhtml, mny, msg, obi, odp, ods, odt, ofx, one, onepkg, ost, pages, pdf, php, pot, potm, potx, pps, ppsm, ppsx, ppt, pptm, pptx, ps, pub, qba, qbb, qdb, qbi, qbm, qbw, qbx, qdf, qel, qfp, qpd, qph, qmd, qsd, rtf, scd, sdc, sdd, sdp, sdw, shw, sldx, sxc, sxd, sxp, sxw, t01, t02, t03, t04, t05, t06, t07, t08, t09, t98, t99, ta0, ta1, ta2, ta3, ta4, ta5, ta6, ta7, ta8, ta9, tax, tax2008, tex, texi, toc, tsv, tvl, txf, txt, wk1, wk3, wk4, wks, wp, wp5, wpd, wps, wri, xhtml, xlam, xls, xlsb, xlsm, xlsx, xltm, xltx, xml, xsf, xsn.*

As regards "sensitive *folder* types", LimeWire 5.2.8 does not and cannot share a user's "My Documents" folder, "Documents and Settings" folder, "Desktop" folder, or "C" drive. This means these folders cannot be shared even if the user tries to do so and that the settings preventing the sharing of these folders cannot be changed.

As the Committee can see, the list of "sensitive file types" and "sensitive folder types" that are not shareable by default has grown considerably. This list is dynamic and responsive, built to be able to maintain user safety on an ongoing, updatable basis. And to be clear, LimeWire does not share Documents by default.

The Report, Section (A)(1), p. 8 *"LimeWire 5 now has a new dangerously ambiguous "share all" feature on major user-interfaces."*

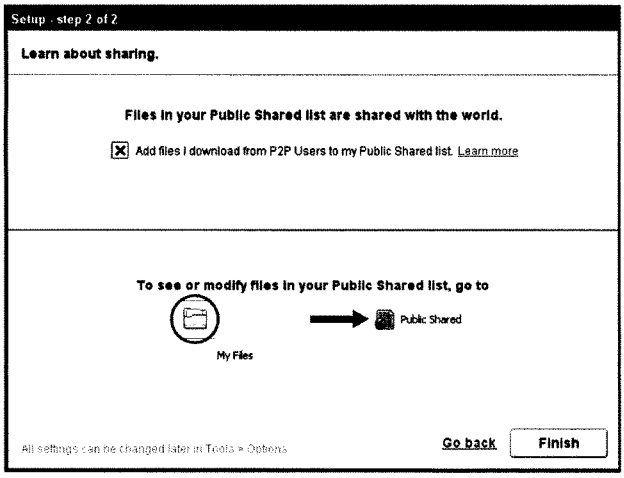
- ✓ In LimeWire 5.2.8 (production release date July 22, 2009), there is no "share" button, instead sharing is accomplished via clicking a file and placing into the "Public Shared list", or clicking a file and dragging it to the "Public Shared list" (for further details on how to share in LimeWire 5.2.8, see pp.12-13, infra.). Also, the phrase "P2P Network" no longer exists, having been replaced with "the world". Where a user's computer has never had LimeWire installed, the

---

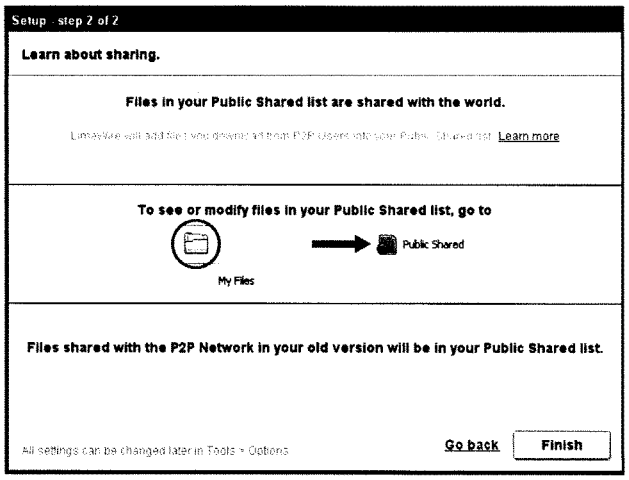
document (because merely changing the settings to allow document sharing does not automatically share any documents), upon upgrading to a more recent version of LimeWire 5.x, then those documents will be shared per the user's settings.

In LimeWire 5.2, allowing Document sharing is accomplished by going to *Tools -> Options -> My Files*, and clicking "Configure" under the heading "Sharing" and at the end of the notice that "LimeWire is preventing you from unsafe searching and sharing" at which time a window pops-up with the title "Unsafe File Sharing" along with the additional notice that "Enabling these settings makes you more prone to viruses and accidently sharing private documents. We strongly recommend you don't enable them." The user then affirmatively checks a box stating "Allow me to add Documents to my Public Shared list and share them with the world."

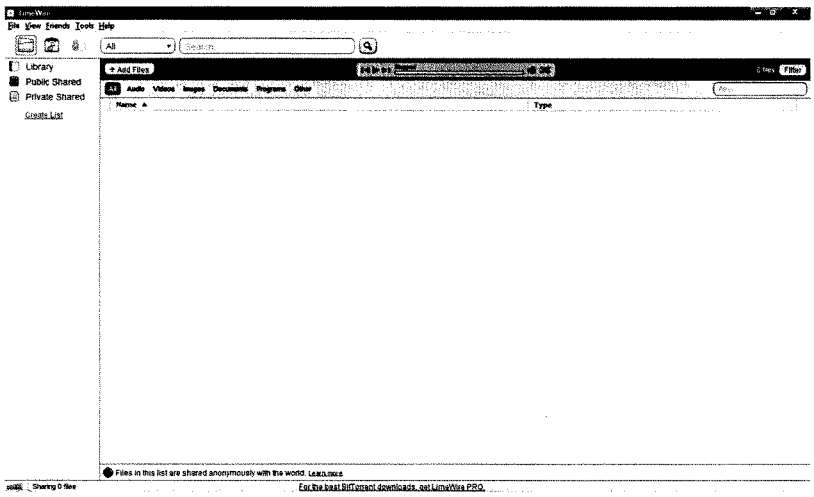
following screen appears during the initial run of 5.2.8. In clear, layperson language this screen both explains the concept that placing a file into the LimeWire "Public Shared list" makes that file available "to the world", and allows the user to set their default sharing for downloaded files:



✓ Where a user's computer previously had a prior version of LimeWire installed, the following screen appears during the initial run of 5.2.8. This screen also confirms previous sharing settings:



✓ Having explained the concept that "Files in your Public Shared list are shared with the world", the sharing interface is then presented to the user:



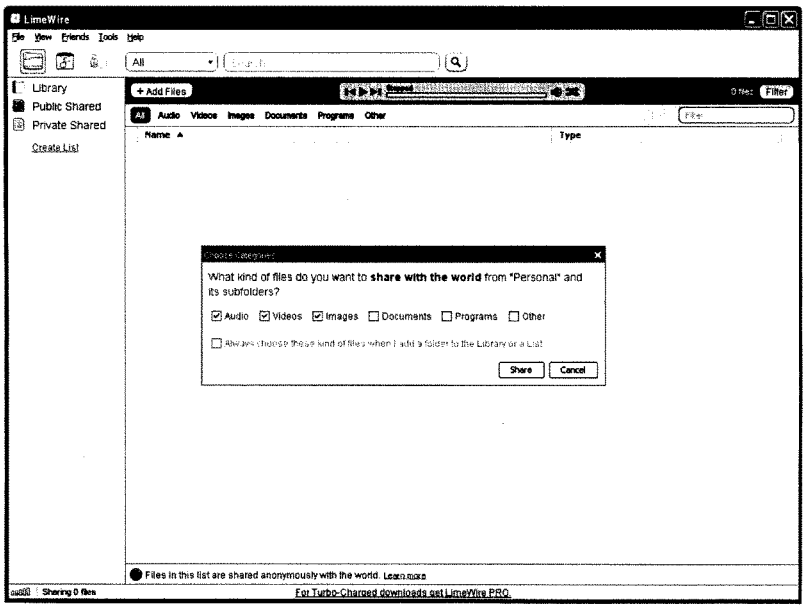
✓ Further, in LimeWire 5.x up to 5.2.8, there was never a one-click "share all" button that allowed sharing with the P2P network. Always the user had to highlight a category of file type, click "share" and then scroll and click "share all with the P2P Network". Mr. Sydnor's report did undercover a bug (see the Report, p.9, first paragraph). That bug has been fixed.

✓ Having informed the user that "Files in your Public Shared list are shared with the world" and shown the user where these settings can be altered, sharing is then accomplished via one of three methods:[5]

- ✓ The user highlighting "Library", right clicking the exact file in the "Library" the user wishes to share, and on the pull-down menu that follows, scrolling down to "Add to List", then click "Public Shared"; or
- ✓ The user highlighting "Library", clicking the exact file in the "Library" the user wishes to share, and dragging that file into "Public Shared" on the left side of the screen [6]; or

[5] In the event a user had a previous version of LimeWire on his/her computer, LimeWire 5.2 confirms his/her previously chosen sharing settings (see screen shot, bottom of page 11, supra.), and continues to share the files the user elected to share in the previous version. So, files may also be shared in this manner.

- ✓ The user dragging a file or folder from the user's computer into "Public Shared". **Note** here that dragging a folder into "Public Shared" results only in the informed and consented to sharing of the *contents* of that folder at the *particular* time it is dragged to "Public Shared". It is thus not the same concept as a "shared folder" because: 1) no file added to that folder at any later point in time will be shared with the P2P network by default; and 2) downloaded files will not by default be placed in any folder a user has dragged to "Public Shared". Further, in *no event, even if the user has changed their default settings* will dragging the contents of a folder into "Public Shared" result in the sharing of the Documents in that folder.
- ✓ In the event a user drags a folder into "Public Shared", the user is presented with a clear, easily understood information box asking which types of files in the folder the user wishes to share:



[6] In all instance where a user shares a file from the Library by choosing a particular file and right clicking, the user can also select all files in the Library via Control+A and either right click and chose "Add to List" and then select "Public Shared", or drag the entirety of the selected files into "Public Shared".

- ✓ Also and viewable in the immediately preceding screen shots, in the "Public Shared" screen, always appearing at the bottom is the notice: *"Files in this list are shared anonymously with the world. Learn More".*
    - ✓ Clicking "Learn More" links directly to a page stating: "*Files that are in your Public Shared list are shared anonymously with the world. This means that files in this list are available to be downloaded by all other users of LimeWire and other file sharing programs worldwide. All files in your Public Shared list are shared anonymously. This means other file sharing programs or P2P Users who may access your shared files do not recognize you by your name, address or email address, rather they recognize the IP Address of your computer. File sharing programs communicate to other file sharing programs using a computer's IP Address."*
- ✓ Even before 5.2.8, the "share" button in LimeWire versions 5.x up to 5.2.8 is not ambiguous and always required the user to click "share" and then select "share all with the P2P Network". Even assuming a user did do the above, Documents would not be shared unless a user changed his/her default settings, a very laborious process. See pp. 9-10, fn. 4; pp. 15-16.

The Report, Section (A)(2), p. 9 *"The effects of LimeWire 5's "Share all" feature depend upon an obscure file-sharing construct called "My Library."*

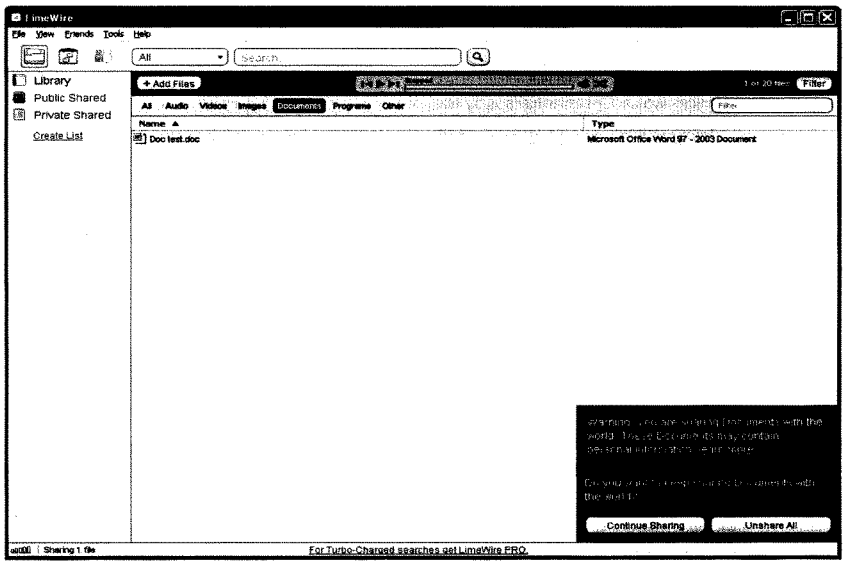
- ✓ In LimeWire 5.2.8, "My Library" no longer exists. There is still a "Library", but LimeWire 5.2.8 leaves the library empty by default. Further, if a LimeWire 5.x but pre-5.2.8 user was managing a folder in their "My Library", the LimeWire 5.2.8 "Library" will remove all files that were in the managed folder and which were not being shared. If a user has previously shared files with the P2P network with an earlier version of LimeWire, then LimeWire 5.2.8 will populate a user's "Library" and "Public Shared" list with those previously shared files. However, Document file types will not be shared, even if they were downloaded from the P2P network previously using an earlier version of LimeWire. However, if a user has gone through the process of changing their default settings in a LimeWire 5.x version (see pp. 9-10, fn. 4; pp. 15-16) to allow document sharing, and did share documents (again, only ever following an affirmative act) with the P2P network, documents downloaded from the P2P network with a prior version of LimeWire 5.x will be also be put into the "Public Shared" list.
- ✓ In any event, there is nothing obscure about the concept of "My Library". Many popular software programs employ a "library" feature, including iPhoto, and Picasa.

The Report, Section (A)(3), p. 12 *"Users can reasonably disregard LimeWire 5's "warnings" and enable document-sharing."*

- ✓ This comment is hard to understand – indeed, a user can disregard the warnings in LimeWire 5.x and enable document sharing. But note that even after enabling Document sharing, Documents *cannot* be shared by sharing a folder: LimeWire will ignore Documents that exist in a folder a user shared even if Document sharing is enabled. Moreover, Documents added to that folder

later by a user are not automatically placed into the LimeWire or shared. In fact, even with Document sharing enabled, LimeWire will not even put the Documents within a folder into the LimeWire Library. LimeWire simply will not see the Documents and will ignore them for all purposes. In all instances where a user shares a Document, they must do so by clicking on that particular Document. And that is after and in addition to the use changing the default settings to allow Document sharing by doing the following:

- a user must go to *Tools* then *Options*, then
- under the **warning** ***"LimeWire is preventing you from unsafe searching and sharing"*** click "Configure", then
- ignore a **second warning** that, ***"Enabling these settings makes you more prone to viruses and accidently sharing private documents. We strongly recommend you don't enable them",*** then
- Affirmatively checks a box stating ***"Allow me to add Documents to my Public Shared list and share them with the world",*** then
- go back to his/her Library and *affirmatively* select a *particular* Document and place that particular Document in a list called "Public Shared", then
- disregards a **third warning** that pops-up stating: **"Warning: You are sharing Documents with the World. These Documents may contain personal information. Do you want to keep sharing Documents with the world?"** (see screen shot on p. 16, supra), and then
- click "Continue Sharing".
- But, *even at this point*, if a user decides they do not want to share that particular Document, they are presented with the option to "Unshare All" at the click of one button. If the user chooses to "Unshare All", not only does LimeWire 5 unshares that Document, but reverts to the default settings that prohibited Document sharing in the first place:



- ✓ If a user wants to share a Document after having selected "Unshare All", they must repeat the whole process over again.

<u>The Report, Section (B)(1), p. 14</u> *"LimeWire 5 violates at least eight of the DCIA Best Practices (1) LimeWire 5 will share User-Originated files by default."*

- ✓ The implication created here is false. The Report states that LimeWire can share user-generated files "if *no* version of LimeWire *was* installed on a user's computer *when* LimeWire 5 was installed." (Report, p. 15). The implication the Report seems to want to create is that LimeWire 5 will share user-generated files if no version of LimeWire was *ever* installed on a user's computer. Such is not true: if no version of LimeWire was *ever* installed on a user's computer, in no instances will *any* files, User-Generated or otherwise, be shared by default.
- ✓ If, as the Report states, *"no version of LimeWire was installed on a user's computer when LimeWire 5 was installed" but* there was *previously* a version of LimeWire installed on the user's computer, *and* that user shared files with the P2P network, *then* LimeWire 5 will assume that the user intended to share those files and wishes to continue doing so. This was the case with the example provided in the Report, but the Report failed to mention the previous installation and prior affirmative sharing done by the user.
- ✓ Even still, where a user had a 4.x version of LimeWire and elected to share files (including Documents), a later installed version of LimeWire 5.x will not share previously shared Documents. If a user had a version of LimeWire 5.x on their computer and changed their default settings to share Documents (<u>see</u> pp. 9-10, fn. 4, and pp. 15-16, <u>supra</u>.) *and* shared Documents

(because merely changing the settings won't result in sharing without further affirmative action by the user), then a later installed 5.x version of LimeWire will continue to share those Documents. Again, the software assumes, with good reason, that sharing Documents in such circumstances was an intentional act by the user.

- ✓ Because LimeWire version 5.x will not by default share any files of any sort unless a user had a previous version of LimeWire on the same computer *and* chose to share files with the P2P network, one has to assume that Mr. Sydnor's screen shot showing "Sharing 1,244 files" is merely showing the 1,244 files Mr. Sydnor affirmatively undertook to share when using a previously installed version of LimeWire.

The Report, Section (B)(2), p. 15 *"LimeWire 5 will share thousands of User-Originated Files without any clear, timely, and conspicuous plain-language warnings."*

- ✓ This is false. All LimeWire 5.x versions require an affirmative act on the part of the user to share files. Versions 5.x up to 5.2.8 require a highlighting of a type of file category, then clicking "Share" then clicking "Share all with the P2P Network". For sharing in LimeWire 5.2.8, see p. 13, supra. In the event a user undertook those affirmative acts in an earlier version of 5.x, following reconfirmation of sharing settings, LimeWire 5.2.8 will continue to share previously shared files.

The Report, Section (B)(3), p. 15 *"LimeWire 5 shares "Sensitive File Types" by default."*

- ✓ This is false. By default, LimeWire 5.x will *not* allow the sharing of Documents. Period. (See pp. 9-10, fn. 4; pp. 15-16).
- ✓ Here, the Report creates confusion by redefining "sensitive file types" to include "Images, Audio and Video." (Report, pp. 15-16). In so doing, Mr. Sydnor is defining as "sensitive" nearly 1 *trillion* files that the computing public have made available on the internet.[7]
- ✓ Further, the industry has never defined "sensitive file types" include "Images, Audio and/or Video." See the DCIA ISPG *Voluntary Best Practices*, which defines "Sensitive Files Types" as: *"file types which are known to be associated with personal or sensitive data, for example, those with file extensions such as **.doc or .xls** in Windows Office, **.pdf** in Adobe, or **the equivalent** in **other** software programs."* This is the definition the industry uses and this is the definition LimeWire uses.
- ✓ In any event, LimeWire does *not* share image, audio or video files by default, rather it *permits* the sharing of such files be default: only after the affirmative act of the user will LimeWire 5.x by share files.
- ✓ No files are shared by default for a new LimeWire user.[8]

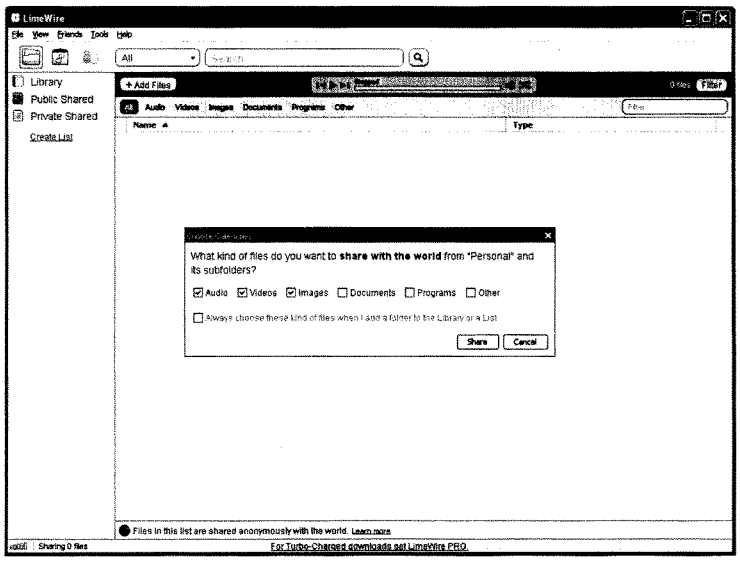
---

[7] TechCrunch, April 7, 2009 (http://www.techcrunch.com/2009/04/07/who-has-the-most-photos-of-them-all-hint-it-is-not-facebook/).

[8] To be clear, for a previous LimeWire user, those files (1) shared with the previous version will be re-shared by LimeWire 5.x, and (2) non user-generated files downloaded from the P2P network will be re-shared by default. However, where previous sharing was with LimeWire version 4.x and included Documents, LimeWire 5.x will *not* re-share those Documents. Rather, 5.x will *unshared* Documents that were shared using 4.x.

The Report, (B)(4), p. 17 *"LimeWire 5 enables recursive sharing by default."*

- ✓ This is misleading. Lime Wire 5.x does not share folders by default, there is no automatic sharing of folders, and indeed "folder" sharing as such is no longer a feature of LimeWire. Specifically, "folders" are not shared, rather the contents of a folder at a particular moment in time may be shared. This however is not a "shared folder" because 1) no file added to that folder at any later point in time will automatically be shared with the P2P network or even added to the LimeWire Library by default; and 2) downloaded files will not by default be placed in any such folder for re-sharing with the P2P network; 3) Documents in that folder will not be shared no matter if the user has enabled Document sharing or not.
- ✓ Further, in LimeWire 5.2.8, in no event will dragging the contents of a folder into "Public Shared" result in the sharing of the Documents in that folder.
- ✓ In addition, in LimeWire 5.2.8, an attempt to share all files in a folder triggers a screen asking specifically what file types from the folder the user wishes to share:



The Report, (B)(5), p. 18 *"LimeWire 5 does not uninstall completely."*

- ✓ This is also false. Uninstalling LimeWire by using the standard Add/Remove Program functionality completely removes the LimeWire software from a user's computer. Certain files that LimeWire used do remain on a user's computer. This is to ensure continuity of user intended functionality and is a common practice among software creators and/or distributors.

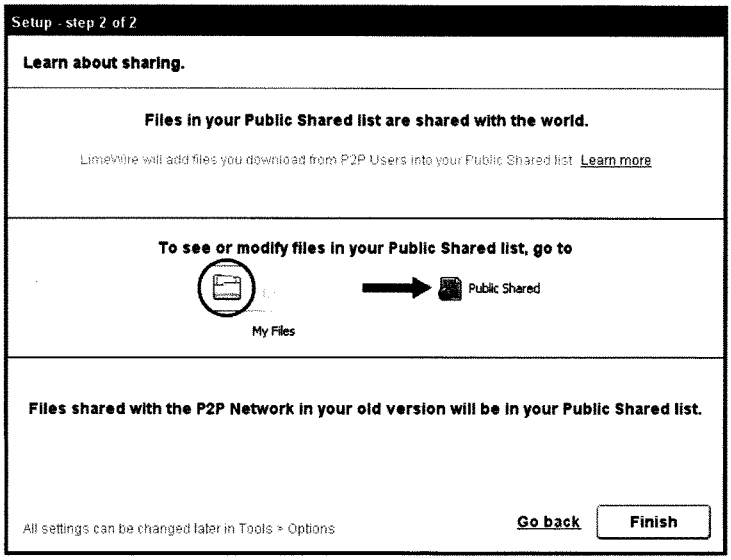
This is data only. Uninstalling LimeWire using Add/Remove Program results in the 100% removal of the software.

The Report, (B)(5), p. 19 *"For example, I set up a test computer that had 1752 audio, image, and document files stored in various subfolders of its My Documents folder. I then confirmed that no version of LimeWire was installed on that computer, and then completed a default installation of LimeWire 5.1.3.*

1752 files—including document files—were shared by default. Not only did a default installation of LimeWire 5 permit sharing of document files, it actually shared all of the document files in My Documents and its subfolders—with no input from, or warning to, the user, who certainly did not "affirmatively elect" to share document files, or any other files.

LimeWire's challenge backfired because neither LimeWire 5 nor prior versions of LimeWire uninstall completely. As Usability and Privacy explained seven years ago: "[U]sers often work in shared computer settings, so it is quite possible for one user to change all the settings and another to know nothing about it." ***Consequently, a user installing LimeWire 5 might not know that a different user had once uninstalled an earlier version of LimeWire 5 because it had been misconfigured. That was the scenario underlying the test-computer experiment just described."***

- ✓ Again, the stated analysis leaves out myriad significant details and multiple steps a user must take to replicate the stated result and in so doing misinforms as to how LimeWire 5 actually works . The only clue the Report gives as to these missing details are found in the two sentences placed last: "*Consequently, a user installing LimeWire 5 might not know that a different user had once uninstalled* ***an earlier version of LimeWire 5 because it had been misconfigured. That was the scenario underlying the test-computer experiment just described."***(emphasis added).
- ✓ Here is what Mr. Sydnor had to do for his test to yield the sharing of Documents:
  - Install LimeWire 5.x, go to *Tools>Options> Security* and click *Configure* under the heading "Unsafe Categories" >
  - disregard the following warning, "We strongly recommend you do not enable these settings", and affirmatively check a box stating "Allow me to share documents with the P2P Network" >
  - click "O.K." in disregard for the following warning, "Enabling these settings make you more prone to viruses and accidentally sharing private documents",
  - *and then* go back to his computer's hard drive >
  - drag the files to his LimeWire "P2P Network" list >
  - then use "Add/Remove Program" to uninstall LimeWire >
  - then reinstall a version of LimeWire 5.x.
  - At that time, the newly installed LimeWire 5.x will resume sharing per the settings selected in the earlier installed 5.x. The software reasonably assumes that after all the above steps have been taken by the user, the user intended to share. With a user's upgrade from a 5.x to LimeWire 5.2.8, that user's P2P sharing settings are reconfirmed



- ✓ LimeWire 5.2.8 nonetheless improves on the issue by not allowing sharing of the "My Documents" folder, "Documents and Settings" folder, "Desktop" folder, or "C" drive.

The Report, (B)(6), p.20 *"LimeWire 5 does not require users upgrading from prior versions to "reconfirm" their "previously chosen sharing selections."*

- ✓ LimeWire 5.2.8 reconfirms a user's sharing settings from a prior version and at the same time provides the user the information necessary to change those settings. See the immediately preceding screen shot.

The Report, (B)(7), p. 21 *"LimeWire 5 fails to warn users sharing more than 500 files."*

- ✓ LimeWire 5 shows the user every file that the user is sharing. The VBPs were created in response to inadvertent sharing. Where sharing happens only after affirmative action by the user and where the event of a sharing is accompanied by clear and positive feedback to the user, by for example, clearly displaying all of the files that are being "shared with the world" by file name, such a warning is no longer called for.

Thank you for the opportunity to provide these clarifications regarding the safety and security features of LimeWire 5.

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

Mr. Sydnor is senior fellow and director of the Center for the Study of Digital Property at the Progress and Freedom Foundation. He will testify about issues discussed in the recently published paper entitled, "Inadvertent File Sharing Re-Invented: The Dangerous Design of LimeWire 5."

Mr. Sydnor.

STATEMENT OF TOM SYDNOR

Mr. SYDNOR. Thank you, Chairman Towns, Ranking Member Issa, and honorable members of the committee. I thank all of you for holding this, the committee's third hearing on inadvertent file sharing.

I note in his written testimony that Mr. Gorton has said that 2 years ago after the last hearing "LimeWire began the process that culminated in all but eliminating inadvertent file sharing with the LimeWire application." Recent media reports from, for example, Today Investigates as well as Mr. Boback's testimony make clear that statement is simply not true. In my testimony today I hope to explain a little bit about why.

The essential question in this hearing is, as I think the ranking member phrased it, is this "déjà vu all over again." After the committee's 2003 hearing identified two features in file sharing programs that had been shown to cause what I would call catastrophic inadvertent file sharing, that is to share thousands of personal files that clearly no one would ever want to share over the Gnutella file sharing network, after that hearing highlighted the dangers of those features, LimeWire worked with its then trade association, P2P United, to develop a code of conduct that would have prohibited their use.

It looked as if the problem was solved. But what actually happened is that LimeWire went out and actually systematically disregarded that code of conduct, incorporating both of those features into its program. As a result, LimeWire found itself starring in many of the high profile incidents of catastrophic inadvertent file sharing.

Now in the aftermath of the committee's 2007 hearing, LimeWire found a new trade association, the Distributed Computing Industry Association, and worked with it to promulgate a new set of industry self-regulations which it allegedly implemented in the versions of its program called LimeWire 5. LimeWire provided compliance data that led its trade association to deem it the poster child for compliance with those voluntary best practices.

The question is, has LimeWire this time actually done what it claimed it would do? In my report, the Inadvertent File Sharing Re-Invented: Dangerous Design of LimeWire 5, the answer is clearly no. It has not. Nothing that has happened since the release of that report changes that conclusion. Essentially, my report identified three fundamental problems in the recent versions of LimeWire that we could call LimeWire 5.1.

First, these programs are dangerously unpredictable. The simple truth of the matter is this: Mr. Gorton says his program won't share document files by default. If you will look in my written testimony, you will find a screenshot taken this weekend on a test

computer that was set up to look exactly like my personal computer at home, my main home computer, which is to say that it had 16,798 document, image, video, and audio files stored in subfolders of its My Documents folder.

In this test computer there was no version of LimeWire presently installed. I completed a default installation just as Mr. Gorton described in his 2007 testimony by clicking next, next, next all the way through the process. The result was 16,798 files shared, including document files, shared by default simply by installing the program.

That is an entirely unacceptable result. That is LimeWire 5. The truth of the matter is that if any normal computer user installs this program on an ordinary home computer, they have no way to know what it will do to them by default. It is dangerously unpredictable. It is dangerously unpredictable because LimeWire has failed to correct the causes of that dangerous unpredictability that have been disclosed to it for years.

The second fundamental problem is that it manifests at least eight violations of the voluntary best practices that it supposedly implements. These are not technical violations. These are violations of the key substantive requirements. There are eight. LimeWire appears to be taking voluntary self-regulation no more seriously in 2009 than it did in 2003.

Finally, what LimeWire told the committee in a letter dated May 1, 2009 is that it had eliminated the problem of catastrophic inadvertent sharing of sensitive files by eliminating from its program something it called "recursive sharing of folders." This means that if you selected a folder to be shared, not only would you share the files in that folder, you would share all the files in all of its subfolders.

This design is indeed extremely dangerous. It enables one mistake to result in the sharing of literally thousands of files, personal files, all your documents, all your family photographs, all your scanned documents, all your home movies, and your entire music collection.

If that happens, you are set up for at least three forms of financial ruin. You can lose your job. You can become a victim of identity theft. You can be sued for copyright infringement. There are devastating results from virtually every type of file you would be sharing.

Chairman TOWNS. Could you summarize, Mr. Sydnor?

Mr. SYDNOR. Pardon?

Chairman TOWNS. Could you summarize?

Mr. SYDNOR. Certainly. The short of it is that LimeWire's own Web site design proves that it knew that this design was dangerous. Has it corrected it in LimeWire 5.2.8? No. What it did was to take out the dangerous feature that I identified in LimeWire 5.1 and reinsert an old dangerous feature, the recursive sharing of folders.

Mr. Gorton's written testimony tells you that there are three ways to share files in the most recent version of his program. That is wrong. There are four. The fourth way is to click the "Add Files" button revealed in his own screenshots. There you will once again be recursively sharing folders, the very feature that Mr. Gorton

and his trade association told this committee and other committees was the cause of catastrophic inadvertent file sharing.

We are not, still years later, witnessing good faith behavior. Thank you.

[The prepared statement of Mr. Sydnor follows:]

"Inadvertent File Sharing over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security"
A Hearing before the House Committee on Oversight and Government Reform

Written Testimony of Thomas D. Sydnor II,
Senior Fellow and Director of the Center for the Study of Digital Property,
Progress & Freedom Foundation

July 29, 2009

Chairman Towns, Ranking Member Issa, and Members of the Committee on Oversight and Government Reform, I thank you for holding the Committee's *third* hearing on the needlessly persistent problem of inadvertent file-sharing. My name is Thomas D. Sydnor II. I am a Senior Fellow and the Director of the Center for the Study of Digital Property at the Progress and Freedom Foundation (PFF), a nonprofit, nonpartisan think tank founded in 1993 to study the effects of the digital revolution upon commerce and society.

"Inadvertent file-sharing" affects users of popular file-sharing programs used primarily to illegally copy and distribute popular music, movies and software. Predictably, many users of these programs are preteen or teenage children, so inadvertent sharing often affects not just the particular user of a program, but entire families and the employers of family members. Inadvertent sharing occurs when users of these programs end up distributing to potentially thousands of anonymous strangers files that they did not *intend* to publish to the world at large. Two different "types" of files can be inadvertently shared.

First, users may inadvertently distribute *downloaded* files that they acquired by downloading them from a file-sharing network. Users affected by this type of inadvertent sharing often become copyright infringers or distributors of pornography or child pornography. Second, users may inadvertently distribute *personal* files already stored on their personal computer or later created or acquired through some means other than downloading. Users affected by this type of inadvertent sharing often "share" hundreds or thousands of files that could end careers, facilitate identity theft, and turn the user into a high-volume infringer of the copyrights in *thousands* of lawfully acquired songs or videos.

I have now co-authored or authored three studies of the causes of inadvertent file-sharing, and I have testified about these studies before two Congressional Committees. In 2007, as an attorney-advisor in the Copyright Group of the United States Patent & Trademark Office, I co-authored *Filesharing Programs and "Technological Features to Induce Users to Share,"* a report which explained why inadvertent sharing had recurred long after its causes and consequences were thought to have been understood and remediated.[1] I also testified at this Committee's *second* hearing on inadvertent sharing in July of 2007.[2]

---

[1] Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (USPTO Mar. 2007) at http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf.

Later, I co-authored *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform*, a paper which sought to correct and clarify misleading or inaccurate information provided to the Committee in 2007 by LimeWire LLC.[3] On May 5, 2009, I testified about inadvertent sharing during a legislative hearing before a Subcommittee of the House Committee on Energy and Commerce.[4] Most recently, in July of 2009, I authored *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5*.[5] Accept as otherwise noted, below, these prior papers and testimony provide sources for the claims made below.

The problem of inadvertent sharing should have been detected and resolved long ago. For example, the developers of the file-sharing program Napster—by actually studying the contents of file-sharing networks—detected and avoided the problem as early as 2000. In 2001, the ground-breaking study *Free Riding on Gnutella* warned that distributors of file-sharing programs might deploy "technological features to induce users to share" because so few users were *intentionally* "sharing" popular files. In 2002, the now-famous study *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, alerted even unobservant distributors of file-sharing programs to inadvertent sharing's consequences and causes.

Nevertheless, nine years later, inadvertent sharing remains a widespread and very dangerous problem. In late February of 2009, inadvertent file-sharing disclosed to Iran the plans for Marine One, President Obama's helicopter. Today Investigates also published a report on inadvertent file-sharing that revealed that the citizens of New York State alone were "sharing" over 150,000 tax returns over "peer-to-peer" file-sharing networks used mostly to pirate popular music and movies.[6] This report thus suggests that, nationally, over 2,000,000 tax returns were being inadvertently shared in February of 2009—an enormous data-security problem. Today Investigates also profiled the Bucci family, whose daughters, by misconfiguring the LimeWire file-sharing program, inadvertently "shared" their parents' tax returns with identity thieves who stole the family's tax refund.

To illustrate one reason why inadvertent sharing is still pervasive today—and can be expected to remain dangerously common in the future—I conducted an experiment this past weekend: I set up a test

---

[2] *See* Written Testimony of Thomas D. Sydnor II and Appendix A, *Hearing on Inadvertent File Sharing on Peer-to-Peer Networks Before the H. Comm. on Oversight and Government Reform*, 110th Cong. (July 24, 2007), at http://oversight.house.gov/story.asp?ID=1424.

[3] Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform* (PFF Oct. 2007) at http://www.pff.org/issues-pubs/pops/pop14.22inadvertentfilesharing.pdf.

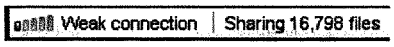
[4] Prepared Statement of Thomas D. Sydnor II, *Legislative Hearing on... H.R. 1319 The Informed P2P User Act before the House Comm. on Energy and Commerce, Subcomm. on Commerce, Trade and Consumer Protection*, 111th Cong. at http://www.pff.org/issues-pubs/testimony/2009/090505_P2P_sydnor_testimony.pdf.

[5] Thomas D. Sydnor II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF July 2009) at http://www.pff.org/issues-pubs/pops/2009/pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf.

[6] Today Investigates, *New warnings on cyber-thieves*, at http://today.msnbc.msn.com/id/26184891/vp/29405819%2329405819.

computer configured like my own family computer, which stores 16,798 personal documents, images, videos, and audio files in thousands of subfolders of a folder called *My Documents*.

After confirming that *no* version of LimeWire was installed upon this test computer, I then did something very dangerous: I downloaded the latest version of LimeWire 5, (version 5.2.8) and completed a "default" installation of the program. In other words, I clicked "Next," or accepted every default setting proposed by LimeWire; I did not change the "default" settings of LimeWire 5.2.8 in any way. Here were the results, enlarged for viewability:



In short, 16798 document, image, video, and audio files were automatically "shared" with tens of thousands of anonymous strangers *just by installing LimeWire 5.2.8*. Were this my actual family computer, my family would be sharing all of our work-related and personal documents, all of our scanned tax-related and identifying documents, many home movies, all of our family photos, and over 3,800 copyrighted audio files. This would likely ensure that my family would suffer one of three forms of financial ruin, (job loss, identity theft, or an infringement lawsuit). It would also expose my family and children to risks far worse than mere bankruptcy:

> [C]hild... predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers.... [T]hese individuals will [then]... download all additional information being shared from that computer.... This accompanying information can be used by the predator to locate... the potential victim.[7]

This latter threat is neither hypothetical nor remote: *The Washington Post* reports that in Virginia alone federal investigators from the Internet Crimes Against Children Task Force were able to obtain child pornography "from nearly 20,000 private computers in the state...."[8]

No rationally designed computer program should inflict risks like these upon families *just by being installed*. Worse yet, LimeWire *also knows* that LimeWire 5.2.8 can cause inadvertent sharing for *other* reasons. Every version of LimeWire 5 released to the public—from LimeWire 5.1.1 to LimeWire 5.2.8,

---

[7] *See* Written Statement of Tiversa at 5, *Legislative Hearing on H.R. 2221 and H.R. 1319 Before the Subcomm. on Commerce, Trade and Consumer Protection of the H. Comm. On Energy and Commerce*, 111th Cong. (May 5, 2009). The term "predator" is a frighteningly apt description of some members of the LimeWire file-sharing "community." *See, e.g., United States v. Park*, 2008 U.S. Dist. LEXIS 19688, (D. Neb. March 13, 2008) (a LimeWire user shared videos of an adult raping a little girl "bound with a rope and being choked with a belt"); *United States v. O'Rourke*, 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (a LimeWire user was held to be a "danger to the community" because he allegedly shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged").

[8] Chris L. Jenkins, *Officials Find Child Pornography on 20,000 Va. Computers*, The Washington Post, VA03 (Apr. 10, 2008) (reporting on the results of a state-level report prepared by federal agents) at http://www.washingtonpost.com/wp-dyn/content/article/2008/04/08/AR2008040803930.html.

which was released late last Wednesday—has contained other "features" that LimeWire *knew* were unacceptably dangerous.

In short, the problem of inadvertent sharing has persisted for nine years because distributors of file-sharing programs like LimeWire LLC have repeatedly responded to even the most serious and well-documented concerns about inadvertent sharing with half-measures, misrepresentations, whitewash, and other conduct that, considered in its entirety, could strongly suggest bad faith—an *intent* to cause and perpetuate inadvertent sharing. If these concerns prove to be warranted, then the numerous breaches of national, military, commercial, and personal security that this Committee and others have repeatedly documented were probably nothing more—or less—than the acceptable "collateral damage" of schemes intended to trick users into sharing popular music and movies, the types of files that drive high volumes of traffic toward file-sharing networks.

Given this long history of repeated failure and potential wrongdoing, it would be absurd to, yet again, rely upon entities like LimeWire LLC to remediate inadvertent sharing. History suggests too well what the consequences of doing so could be: more breaches of national and military security; more needless damage to private enterprises that could otherwise drive economic recovery; more identity theft; more endangered children; more early-releases for dangerous pedophiles; and more needless lawsuits between copyright owners and American families.

Nevertheless, the measures needed to *comprehensively* remediate inadvertent sharing are neither mysterious nor complex—they simply are not compatible with the interests of companies, like LimeWire LCC, that still insist upon trying to build businesses based upon unlawful uses of their programs. Consequently, I would respectfully suggest that this Committee should now pursue a two-pronged remedial strategy that need not rely upon the competence and good faith of entities like LimeWire LLC.

First, I would respectfully suggest that the Committee should formally refer this matter to those law-enforcement agencies that *currently* possess both the civil enforcement authority needed to effect a complete and swift remediation of inadvertent sharing *and* the criminal enforcement authority that may be needed if some of the conduct described below proves to be as deliberate as if often seems to be. The U.S. Department of Justice possesses relevant criminal enforcement authority, and because criminal copyright infringement is a "predicate act," it also possesses potentially relevant expedited civil enforcement authority under the Racketeer Influenced and Corrupt Organizations Act (RICO).[9] The state attorneys generals have also been concerned about inadvertent sharing since 2004; they also possess not only adequate criminal enforcement authority, but even broader civil enforcement authority under their state consumer protection acts.

Second, and simultaneously, I would also respectfully suggest that the Committee should support efforts to amend and enact H.R. 1319, The Informed P2P User Act, bipartisan legislation now pending in the House Committee on Energy and Commerce. Granted, existing laws already provide the authority needed to send a blunt and powerful message that would deter distributors of piracy-adapted file-

[9] *See MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 961 (2005) (Breyer, J., concurring) (noting that RICO could deter entities that intend to promote or cause widespread copyright infringement).

sharing programs from causing further inadvertent sharing or perpetuating that which they have already caused. Nevertheless, H.R. 1319 would target an intriguing "lighter-touch" approach toward the core problem underlying every incident of inadvertent sharing.

H.R. 1319 recognizes that the decision to publish a given file to the world at large is an extremely serious one that can implicate an array of state and federal civil and criminal laws—particularly if the file is to be published over a network as shadowy and lawless as the Gnutella file-sharing network to which programs like LimeWire connect. H.R. 1319 would thus grant to the Federal Trade Commission the additional remedial authority that the Commission needs in order to ensure that users of inherently dangerous programs like LimeWire never distribute *any* file *unless* they have received appropriate notice and then taken affirmative acts that clearly express their intent to "share" that file with anonymous strangers.

To understand the need for this two-pronged remedial strategy, it is critical to recall that this Committee, other agencies of the federal government, researchers, and security companies have long made extraordinary efforts to inform developers of programs like LimeWire about the causes and consequences of inadvertent sharing and given those developers repeated opportunities to remediate the problem voluntarily. Time and again, developers of such programs have failed to do so—and failed in ways suggestive of something worse than mere incompetence. Consider, for example, the following summary of *some* of LimeWire LLC's responses to this Committee's investigations of inadvertent sharing.

After the Committee's 2003 hearing on inadvertent sharing highlighted two features in file-sharing programs that were causing catastrophic inadvertent sharing, LimeWire and other distributors drafted a self-regulatory *Code of Conduct* prohibiting use of either feature—and then deployed both of them.

LimeWire inflicted the problem of inadvertent sharing upon its users—and itself—in the most effective way possible: it incorporated into its program "features" that had already been proven to cause catastrophic inadvertent sharing by computer-science research and this Committee. I have discussed LimeWire's 2002 to 2007 conduct in detail in *Filesharing Programs and "Technological Features to Induce Users to Share."* Consequently, I want to focus here on one "feature" that may best illustrate the seeming blatant bad faith displayed by LimeWire LLC from 2003 to 2007.

A "search wizard," as that term is used here, is a subroutine that activates *only* the first time that a given file-sharing program is installed on a given computer. When activated, it scans the computer's hard drive(s) for "media files" and "recommends" that a new user should recursively share folders that the program's developers think that new users might want to share. Search-wizards actually deployed usually "recommended" that new users whose computers stored large music collections in subfolders of their *My Documents* folder should share their *My Documents* folder and all of its subfolders. Users accepting this "recommendation" would thus share almost all of their personal files: all of their personal and work-related documents, all of their scanned or faxed work-related or personal documents, all of their home videos and family photos, and—of course—all of the many thousands of copyrighted audio files in their collections of popular music.

In retrospect, the mere existence of search wizards seems inexplicable for two reasons. First, search wizards target vulnerable new users—and new users of file-sharing programs will tend to be preteen and teenage children. Second, it is simply absurd for *anyone* to have urged *children* to recursively share the *My Documents* folder of their family computer. No one who understood the consequences should agree to share all the files in their *My Documents* folder and all of its subfolders. Consequently, reasonable program developers could never have released programs that delivered such dangerous "recommendations" to vulnerable teenage and preteen children.

But distributors of popular file-sharing programs did just that. Search wizards were deployed in many such programs, and some distributors (like LimeWire LLC) actually *began* deploying search-wizards *after* their obvious consequences had been confirmed and condemned by computer-science research, by this Committee, and by the *Code of Conduct* developed by distributors of file-sharing programs including LimeWire LLC. The following search-wizard chronology makes this point:

> **June of 2002**: In *Usability and Privacy, A Study of KaZaA Peer-to-Peer Filesharing*, computer-science researchers from HP Labs conclude that two "features" in the KaZaA file-sharing program, including a search-wizard, were causing users to share so many sensitive files inadvertently that identity thieves had begun data-mining file-sharing networks for inadvertently shared credit-card numbers. Distributors responded by continuing to deploy search wizards.
>
> **June of 2003**: A year later, hearings on inadvertent sharing held by the House Committee on Oversight and Government Reform and the Senate Committee on the Judiciary caused the distributors of KaZaA to belatedly recognize *Usability and Privacy* as "intelligent research," and to promise to remove both of the dangerous features it had criticized.
>
> **July of 2003**: The distributors of KaZaA did remove the dangerous features condemned by *Usability and Privacy* and the hearings, but they did so in an almost inexplicable way: both features, including the search wizard were removed in a way that *perpetuated* all of the consequences of the catastrophic inadvertent sharing that they had already caused.
>
> **September of 2003**: The distributors of LimeWire and other programs responded to the Committee's hearing on *Usability and Privacy* by promulgating a self-regulatory *Code of Conduct* that should have precluded use of KaZaA-like search wizards
>
> **Fall of 2003**: Copyright owners begin suing users of file-sharing programs "sharing" hundreds or thousands of infringing files. Published research found that such enforcement caused most users to drastically reduce the number of files that they shared, but oddly, a few kept on sharing hundreds of infringing files—almost as if they did not realize that they were sharing files at all.
>
> **January of 2004** (approximately): The distributors of LimeWire deployed a KaZaA-like search-wizard in their program. Its share-*My-Documents* "recommendations" appeared automatically during a default installation of LimeWire.
>
> **August of 2004**: Predictably, LimeWire's aggressive search wizard quickly caused catastrophic inadvertent sharing. Consequently, a reporter from the Boston Globe soon asked LimeWire LLC why its users were sharing classified military data. A LimeWire executive blamed its search

wizard: "One possible weakness in LimeWire is a feature that automatically scans the user's hard drive, looking for files to be shared over the network. [The representative] said this feature can make it easy to expose private information by mistake." Nevertheless, LimeWire kept deploying the search wizard.

March of 2007: the United States Patent & Trademark Office published an empirical analysis of five popular file-sharing programs entitled *Filesharing Programs and Technological Features to Induce Users to Share*. It specifically criticized LimeWire for violating its own *Code of Conduct* by deploying a search wizard. LimeWire kept deploying its search wizard.

June of 2007: The House Committee on Oversight and Government Reform, following up on its own 2003 hearing and the USPTO report, asked LimeWire to explain why it was it was still deploying a search wizard. LimeWire declined to explain, but it did—finally—remove the search-wizard from its program. But like KaZaA in 2003, LimeWire removed the search wizard while *perpetuating* all inadvertent sharing it had previously caused.

Such conduct—which was part of a larger pattern of similar conduct—cannot be easily attributed to good faith, negligence or even gross recklessness. On balance—and absent the alternative explanation that LimeWire LLC has so far declined to provide—it seems more likely to reflect *deliberation*: an intent to deploy a known means of directing absurdly dangerous "recommendations" towards vulnerable persons in order to cause them to share files inadvertently.

After the Committee's 2007 hearing on inadvertent sharing allegedly alerted LimeWire to the dire and pervasive consequences of inadvertent sharing, it responded by, among other measures, deploying inadvertent-sharing warnings that seem to have been designed to fail.

Conduct like that described above ensured that in 2007, the Committee had to open its *second* investigation into the causes and consequences of inadvertent sharing. But this time, the Committee secured far more detailed testimony about the *consequences* of inadvertent sharing. That testimony left even Lime Group CEO Mark Gorton shocked by the results of LimeWire's reckless-at-best conduct:

> I had no idea that there was the amount of classified information out there or that there were people who are actively looking for that and looking for credit card information.
>
> I think I've 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, you know, military documents, it really makes you think twice....
>
> I absolutely want to do everything in my power to fight inadvertent file-sharing. And I am sorry to say that I didn't realize the scope of the problem....[10]

[10] *Inadvertent File-Sharing over Peer-to-Peer Networks: Hearing Before the H. Oversight and Gov. Reform Comm.*, 110th Cong., 114-15, 117 (July 24, 2007).

Nevertheless, after the 2007 hearing, LimeWire opted for a familiar response: it decided to "help" its *new* trade association, DCIA, draft a *new* set of "voluntary" industry-self regulations so that responsible implementation of these *new* self-regulations could, again, be declared to have made inadvertent sharing a mere urban myth—an increasingly outdated concern.

Consequently, for two reasons, little need be said about the half-measures that LimeWire adopted from mid-2007 to 2009 while it was allegedly drafting and implementing what would become the DCIA *Voluntary Best Practices for P2P File-Sharing Software Developers To Implement To Protect Users Against Inadvertently Sharing Personal or Sensitive Data,* (the "*VBPs*") in what would become "LimeWire 5." First, the Marine One and Today Investigates reports alone suffice to prove the inadequacy of these measures. Second, whatever good these measures did is now largely irrelevant: LimeWire 5 actually eliminated most of these measures from more recent versions of the LimeWire program.

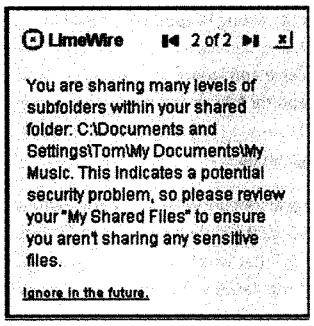
Nevertheless, one example may show why these many measures tended to fail.[11] For example, in the Lime Group CEO Mark Gorton's May 1, 2009 letter to the Committee (the "Gorton Letter"), LimeWire proudly explained that it incorporated into its "first major release following [Mr. Gorton's 2007] testimony" a new feature that would alert users to potential inadvertent sharing and help them remediate it by displaying a new you-are-sharing-too-many-files-or-folders warning:

> The third major change was designed to warn the use in the event an inordinate number of files were being shared, or a large number of folders were recursively shared, LimeWire displayed a warning telling the user that many files were being shared and giving the user the ability to go to their options menu and change this.

As LimeWire described it, this "warning" sounds like it should have been quite effective at alerting users to dangerous inadvertent sharing and helping them to remediate it. Nevertheless, subsequent events—like the Today Investigates report—reveal that it was actually a miserable failure.

And when you examine the delivery and appearance of this warning, the reasons for its miserable failure become clear. LimeWire "warned" its users that they were sharing too many files or folders by making a tiny little square full of 6-point type appear in the lower-right-hand corner of the screen and then automatically disappear seconds later:

[11] I analyzed other problems with LimeWire 2007 warnings and remedial measures in my second co-authored paper on inadvertent sharing, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform.*



At first, this might *seem* like a thoughtlessly designed warning: someone managed to bury the lead—"**potential security problem**"—two-thirds of the way down a box full of jargon and small print. Moreover, note that the Gorton Letter misrepresented this warning's effects: it *never* gave users "the ability to go to their options menu and [correct potential inadvertent sharing]"—it gave them only the ability to disable the warning.

Nevertheless, the overall design of this warning is so bizarre as to suggest deliberation. Why cram the warning into a little square when the entire screen was available? Why make the little square appear in the bottom-right hand corner of the screen (and thus, in the bottom right-hand corner of the user's peripheral vision)? Why would a warning about a "potential security problem" disappear automatically? And why on Earth is the background *baby blue*—a color generally associated with neither LimeWire nor "security problem" warnings?

Nevertheless, a familiar source seems to have "inspired" the odd design of the LimeWire "security problem" warning. Many users of the versions of LimeWire that displayed this warning routinely received *another* type of notice. This notice was not meant to alert users to a "security problem"—merely to note a routine event that users would usually want to ignore. Consequently, these notices would appear frequently in a little baby-blue square in the lower right of the screen and then automatically disappear seconds later. They looked like this:

It is difficult to imagine that any entity acting in good faith could manage to create a "security-problem" warning that just happened to look and behave a lot like the "You have new mail" notifications that users would routinely vaguely perceive and ignore. It is even more difficult to imagine that any entity at all would engage in such conduct and then brag about it to this Committee during its *third* investigation of inadvertent sharing. LimeWire LLC must think that such acts speak to its good faith and commitment to remediating inadvertent sharing. So do I.

In short, as 2009 brought forth new disclosures like the Marine One and Today Investigates reports, any remaining claim that LimeWire LLC might have had to good faith rode upon the behavior of the new version of its program, "LimeWire 5," that was to implement DCIA's *Voluntary Best Practices—the latest* set of anti-inadvertent-sharing self-regulations promulgated by LimeWire's *latest* trade association.

But the result was a virtual re-run of 2003: once again, LimeWire 5 failed miserably to comply with the *DCIA* VBPs. Once again, both LimeWire and its trade association denounced and renounced a particular "feature" as *the* cause of inadvertent sharing—only to see its effects recreated in LimeWire 5.1, and the feature *itself* re-introduced in LimeWire 5.2.8, the latest version of LimeWire 5.

After the Committee opened its 2009 investigation, every version of LimeWire 5 has violated the DCIA *Voluntary Best Practices* and contained features that LimeWire LLC *knew* were dangerous.

I provided a detailed analysis of the behavior of what could be called "LimeWire 5.1" in my paper *Inadvertent File-Sharing Re-Invented: the Dangerous Design of LimeWire 5*. The following testimony thus summarizes major problems with LimeWire 5.1 and analyzes whether those, or other, major problems affect the latest version of LimeWire 5, LimeWire 5.2.8, which was released late last Wednesday.

The unpredictably and deliberately dangerous, *VBP*-violating design of LimeWire 5.1: My paper on LimeWire 5 identified an array of problems with the 5.1.1, .5.1.2, 5.1.3 and 5.14 versions that LimeWire distributed from early March of 2009 until July 22, 2009. Three of these problems can be summarized briefly.

First, these versions of LimeWire 5 are dangerously unpredictable programs because LimeWire 5 and previous versions of the LimeWire program do not "uninstall" completely. Consequently, if users—like the Bucci family profiled by Today Investigates—try to halt inadvertent sharing by removing or uninstalling a misconfigured copy of LimeWire from their computer, they unknowingly implant within it a ticking time-bomb. If any identical or later version of LimeWire is ever again installed on that computer, obscure files stored in a hidden folder *invisible* to the average user can cause the newly-installed version to *automatically* begin sharing *all* files shared by the previously uninstalled version. As a result—and particularly if a family computer is being used by more than one person—there is no way for ordinary computer users to determine what files LimeWire 5 may share *just by being installed.* It may not share any files. It may share all the document, image, video, and audio files in *My Documents* and its subfolders; it may share only some of those files, or it may do something even worse. Absent careful forensic analysis of the hidden folders and files on a given computer, there is no way to be sure.

Second, while DCIA relied upon data from LimeWire to declare LimeWire 5 the "poster child" for implementation of its *Voluntary Best* Practices, versions of LimeWire 5.1 appear to violate at least *eight* critical obligations imposed by the *VBPs*: (1) LimeWire 5.1 can share User-Originated Files by default; (2) it shares User-Originated Files without timely and conspicuous warnings; (3) it shares "Sensitive File Types" by default—like the image files that store entire collections of scanned financial documents and family photos; (4) it recursively shares *folders* by default; (5) it does not uninstall completely; (6) it does not make users of prior versions "reconfirm" their "sharing selections"; (7) it can "share" entire *networks* by recursively sharing *Documents and Settings*; and (8) it gives no "prominent warning" to users sharing more than 500 files.

Third, and worst of all, LimeWire 5.1 incorporated a new feature that it *knew* was hopelessly dangerous. One mistaken click on LimeWire 5.1's dangerously ambiguous "share all" feature can publish *all* of the audio, video, image, and documents files in a user's "Library." LimeWire's own website thus warned that a user's "Library" must never include "any folder... that contains personal information." But by default, LimeWire 5 will *automatically* include in a user's "Library" all of the documents, family photos, scanned documents, home movies and entire collections of popular music and movies stored in *My Documents* and its subfolders. This seemingly deliberate wrongdoing thus put millions of families one click away from multiple threats of financial ruin—or something worse.

The unpredictably and deliberately dangerous, *VBP*-violating design of LimeWire 5.2.8: the Committee may hear claims that the latest version of LimeWire 5, LimeWire 5.2.8, corrects many or all of the concerns expressed in my latest paper. Any such claims are 66% wrong and 100% misleading.

First, LimeWire 5.2.8 is still a dangerously unpredictable program. It will perpetuate any and all inadvertent sharing caused by both currently installed *and previously uninstalled* prior versions of LimeWire 5 and most earlier versions of the LimeWire program.

Second, LimeWire 5.2.8 still appears to violate most of the major substantive obligations imposed by the DCIA *VBPs*. Indeed, since LimeWire 5.2.8 will *perpetuate* all inadvertent sharing cause by LimeWire 5.1, it also appears to perpetuate *all* of the *VBP* violations described in my latest paper.

Third, while LimeWire 5.2.8 did eliminate the *new* Library-*My-Documents*/"Share-All" feature that LimeWire *knew* was dangerous, it replaced this *new* dangerous feature with a *old* feature that LimeWire also *knew* was dangerous: recursive sharing of folders.[12]

[12] The phrase "recursive sharing of folders" is actually a shorthand way to describe a more complex reality. Folders are data-management tools intended to present the files stored on the hard drive of a personal computer in a hierarchical structure so different kinds of files will be easier to find, manage anc back-up. But the folder-structure on an ordinary personal computer was *never intended* to segregate a subset of the user's personal files that he or she might want to "share" with anonymous strangers. Nevertheless, earlier versions of LimeWire used folders (to quote the Gorton Letter) as a "shortcut for selecting many files and sharing them individually," even though folders are inherently ill-suited for that purpose. Worse yet, by default, most earlier versions of LimeWire would share folders *recursively*: in

Recall that LimeWire LLC and its trade association DCIA spent the spring of 2009 telling this Committee, Congress, and the public that *recursive sharing of folders* was a now-outdated feature that had been the root cause of most catastrophic inadvertent sharing:

> DCIA *VBPs*: "'Recursive Sharing' means the automatic sharing of subfolders of any parent folder designated for sharing.... Recursive Sharing shall be disabled by default...."
>
> DCIA Testimony to Congress: "[Inadvertent file-sharing is] an increasingly outdated concern over a very specific feature [recursive sharing of folders] of a small number of applications...."
>
> May 1, 2009 Gorton Letter: "LimeWire 5 did away with recursive sharing... did away with folder sharing...."

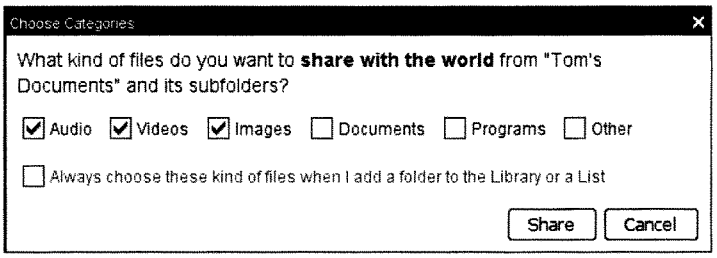
My most recent paper agreed that recursive sharing was an absurdly dangerous behavior, but it noted an equally dangerous flaw in the account of LimeWire 5 being offered by DCIA and LimeWire. LimeWire 5.1 *did still enable default recursive sharing of folders* during its installation-and-set-up process, but even after the program was installed and running a more serious problem remained: recursive sharing of folders was hopelessly dangerous because it made it far too easy for one mistake to "share" thousands of personal files inadvertently. Because LimeWire 5.1, by default, recursively loaded the contents of a user's *My Documents* folder into a "Library" that could be shared with one click of its ambiguous "Share all" button, it had re-created—in a slightly different way—the same conditions that made recursive sharing of folders so dangerous.

When confronted with the contradiction between its own website warnings, the default behavior of LimeWire 5.1, and the obvious defects in its "Share all" feature, LimeWire had little choice but to cease further deployment of this deplorable combination of features—though, once again, it has again chosen to perpetuate *any and all* inadvertent sharing that these features have already caused among the more than 50% of LimeWire users who were already using LimeWire 5.1.

Nevertheless, in LimeWire 5.2.8, the next general release after 5.1.4, LimeWire LLC did not really *remove* the library-*My Documents* and "Share all" features of LimeWire 5.1. Rather, LimeWire 5.2.8 *replaced* them with a familiar, tested substitute. As the following screenshot excerpt shows, LimeWire 5.2.8, *once again* has re-enabled *default recursive sharing of folders*:

---

other words if a user indicated that they wanted to share folder X, LimeWire would interpret that as a request to share all of the files stored in folder X *and* all of the files stored in all of the *subfolders, sub-subfolders, etc. of folder X*. Using this sort of *recursive sharing of folders* as a "shortcut for selecting many files and sharing them individually," ensured that one mistake could inadvertently share thousands or tens of thousands of a user's personal files.



The statement "and its subfolders" reveals what testing confirms: LimeWire 5.2.8 has re-enabled default recursive sharing of folders.

Indeed, preliminary testing suggest that the implementation of default recursive folder-sharing in LimeWire 5.2.8 may be more dangerously unbalanced that most implementations in prior versions of LimeWire. In LimeWire 5.2.8, it appears that while recursive folder-sharing will enable users to again make one mistake that shares thousands of personal files—even if those users were otherwise too unsophisticated to know how to select multiple files and apply an action to them. But should that happen, such LimeWire 5.2.8 users may have no means—other than file-by-file "unsharing"—to correct such all-too-predicable mistakes.

In conclusion, LimeWire *knew* that default recursive sharing of folders is hopelessly dangerous: both LimeWire and DCIA have so concluded, and those conclusions have been thoroughly validated by the years of empirical testing, on live human families, that LimeWire conducted while distributing "pre-LimeWire 5" versions of its program. Nevertheless, LimeWire *reinserted* default recursive folder-sharing into the latest version of its program, LimeWire 5.2.8.

Conduct like this—and the similar conduct described above and in my published papers and prior testimony on inadvertent sharing—lead me to conclude that the two-pronged, law-enforcement-based remedial approach that I have outlined, above, would be far more likely to protect the security of the our nation, our military, our economy, our families, our children, and even our copyright owners than any further reliance upon the competent, good-faith remediation of inadvertent sharing by entities like LimeWire LLC.

Chairman TOWNS. Thank you very much. Let me thank all of you for your testimony.

Mr. GORTON. Mr. Chairman, may I make a brief comment?

Chairman TOWNS. You will have an opportunity.

Mr. Gorton, the latest edition of LimeWire came out just last week. Are you telling us that the latest edition of LimeWire prevents unintentional file sharing?

Mr. GORTON. I believe in almost all cases it prevents unintentional file sharing.

May I briefly comment on Mr. Sydnor's statement? He tells a story of installing LimeWire on a computer that has no LimeWire currently installed and by default it shares thousands and thousands of files, including documents. I think it is important to point out what Mr. Sydnor didn't state. Again, I am assuming that this was the same thing that was in his written report.

In order to achieve the result that Mr. Sydnor just described, what he had to do was install a version of LimeWire on a computer and turn off all of the security settings that prohibit document sharing. Again, that single step in itself takes nine clicks and three warnings. He had to proactively go and share thousands and thousands of files.

So he basically sets up the program for the most dangerous possible situation. He then uninstalls LimeWire from his computer, which uninstalls the program but does leave settings. That is common industry practice. I mean, this is what is done by Microsoft, by Apple, and by Google. This is how settings are generally kept when programs are uninstalled. He then goes through the steps that he refers to in his testimony where he installs a new version of the program which then has its prompt.

But a user who affirmatively goes and sets up his computer and disregards so many warnings, at some point people do actually wish to share files. It is not that all sharing is inadvertent sharing.

I would just like to point that out as just one example of the methodological tricks that Mr. Sydnor plays in his reports. I would just encourage you to be careful and look very hard at his statements. I read his report and I was sort of shocked at first until I started parsing the words. It is a very cleverly worded report but I don't find it to be very accurate.

Chairman TOWNS. Mr. Sydnor.

Mr. SYDNOR. Thank you, Mr. Chairman. To frame what Mr. Gorton just said in a slightly different way, what I did is exactly what the Bucci family profiled in the Today Investigates report on inadvertent file sharing back in 2009 did. What happened is that their daughters installed a version of LimeWire on the family computer but misconfigured it.

The next thing you know, the family is inadvertently sharing tax returns and becomes the victim of identity theft. Then the Bucci family did exactly what you would think a normal person would do when they discover that type of problem. They uninstalled the program. That is exactly what I did in my test setup. I set up a version of LimeWire, created inadvertent file sharing, and then, to correct it, uninstalled it just the way an ordinary consumer might do.

In other words, the hypothetical that I presented to the committee is not at all hypothetical for the Bucci family or probably hun-

dreds of thousands of other families and computer users who have uninstalled some version of LimeWire 5. Mr. Gorton is asking you to accept the proposition that if somebody removes his program from their computer, that indicates their desire at some point in the future to restart all of the sharing that it might have been causing. That assumption simply does not accord to reality.

The difference between Mr. Gorton's account of how his program behaves and my report is that I try to look at how ordinary people would actually be using this program. Mr. Gorton is talking to you about ideal situations. Yes, if you install his program on a computer that you know no third party has ever had access to and you know that you have never ever installed any version of LimeWire on even years earlier, it will not share files by default. But that is not the ordinary situation for an ordinary family computer. It is certainly not the situation with mine and certainly not the situation for your constituents. Thank you.

Chairman TOWNS. I am going to ask you some questions now because my time is about to expire on me.

Mr. Gorton, the testimony we heard this morning demonstrates that there are still major problems with the most recent version of your software. By default it shares downloaded files. By default it shares images, music, and videos that may have been inadvertently shared in previous versions of LimeWire. It leaves behind hidden files when a user attempts to completely remove the software from their computer. Why haven't you fixed these problems and when will you fix the problems?

Mr. GORTON. Mr. Chairman, I am sorry. Let me just quickly address Mr. Sydnor's most recent answer.

Chairman TOWNS. But my time is expiring.

Mr. GORTON. The example he just gave about the Bucci family where the daughter accidentally set things up to share files, I strongly suspect that probably happened with a version of LimeWire 4 and not LimeWire 5. If there was an old version of LimeWire 4 that was uninstalled, if someone installs a version of LimeWire 5, it automatically unshares all documents, including tax returns. This is even if you upgrade from a version of LimeWire 5 to a new version of LimeWire 5. It puts up a warning that says, do you want to share these? It makes you very conscious of these things.

We have worked very hard to try and bring all of these issues up to the front and make it very transparent to users.

Mr. ISSA. I would ask unanimous consent, Mr. Chairman, for you to have such time as may be necessary for them to answer your questions.

Chairman TOWNS. Thank you very much. Because we try to run this committee by rules.

Mr. GORTON. I am sorry but would you mind repeating the question?

Chairman TOWNS. I would be delighted to. First of all, let me go back. The testimony we heard this morning demonstrates that there are still major problems with the most recent versions of your software. By default it shares downloaded files. By default it shares images, music, and videos that may have been inadvertently shared in previous versions of LimeWire. It leaves behind hidden

files when a user attempts to completely remove the software from their computer. My question is, why haven't you fixed these problems? I guess the second part will be, since you haven't fixed them, when will you fix them?

Mr. GORTON. I think as I just said, I believe that most of the problems that you are talking about we actually have already fixed. Again, I would caution you to be very careful of taking the testimony that you hear literally. I would encourage you to go through the steps that Mr. Sydnor——

Chairman TOWNS. You saw the demonstration.

Mr. GORTON. Yes. I am not saying that inadvertent file sharing does not happen in this world. What I am saying is that the sorts of things that you are seeing would be very unlikely to happen with the current version of LimeWire. There are hundreds of file sharing applications in the world. There are dozens of different file sharing applications which LimeWire is capable of searching. So the fact that you are seeing tax returns and other documents that were shared inadvertently does not mean that they are coming from a new version of LimeWire.

I will say that probably many of those documents are coming from old versions of LimeWire. I would encourage all people in the world who are running old versions of LimeWire to upgrade to the new versions to address these problems. Unfortunately, though we have done our best to try to communicate to people to upgrade to the new versions, we have not been able to persuade everyone to do that.

Chairman TOWNS. Mr. Gorton, reading back over your testimony from the last time, you are basically saying the same thing you said then. I just want to let you know that.

I now yield to the ranking member.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. Gorton, you said you are a technologist in your statement. Some would say I am an old technologist so bear with me. Do you know who Peter Norton is?

Mr. GORTON. Of Norton Anti-virus?

Mr. ISSA. Yes.

Mr. GORTON. I have heard of him.

Mr. ISSA. I go back to when he was just Peter. That is how old I am.

What was his goal in his product from what you can see from Norton Anti-virus? Wasn't it to protect customers from losses, from damage to their computers? Didn't he create a whole industry to do it? These are semantics now, but isn't that the history?

Mr. GORTON. I believe so.

Mr. ISSA. Are your customers less important to you than his customers?

Mr. GORTON. No.

Mr. ISSA. Do you try to protect your customers?

Mr. GORTON. Yes, we do.

Mr. ISSA. OK, then let us go through some steps. Why is it that you still have 4.18 on your site? You still offer today for download out of date software that is inherently more vulnerable by your own statements. Why do you still do that?

Mr. GORTON. I am not aware of us doing that.

Mr. ISSA. My own people who are not technologists checked on it today. It is still there.

Now, you talked about de facto standards. You quoted Microsoft. I will leave Microsoft out of it for a moment. When I uninstall your product, do you provide an uninstall capability?

Mr. GORTON. Yes.

Mr. ISSA. So you don't rely on the default of Microsoft. You control the uninstall. Isn't it true that when you uninstall with your own software, your software programmers or your technologists could move those switches back or allow the customer to make that decision? Isn't that something you could easily write into the code?

Mr. GORTON. Yes.

Mr. ISSA. OK. So you still have the old software. You have an uninstall routine that does not, in fact, re-protect or offer an opportunity to re-protect the customers. Isn't that true, at least as of today?

Mr. GORTON. So document sharing is turned off by default in LimeWire 5. In LimeWire 4, when you reinstall——

Mr. ISSA. No, no. Hold on for a second. I have LimeWire 4.18.

Mr. GORTON. Yes.

Mr. ISSA. I update to LimeWire 5.2.8.

Mr. GORTON. Yes.

Mr. ISSA. I go to uninstall. Does your software give me the opportunity to fully protect, to take those items which I had maybe chosen to turn on or not, I notice, by the way, that MP3, MPEG, and so are not on this list but DOC, WRI, DVI, LaTeX, and so on, do you in your uninstall provide the re-protection or do you leave it sort of switched as it was?

Mr. GORTON. If you have version of LimeWire 4 and you upgrade or install——

Mr. ISSA. I have already updated. I am talking about your current version, when I uninstall your current version.

Mr. GORTON. No, when you install the current version it automatically will unshare documents that were previously shared.

Mr. ISSA. Right. But now I have chosen to share them. Now I am uninstalling the software. Does your software allow me to unshare them at the time that I am uninstalling? You are in control of that, right? This is not a Microsoft standard. You are in control of that decision.

Mr. GORTON. That is true but when you——

Mr. ISSA. OK. So I think we have kind of come through some of the things you could do. I am not saying you must do them all. I am saying you could do them. You are not doing them for your customer. Now, you are not forcing people to upgrade to LimeWire 5?

Mr. GORTON. We have no mechanism to do that.

Mr. ISSA. Oh, you don't? Wouldn't it be relatively simple? As an old software guy to a younger software guy, you could create the capability where when LimeWire 4 users try to share they would see that they are blocked from sharing with LimeWire 5.2 and above unless they upgrade. That wouldn't be hard for you to do. LimeWire 5.2 could deliberately be incompatible with LimeWire 4.1. You could create a block on that. That is doable, isn't it?

Mr. GORTON. Yes, we could break compatibility with it.

Mr. ISSA. So, if you care about your customers and you know that LimeWire 5.2.8 has much better protection for them, if you wanted to protect your customers one of the easiest ways is to force out the older generation software. That is something which, since you write the software, you are in control of doing.

I spent 20 years in automotive security. I think about security and I think about what can I do for my customers. I also think about how to make car alarms not go off. That is the hard part. Making them go off was easy. It sounds like sharing, which is easy, is what you do.

These are simple questions and I could go on for a lot longer with them. Any consultant you hire could help you with those. If you were thinking in terms of security, you would have asked and answered those questions for your customer.

Anyone can make a car alarm that goes off all night. It is hard to make one that doesn't go off except when someone is stealing your car. Anyone can make file sharing easy. What are you doing to protect your customers so that file sharing is not something that leads to these inadvertent acts for them or others?

Mr. GORTON. We have taken a large number of steps, which I have documented in my written testimony. But I also——

Mr. ISSA. I appreciate that but you don't get credit for what you can't answer today that was that simple.

Mr. GORTON. Many of the steps that we have taken have come from outside suggestions. We would be happy to look at any suggestions that you have or anyone else has as to how we can improve our program. We have taken a large number of steps. Are we perfect? No, we are not perfect. We would be happy to look at anything and continue to work going forward to get as close to perfect as we can get.

Mr. ISSA. I appreciate that. My time for new questions has expired. Could the other two gentlemen just comment on the line of questioning I explored, please?

Mr. SYDNOR. Ranking Member Issa, thank you. I think that is exactly correct. The problem that you have illustrated and that I think you can see live here is that Mr. Gorton has made some improvements, but he made improvements that relate to types of documents that don't actually drive a lot of traffic toward the Gnutella network. So whenever you see somebody who is inadvertently sharing document files, sensitive personal documents, my experience of actually looking at what happens on Mr. Gorton's network, something that LimeWire itself really does not do much of, shows that whenever that is happening they are sharing many other types of files.

I illustrated the dangers of that in my 2007 testimony, basically pointing out that if that happened to my family, yes, the document files would be important to me but the most dangerous files in terms of identity theft and the safety of my children would actually be the image files. Those would be the most dangerous. I laid that out in my 2007 testimony.

Lest anyone think that I was wrong, I will just quote some testimony from Mr. Boback. "Tiversa has documented cases where child pornographers and predators are actively searching P2P networks for personal photographs of children and others that are stored on

private computers. Once the photographs are downloaded and viewed, these individuals use the browse host function provided to view and download all additional information being shared from that computer."

The changes Mr. Gorton's program makes don't solve that problem. They don't solve the massive copyright infringement problem. They are half measures.

Mr. BOBACK. My only comment is that LimeWire has made changes in the time since our last testimony. However, from our oversight view of that, they have lost market share since that time. Users have transitioned to other places and other clients as LimeWire has made the changes.

Our own personal concern with LimeWire 5.0 and up is that for some unexplained reason, Tiversa, which is the only oversight to a number of peer-to-peers, was hard coded in a block so that we would be unable to see every user of 5.0 and up. Now, we don't interfere with the network at all. We don't touch LimeWire clients. We don't stop downloads. We have never taken a dollar from the Motion Picture Association or the recording industry. However, for some reason our entire IP address range that Tiversa uses to monitor has been hard coded, which means someone literally typed into the LimeWire code to not ever connect to anyone associated with Tiversa. We posed the question to the CEO of LimeWire and I still have yet to have a response.

Mr. ISSA. Mr. Chairman, I would ask unanimous consent to include in the record at this time the screenshots in HTML format from July 28, 2009 showing the previous versions of LimeWire that were available as of that date. I would like that included in the record.

Chairman TOWNS. Without objection, so ordered.

[The information referred to follows:]

- Music Blog
- Music Store

Other languages:
English English

LimeWire

- Home
- Features
- Support
- Development

Get LimeWire for Your Platform

Latest Release

The latest stable release of LimeWire is **5.2.8**. For more information, see the release notes.

- Windows *(NT, 2000, XP, Vista)*
- Mac OS X *(10.5 Leopard Intel 64-bit Only)*
- Linux *(Ubuntu, Debian)*
- Other Systems *(OS/2, Solaris, Linux)*

Get LimeWire PRO for **free** when you complete an offer with TrialPay.

Get It Free

Past Releases

These versions of LimeWire are no longer maintained, but are made available to you for your convenience.

- LimeWire 4.0.10 *(For Mac OS 9.2)*
- LimeWire 4.8.1 *(For Mac OS X 10.1 - 10.1)*

- LimeWire 4.12.15 *(For Mac OS X 10.2 - 10.3)*
- LimeWire 4.18.8 *(For Windows 95 - Vista; Mac OS X 10.4 Tiger - 10.5 Leopard; Linux)*
- LimeWire 5.1.4 *(For Windows NT - Vista; Mac OS X 10.5 Leopard Intel 64-bit; Linux)*

Get LimeWire PRO

Get PRO for a single payment of only $13.95.

Get PRO

Extend your PRO benefits!

Get PRO for 1 year 20% off. Only $34.95!

Extended PRO

About

- LimeWire
- The Company
- Team
- Press Room
- Contact
- Careers

Legal

- License
- Refund Policy
- Privacy Policy
- Copyright Information
- Using P2P Safely

Other languages:
English English

Portions of this web site are available under a Creative Commons license, where noted. © 2000 - 2009 Lime Wire LLC.

Mr. ISSA. Mr. Chairman, it is interesting that Mr. Gorton was so livid in saying that ISPs could protect and then showed that he can protect from a specific range of a particular ISP.

Chairman TOWNS. That is interesting. I now yield to the gentleman from Maryland, Mr. Cummings.

Mr. CUMMINGS. I am sitting here and listening to all of this. I heard what Mr. Issa said from the beginning. He said that if we were to find certain things happening here, this is something that should be referred to the Justice Department. After seeing what Mr. Boback presented here a moment ago, it is chilling what the public now has available to it, the idea that you can look at the First Lady's information, figure out where she is going, how she is getting there, and so forth and so on and tax records and things of that nature. In some kind of way we have to get to the bottom of this.

I have been sitting here listening to you, Mr. Gorton, trying to figure out whether you have sincerely done everything you can to protect the American people with regard to this kind of information being put out there. But now I am going to pick up right where we left off with Mr. Boback, with what you just said.

Why did LimeWire, Mr. Gorton, block Tiversa from access to its portals after assuring the Committee on Oversight and Government Reform, this committee, that it was fully committed to correcting the inadvertent file sharing troubles to which it had contributed? First of all, is what he just said true? Did you all block Tiversa?

Mr. GORTON. I don't have any specific knowledge of that so I can't say.

Mr. CUMMINGS. Wait, wait. So you are saying you don't know whether it happened?

Mr. GORTON. That is correct.

Mr. CUMMINGS. OK, go ahead.

Mr. GORTON. But I can tell you a little bit about what LimeWire does to fight spam. Again, now we are getting into a little bit of sort of the technical details of the way peer-to-peer networks work. But peer-to-peer networks are distributed. What that means is that each of the computers on that network are connected to each other through sort of a chain effect. Messages and searches are conducted as messages are passed from one computer to the next. There are certain people and computers in this world who are spammers who respond to every search that is done on LimeWire with all sorts of messages and things like that.

Mr. CUMMINGS. Mr. Gorton, I am going to have to cut you off. The only reason I am going to cut you off is that I don't have that much time. They only give us 5 minutes.

Let me just ask this of you, Mr. Boback. I am going to come back to you if I have time. Do you think he is doing all that he can to address the problems that you showed us in the demonstration? What else could he do? That is what my constituents want to know.

Tonight I am going to have a town hall meeting over the phone. If people saw this while we have this new piece about digital records and all that, people are going to say, "wait a minute, hold it. The fact that I have cancer or my whole IRS return and all my records will all be out there in cyberspace?"

Has he done all that he could have done in your opinion? Were you blocked from helping him?

Mr. BOBACK. In my opinion, no, they have not done everything that they could possibly do. We provided an option after the 2007 hearing where we were willing to work with them, to say we see some obvious solutions of how you can do this. Rather than just blocking at the ISP, there are a number of things you can do. Those conversations ceased shortly thereafter. Then 6 months after that we were blocked.

We are not a spammer. We don't respond to searches. We are absolutely passive on the network. When our system gets a search, it passes it right on through without changing the search, without downloading it, without doing anything. We are absolutely passive on the network. We don't block a single file. We don't spam advertising. We don't do $1 in advertising. So therefore we are not a spammer and we were, in fact, blocked as of March 2008. They blocked us 6 months after they ceased discussions as to the solutions that we offered.

Mr. CUMMINGS. Mr. Gorton, back on July 24, 2007, you said that you had no idea there was that amount of classified information out there or that there are people actively looking for that and for credit card information. Is this shocking to you? Does it bother you that this information is out there like that?

Mr. GORTON. Absolutely.

Mr. CUMMINGS. So you are going to promise us some more today of things you are going to do?

Mr. GORTON. I can promise you our ongoing commitment to continue working on this problem. I will say that I think we have made enormous strides in the past 2 years and that certainly the vast, vast, vast majority of inadvertent file sharing with LimeWire has been eliminated in the new versions. We are happy to continue working going forward to do whatever we can do.

We take our responsibility to our users very seriously. We don't want anyone to have an unpleasant experience in any way from using LimeWire. I can certainly see that if someone has their tax records revealed publicly that is a pretty serious thing. We take this seriously and that is why we put in so much effort. We are a small company. A good fraction of the programming resources of our entire company has gone to combating this problem. I think we have made very good progress.

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

Chairman TOWNS. I thank the gentleman from Maryland. I now yield to the gentleman from New Hampshire, Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman. Thank you all for your testimony.

Mr. Gorton, I find your testimony today stunning. You promised us 2 years ago that you were going to fix what ails LimeWire. Your testimony today basically for me is essentially, "why are you picking on me." There are others out there who are facilitating breaches of national security, who are facilitating commission of child sex crimes, who are facilitating the theft of property from musicians and owners of copyright, and who are facilitating identity theft.

Mr. Boback, Mr. Gorton testified essentially that using a recent version of LimeWire you couldn't engage in the kind of activity that you highlighted by showing us in real time what was going on. He then modified that testimony when asked a question by the chairman to say it was very unlikely to happen. Are either of those statements true?

Mr. BOBACK. He is correct in saying that it less likely on LimeWire than it is in some other peer-to-peer clients. However, all of the demonstrations that we showed here today were in fact LimeWire disclosures occurring from a LimeWire client. I could have shown BearShare and other disclosures as well but we specifically have LimeWire.

Mr. HODES. Were you using current versions of LimeWire to do the demonstration today?

Mr. BOBACK. The tax return video was actually a 4.18 version of LimeWire but it accessed information that was out there. What I have found is that most of the users don't want to upgrade to 5.0 because it further decreases their access to other information. Therefore, they don't want to do it.

Mr. HODES. Mr. Gorton, you have heard about the incident in which the blueprints for Marine One, the Presidential helicopter, ended up in Iran?

Mr. GORTON. Yes.

Mr. HODES. Did anyone in your organization attempt to remove that file or take any other action when you heard about that?

Mr. GORTON. We have no mechanism to remove files from people's personal computers.

Mr. HODES. But did you do anything to block access to that information in any way?

Mr. GORTON. Again, the Gnutella network is a decentralized network which LimeWire doesn't run. So I think maybe using an Internet browser is perhaps analogous.

Mr. HODES. Let me ask you this question: When you heard about the plans for Marine One, the Presidential helicopter, ending up in Iran, did you take any action at all? Yes or no.

Mr. GORTON. Yes.

Mr. HODES. What did you do?

Mr. GORTON. We have made changes to the current version of LimeWire so that such a breach would not happen today.

Mr. HODES. Is there any file of information you would try to have removed if it was brought to your attention? For example, if you heard or found there was a file containing directions for making an IED that could harm our soldiers in Iraq or Afghanistan, is there anything you would do?

Mr. GORTON. Again, I think those files should be removed from the network but LimeWire does not control the computers of people around the country.

Mr. HODES. How about child pornography? You understand that LimeWire is being used as we speak to facilitate the commission of child sex crimes? You understand that, right?

Mr. GORTON. Yes.

Mr. HODES. What are you going to do about it?

Mr. GORTON. LimeWire is in the process of working with the New York State Attorney General's Office on specifically this prob-

lem. We, in conjunction with the New York State Attorney General's Office, are building a filter to remove child pornographic material.

Mr. HODES. Why didn't you do that 2 years ago?

Mr. GORTON. We do not have a list of——

Mr. HODES. Why didn't you build the filter you were just telling me about 2 years ago when you came before this committee? We talked about the problem and you promised us you would fix it. Why didn't you do it 2 years ago? Answer my question.

Mr. GORTON. Again, I am pointing out that in order to solve the problem which you are describing, you need to know which material is child pornographic material. LimeWire by itself does not have that knowledge. So we have had to work with outside third parties in order to gain knowledge of what that material is. There are certain organizations in the world whose job it is to maintain lists of that material. LimeWire is in the process of working with them in order to filter that material from the network.

Mr. HODES. Did you start 2 years ago when you promised us you were going to fix the problem? Yes or no, just a simple yes or no, Mr. Gorton.

Mr. GORTON. I don't know the date we started working on this.

Mr. HODES. So you can't tell us that after leaving this committee room 2 years ago when you promised us you would fix it that you started fixing it, right?

Mr. GORTON. I know that it is an ongoing effort that we are working on today and that we hope to resolve it soon.

Mr. HODES. Thank you.

Mr. TIERNEY [presiding]. Thank you, Mr. Hodes. Mr. Foster, you are recognized for 5 minutes.

Mr. FOSTER. The hidden files that persist as you update, are these things files, registry entries, or hidden files? What is the exact nature of these? Is there anything special about them, Mr. Gorton?

Mr. GORTON. I have to say that I am not 100 percent sure but I believe that they are regular files. I believe when they are called hidden they are by no means obscured from the user. If you were to go look in the directory, you would see the preference files. They are not invisible in any way except that people don't normally choose to examine them.

Mr. SYDNOR. Representative Foster, could I correct the record on this?

Mr. FOSTER. Certainly.

Mr. SYDNOR. That is simply false. I am familiar with the nature of the files. I have looked at them. They are stored in a place where users never go in a hidden folder. It is invisible to the ordinary user. Yes, if they de-hide that folder, they could conceivably find it. But by default that folder is invisible. If you can't find that folder, you can't find the files in it. It is as simple as that.

Mr. FOSTER. But this is a standard industry practice to hold things like which could be registry entries or detailed settings?

Mr. SYDNOR. Not that I am aware of. LimeWire leaves an enormous amount of material behind when it uninstalls. I am simply not aware, I just don't believe that it is accurate when Mr. Gorton claims that companies like Microsoft and Google do this. I do not

believe that they leave behind the types of configuration files that could have dangerous effects if they are reactivated by another version of the program that chooses not to overwrite them. It is not true.

Mr. FOSTER. Mr. Gorton, your statement that you can't force an update when this sort of problem occurs, is that a feature of your most recent software as well?

Mr. GORTON. Our current software does have update capabilities but the old LimeWire 4 something, I don't know exactly at what point but there are old versions in which we are not able to send an update message.

Mr. FOSTER. I guess this would be best directed at Mr. Boback. The nuclear option is to block the Gnutella protocol at the very high level Internet router level if this really becomes intolerable, if you start seeing nuclear weapons designs out on this thing and it becomes important to do. The obvious risks there are free speech risks. I personally don't see any mechanism instead of technologies that would allow you to block child pornography that would also not allow you to shut down Falun Gong. This is the tough situation we are in.

First off, businesses, however, can choose to block the Gnutella protocol. A hospital, for example, could just say, "we don't want any file sharing on our computers." Many businesses, I believe, do that. National laboratories, I believe, do block file sharing protocols. Is that consistent with your experience?

Mr. BOBACK. All of our clients block peer-to-peer applications from being downloaded. The problem is that people work around those because they want music, for one. I will tell you that all of our clients of the Fortune 500 have all had disclosures on peer-to-peer despite the recommendations for them to avoid that. In fact, we even found the rules and regulations for IT security saying to block peer-to-peer on a large Fortune 100 company.

Mr. FOSTER. These come from people bringing their computers and files home to places where they are not protected. At least at the workplace there is a simple thing to just wipe out the Gnutella protocol.

Mr. BOBACK. For the most part.

Mr. FOSTER. Similarly, the military, do they block all peer-to-peer connections on the military networks?

Mr. BOBACK. I believe that the military does discourage the use of peer-to-peer. However, being a disbursed group, there is no way to stop it entirely. It is like stopping crime. You have to monitor it and that is what we have chosen to do.

Mr. FOSTER. But on the military subnets, they can presumably just block it. Do you know for a fact whether they do or do not?

Mr. BOBACK. I do not know for a fact.

Mr. FOSTER. Mr. Gorton, it seems to me that the sensible solution to this is that instead of having an exclusive list, a list of things we are not going to share, that the user should have to say yes, I want to share this file and click on it. They should have to march through every single file and explicitly say yes, I recognize this file instead of just clicking on the whole C: drive.

Mr. GORTON. What you describe is the current practice with LimeWire. You have to affirmatively select each file or——

Mr. FOSTER. Every single file, including everything you download?

Mr. GORTON. Downloaded files, I believe on installation you have a choice whether you want to automatically reshare or not reshare files that you download.

Mr. FOSTER. OK. Then this question of trying to recall old versions of it, my understanding is that would be essentially impossible because the Gnutella protocol is a multi-vendor open protocol. There is no way that you can stop those old versions from working. Is that correct?

Mr. GORTON. Yes. It is a piece of software on a person's individual computer and they control it.

Mr. FOSTER. Right. So the only way to stop old versions from working would be, for example, basically for the whole world to block the old Gnutella protocol and reimplement a Gnutella protocol where you actually had control over who gets to write clients and what the procedures are on that. To me, that would be the only the solution that would allow you to actually flush out the problems with the current system. Otherwise you would be left with the old Gnutella protocol doing whatever bad features with whatever bad old versions of the software are out there. Are you aware of any other way that we can flush out the old versions of the software?

Mr. GORTON. It is certainly very difficult because those versions of LimeWire don't just connect to the new versions of LimeWire. They connect to dozens of other P2P clients.

Mr. FOSTER. Which could only be shut down by a worldwide effort to block them and then reimplement a new version that didn't have these problems.

I yield back.

Mr. TIERNEY. Thank you, Mr. Foster. Mr. Connolly, you are recognized for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman. Mr. Gorton, Mr. Sydnor sort of laid out three broad critiques of LimeWire. I wonder if you would respond. The first was that it is dangerously unpredictable. In installing the software, his experience was that just by default 16,798 documents showed up inadvertently displayed. Could you comment? Is your software dangerously unpredictable from your point of view?

Mr. GORTON. I do not believe it is dangerously unpredictable. Again, I think it is worth talking about the situation. In order to get the result that Mr. Sydnor described, he had to install a version of LimeWire 5.0 or greater, disable all of the security features that are built into it, disregard the many warnings, and affirmatively choose to share thousands of files. Then he had to uninstall that version of LimeWire and install a new version of LimeWire. Then, once that new version of LimeWire was installed, there would be warnings that would pop up that would ask him——

Mr. CONNOLLY. I am going to have to interrupt you because we have limited time here. I just want to get at the essence of your answer. I get it. Your view is that he is the one who is dangerously unpredictable, not your software?

Mr. GORTON. I am not sure I would characterize him that way.

Mr. CONNOLLY. But you just went through all the steps he had to take that made him dangerously unpredictable. Is it your contention that if we directed our committee staff to do what Mr. Sydnor did we would or would not come up with the same results here at the committee?

Mr. GORTON. If you got a version of LimeWire 5, removed all the security settings, ignored all the warnings, chose to share files, uninstalled that program and then installed a new upgraded version, you would still be presented with warnings which you could then ignore.

LimeWire is file sharing software. It is not unreasonable to think that people who install file sharing software might actually want to share files. What we try and do is make it so that the files they share are only files they want to share.

Mr. CONNOLLY. Mr. Chairman, I may be a freshman but the light has stayed on red.

Mr. TIERNEY. It is because you are a freshman. [Laughter.]

So you gave the answer and the question in the same breath. [Laughter.]

Mr. CONNOLLY. I thank the Chair.

Mr. Sydnor also said that in addition to being dangerously unpredictable, one of his three points was that you were knowingly dangerously unpredictable. In other words, this isn't accidental or this isn't just a feature of the software that is something we can't really control. You knowingly have, in fact, manufactured, sold, and operated software that has this dangerous default with what he characterized as "devastating results." I assume your view is that is just not true.

Mr. GORTON. That is absolutely untrue. I can tell you that we take this problem seriously. We are actively working to resolve it. I will say that there are situations which can occur in the world which didn't occur to us in testing involving weird combinations of installing old software and new software. As these edge cases come up and they are pointed out to us, we address each one as it comes along.

I would like to think that we have caught every last problem. That is probably not true. But as they are pointed out to us, we go and take the steps that are necessary to ensure that those problems don't continue.

Mr. CONNOLLY. The third point he made was that he could identify at least eight violations of voluntary best practices, suggesting that self-regulation in your case doesn't work.

Mr. GORTON. He did not say what those violations were. This is coming from his paper and my recall of the specifics is not perfect, but I believe that many of those claims about us disregarding those eight best practices are false. I think he may have pointed out an issue or two which we have since resolved. I believe that all eight issues which he discussed before are currently nonexistent.

Mr. TIERNEY. The red light, Mr. Connolly, has truly come on now.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. TIERNEY. We appreciate your questions and thank you for them. Mr. Duncan, you are recognized for 5 minutes.

Mr. DUNCAN. Mr. Chairman, thank you very much. Mr. Boback, I was interested to read in the briefing paper that your company did a demonstration in January 2009. It says that Tiversa was able to locate and download more than 275,000 tax returns. Is that accurate?

Mr. BOBACK. That is accurate. Yes, sir.

Mr. DUNCAN. Do you feel that you basically can get anybody's tax return that you want to?

Mr. BOBACK. Surprisingly we can get a great deal of information. Yes, sir. I don't know about anyone, but most people.

Mr. DUNCAN. When we run for Congress, we basically forfeit or give up any right to privacy and we sort of have to accept that. But do you think there is any real privacy in this country anymore if anybody can get almost anybody's tax returns or medical records or bank records or anything else that they want to get?

Mr. BOBACK. It has definitely been depleted quite a bit with this application, yes.

Mr. DUNCAN. I know that we have taught all of the young people to worship the computers now and so forth and to become addicted to them, but it seems to me that it is sad that we are so controlled now that we basically have done away with almost any privacy that private citizens should have in this country.

How skilled a computer user does one need to be to hack into files that are not intended to be shared?

Mr. BOBACK. It is as simple as doing a Google search. Literally you would type in "tax return" and hit "search."

Mr. DUNCAN. That is what I thought you would say. In fact, several years ago I was driving back from lunch in Knoxville one day and I heard on the CBS radio national news that computer hackers had hacked into the top secret files of the Pentagon that year. It was many thousands of times. I don't remember exactly how many.

Then I remember a few years ago when the front page of the Washington Post had a story about a 12 year old boy hundreds of miles away from the Hoover Dam who had opened the floodgates at the Hoover Dam. I suppose in one way that is funny but in another way it is pretty sad and it is also pretty dangerous, it seems to me, to our national security.

At any rate, Mr. Chairman, thank you very much for holding this hearing.

Mr. TIERNEY. Thank you, Mr. Duncan. We appreciate that.

Mr. Gorton, I just want to ask you a question. You said that you personally knew nothing about the fact that Mr. Boback's system had been shut out of your software, I guess, right?

Mr. GORTON. That is correct.

Mr. TIERNEY. So will you reinstate it now? Will you remove that barrier?

Mr. GORTON. We can certainly talk to Mr. Boback.

Mr. TIERNEY. What would that discussion involve?

Mr. GORTON. As I was saying before, LimeWire has a system for identifying spammers. And then——

Mr. TIERNEY. You consider Mr. Boback's group a spammer?

Mr. GORTON. I do not.

Mr. TIERNEY. So what else is going to be involved in the discussion?

Mr. GORTON. But it may be that there is something about the profile of the way his systems behave that matched our identification for a spammer. We can try and work with Mr. Boback to make sure that he is not falsely identified as a spammer.

Mr. TIERNEY. Why did you break off the conversations with him? I assume those would be the type of things you would have discussed with him after the last hearing. Mr. Boback says you were working along and you stopped the discussion.

Mr. GORTON. I believe the conversations he was referring to were his attempt to get LimeWire to purchase and distribute the software which he is selling and the service which he is selling. He has a system which flags security concerns. It was our preference with LimeWire, rather than to create a system which identified security problems, we would rather eliminate them. We felt that if we did a proper job eliminating inadvertent file sharing there would not be a need for Mr. Boback's software.

Mr. TIERNEY. Set aside whether you want to buy his services or anything of that nature. Why would you block him?

Mr. GORTON. This is what I was saying. We have an automated system which goes and looks for spammers. I believe that his company's systems in some way have a profile of a spammer and they were inadvertently flagged as a spammer.

Mr. TIERNEY. Does this make any sense to you, Mr. Sydnor?

Mr. SYDNOR. Mr. Chairman, no, none whatsoever. Tiversa's service has been operating. I first encountered them some years ago when I began investigating this problem. It has been operating for years. If it triggered some automatic spam filter, it should have done so years ago.

The timing would suggest that right after the last big round of very significant disclosures about very significant episodes of inadvertent file sharing involving LimeWire, which Tiversa did help, as I recall correctly, the reporters and the military identify, that is when the block occurred. That is interesting timing for an automated spam detection system.

Mr. TIERNEY. Mr. Gorton, let me tell you that is how it looks from here. Disabuse us of that notion if you can.

Mr. GORTON. Certainly. First of all, let me start by saying that I think that systems like Mr. Boback's have a positive and constructive role to play. I have no desire to see them shut down.

Mr. TIERNEY. So who in your company do you think had that desire and then physically blocked them?

Mr. GORTON. Like I said, it is an automated system.

Mr. TIERNEY. No, no. Let us back up a second. Somebody had to physically go in and block them out. So who in your company is in charge of doing that?

Mr. GORTON. No. Like I was saying, we have an automated system which identifies IP addresses. There is no human being involved.

Mr. TIERNEY. All right, we have heard that before. What do you think of that, Mr. Sydnor?

Mr. SYDNOR. Mr. Chairman, I simply don't think it is credible. I have known Mr. Boback's company for years, worked with them for years. Their service, so far as I know, has operated relatively similarly. It simply does not make sense that right after the latest

round of disclosures that they somehow for the first time would have tripped the automatic spam filter. That is exactly the sort of very interesting question that I think a law enforcement agency could investigate.

If I could add one final point, it is that I realize there has been a bit of he said/she said between Mr. Gorton and I today about how his program actually behaves. That is totally unnecessary. We are talking about the behavior of a computer program. It will do the same thing every time. I am happy to come in and demonstrate for any member of the committee or the staff exactly how I do my testing and draw my conclusions.

Mr. TIERNEY. Mr. Boback, do you want to add anything to that conversation? I think Mr. Gorton's credibility here is at risk so I want to caution you to that.

Mr. BOBACK. It is clear that we are blocked. We don't spam. We are engaged in Federal, State, and local investigations with law enforcement. The mere fact of his blocking our technology is a direct infringement on our ability to actually prosecute and to work with Federal law enforcement to address these issues. We don't spam. That was clear.

To say that it is automated is not accurate. There is no automated programming. There is no automated system that learns how to program. You can automate updates. You can automate a number of things, but literally someone typed in our IP range. There is no random fitting into your software code. That is hard coded into there, which means someone literally did it. I don't know who that was.

Mr. TIERNEY. Thank you, sir.

Mr. Welch, you are recognized for 5 minutes.

Mr. WELCH. Thank you very much, Mr. Chairman. Mr. Gorton, you were here before and I asked a few questions. You indicated in December 2008 that you were going to engage in a concerted effort to combat and eliminate inadvertent file sharing. Is that right?

Mr. GORTON. Yes.

Mr. WELCH. You saw the results of the test this morning. Apparently using your service we can get information about troop rosters, names, and Social Security numbers in the U.S. Army. Is that anything you approve of?

Mr. GORTON. No.

Mr. WELCH. We can get through your site information about the First Lady's safe house route from the Secret Service. Is that anything you approve of?

Mr. GORTON. Certainly not.

Mr. WELCH. Obviously you don't approve of getting access to confidential information about motorcade routes?

Mr. GORTON. Exactly.

Mr. WELCH. So is it fair to say that whatever it is that you did to "combat and eliminate inadvertent file sharing" was a total, complete, and utter failure?

Mr. GORTON. No, I disagree with that statement.

Mr. WELCH. So however effective it was, it did not successfully stop access to motorcade routes, First Lady safe house information, and troop rosters. That is a fact.

Mr. GORTON. If I may, again, I think——

Mr. WELCH. No, I actually think it is a bit of a joke. The joke may be on us if we don't get a little firmer about this. You have a business model that basically is all about denying intellectual property rights to folks who create music and movies and fostering the sharing of that without any type of respect for the intellectual property rights of people.

It has an over-broad application so that anybody who wants to go on the Web site and get information about Marine One, the First Lady's safe house, or troop rosters can get it. Your routine is to come in here and tell us you are "doing everything [you] possibly can" and profess concern. But your concern doesn't extend to doing that which is effective to stop the problem.

At a certain point reasonable people have to ask the question as to whether the efforts that you are taking are cosmetic, essentially slow walking so that you can maintain the pretext that there is a solution. At a certain point I think we have to ask in Congress whether we are going to take what action is required to protect confidential national security information and intellectual property or not.

Mr. Chairman, if we have another hearing, another hearing, and another hearing after that we are going to have the same story from Mr. Gorton. Then we are going to have another demonstration from Tiversa that shows us whatever he has done lately has failed.

At a certain point it may be appropriate for us to ask folks from the FTC, the U.S. Attorney's Office, and maybe some State Attorneys General who are concerned about access to pornography as to whether there is some legal action that should be taken in order to protect intellectual property, protect our kids from pornography, and essentially protect classified medical and national security information.

I want to thank Tiversa. There is the old Groucho Marx line, do we want to believe Mr. Gorton or our own two eyes? I think your demonstration makes it irrefutable that whatever actions LimeWire has taken to supposedly deal with this inadvertent file sharing are a failure. My conclusion is that they have no serious intention of being successful and stopping it because the main agenda item is providing access to intellectual property to anybody who wants it without any kind of compensation.

I yield back the balance of my time.

Mr. TIERNEY. The gentleman yields back. Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. Gorton, in light of this hard coding question that there isn't time to resolve here, will you agree to answer questions we submit and to provide information as to the people who wrote the software and who would directly know how these IP ranges got in?

Mr. GORTON. Yes, we would be happy to help the committee with that.

Mr. ISSA. I appreciate that.

There was a followup question that I want to understand. I asked earlier and I thought I got an affirmative that you could force users who were using 4.x but wanted access to your switches, that you could create a situation where if they didn't upgrade to the 5 level the new software, I guess it would be 5.2.9, could say it only deals with 5.0 and above or whatever. Then Mr. Foster im-

plied that the open format would deny you that. Could you respond on that and followup?

Mr. GORTON. I guess it is possible for us to come out with a new version of LimeWire that would not connect to other versions. However, with the decentralized network you have a situation where we don't just connect to other LimeWires. We might connect so some other Gnutella compatible program which then itself connected to 4.x. So even if we ourselves deny the connections, the network itself would probably still maintain them.

Mr. ISSA. Following up, I am an old business man so I generally want to figure out where the money goes. That helps me understand the business model. Or you can ask the business model where the money goes. Either way, how do you make your revenue?

Mr. GORTON. We sell LimeWire Pro.

Mr. ISSA. You make it only on the software?

Mr. GORTON. That is correct.

Mr. ISSA. Would you sell more or less software if you better protected your customer, the installer of the product, from inadvertent file sharing?

Mr. GORTON. I suspect we would sell more.

Mr. ISSA. So if, like Peter Norton, the name from the past for us old folks, the DOS 3.3 type people, if you improved your product to have features that would reduce inadvertent file sharing, you would actually sell more product?

Mr. GORTON. That is true. I believe we have done that. I think your conclusion is probably true.

Mr. ISSA. Let me ask you a couple of simple followup questions. Would it be hard to create a browser so that the user can simply, like the search engine or maybe even leveraging the Microsoft and Apple search engines, see what files are presently sharable and unsharable in red and black or whatever? Is there any reason that you couldn't create an easy ability for someone to see the folders that are vulnerable and the files that are vulnerable?

Mr. GORTON. We already have the functionality you are talking about with two different colors. You can click one button to see all the files that you are sharing. We do our best to make it transparent specifically what people are sharing because we want people to be able to check to make sure they are not sharing anything they don't want to share.

Mr. ISSA. Would you be able to build an engine that allowed people to then in mass do a better job of protecting files they want to protect?

Mr. GORTON. I guess I am not really quite sure what you mean by that.

Mr. ISSA. In other words, if I am looking at that, can I quickly click a red file and make it a black file or do the whole subfolder?

Mr. GORTON. That functionality currently exists.

Mr. ISSA. OK. You protect basically DOCs and some of their equivalents, including HTML. Why didn't you include PSTs in that? That is unlikely that output from a Microsoft Outlook file, that is kind of an unusual one to want to share, isn't it?

Mr. GORTON. I am not familiar with that particular file extension. It is possible that there are file extensions in this world that

should be on our documents list which are not currently there. We can add them if there are.

Mr. ISSA. Going back to your model, you would be more popular if you did a better job of protecting your customers, you say. But you have a lot of files that you need to get to looking at and procedures to help protect them. Isn't that right?

Mr. GORTON. We currently do a lot of things to prevent inadvertent file sharing.

Mr. ISSA. Let me ask one question, though. People buy LimeWire in order to be part of a file sharing community. But isn't the primary attraction of LimeWire the fact that there is a tremendous amount of LimeWire-based content out there that they are quickly able to download, including MP3s, MPEGs, and other video and visual files?

Mr. GORTON. People download and install LimeWire primarily to share files. Media files are popular on that list.

Mr. ISSA. Let me ask the final, closing question. If you did a better job, although the individual customer would appreciate it, isn't your model then vulnerable? If you do a good job for me, when I go out to look there is less out there. Without the propagation or the huge amount of interesting content, your product sells worse.

So don't you have an interesting conflict in which it is clear that you should be protecting your customers more but then, if you protect them and they all use the product, what ends up happening is less content is available and therefore the whole category is less desirable? Isn't that essentially your conundrum, that you benefit from a lot of good meaty, juicy shared material and that the failure of your software to protect me has more to do with the fact that you have to create this huge amount of content in order for your whole industry to do well?

Mr. GORTON. I don't think there is a dichotomy the way you phrase it there.

Mr. ISSA. Thank you, Mr. Chairman. I appreciate your indulgence. I yield back.

Mr. TIERNEY. That was the best one question we ever heard.

At this time I want to recognize the chairman, Mr. Towns, for a brief statement. Then I will go to the remaining two people on the panel who have questions. Mr. Towns.

Chairman TOWNS. I have to leave. Let me just say that from what I have heard today, it is clear that private citizens, businesses, and the Government continue to be victims of unintentional and illicit file sharing. At its best, with the proper safeguards in place, peer-to-peer software has great potential. At its worst, it isn't peer-to-peer but predator-to-prey. For our sensitive Government information, the risk is simply too great to ignore.

I am planning to introduce a bill to ban this type of insecure open network peer-to-peer software from all Government and contractor computers and networks. I plan to meet with the new chairman of the Federal Trade Commission to request that the FTC investigate whether inadequate safeguards on file sharing software such as LimeWire constitute an unfair trade practice. The administration should initiate a national campaign to educate consumers about the dangers involved with file sharing software. The FTC needs to look at this, too. The file sharing software industry has

shown that it is unwilling or unable to ensure user safety. It is time to put a referee on the field and to begin to play by rules.

Mr. Chairman, I yield back.

Mr. TIERNEY. Thank you, Mr. Towns.

Ms. Norton, you are recognized for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman. You see that there have been breaches of national security through what is only politely called inadvertent file sharing but the average American, I think, would have been even more concerned about their personal security and especially medical files. I can think of nothing more personal than medical information. I am with the President and people on both sides of the aisle who say that there will be lots of money saved if we could computerize these files so that they could be shared, getting beyond the point of how much that would cost, not to mention making them secure.

Mr. Chairman it probably was in my subcommittee that a number of hearings were held on computerizing the FEHB files, the files for Federal employees. I recall that the unions were basically for it but we always came up with terrible compunctions about the security of these files.

Mr. Boback, in your testimony you apparently spoke of records from a hospital that had been inadvertently shared. This would be every person's nightmare when you talk about inadvertent sharing. They have already seen their personal records, their Social Security, and their financial information get leaked. In the case that you reported, the records contain not only the patients' names but their diagnoses and other sensitive information.

How widespread do you believe the leaking of such information to third parties is from hospitals and medical facilities, Mr. Boback?

Mr. BOBACK. It is extensive. As a matter of fact, that specific file has been out for nearly 16 months now on the peer-to-peer networks and has been taken extensively. It has been downloaded a number of times. So these individuals will be affected for years. In fact, they are not even aware that they are on the list at this point because they have never been told.

Ms. NORTON. That would be my next question. Their files have been breached in the most terrible way. The most sensitive information you have about a person is just out there in the stratosphere. Are patients generally informed that their information has been leaked?

Mr. BOBACK. Forty-one of the 50 States require breach notification.

Ms. NORTON. Forty-one of the 50?

Mr. BOBACK. Forty-one of the 50. At this time there is no national breach notification law. There should be. As patients travel across State lines for medical care, there needs to be a national breach notification law. I believe there was one proposed, H.R. 2221, that gives the FTC some oversight and actually punishment if organizations do not identify these to their consumers. That should pass.

Ms. NORTON. That seems, Mr. Chairman, to be minimally necessary. But let me ask you this: Suppose you do know. You can change your Social Security number maybe. You can take your

credit cards and get new ones. What in the world can you do if information that is true and will forever be true about your medical condition is out there? So now you know it. What do you do?

Mr. BOBACK. At this point there is not much to do. There are credit monitoring and identity theft systems that are trying to work toward protecting medical information, companies like LifeLock. They are trying to put these procedures in place. Are they there yet? No. But identity theft is evolving so rapidly that I will assure you that it is not just a $50 credit card loss or a nuisance to the consumer. It will be very impactful to the consumer and the family in the upcoming years if this is not addressed immediately. This is out of control.

Ms. NORTON. Mr. Chairman, if 41 of the 50 States already understand this, it does seem to me with what you have been able to find at this hearing that we would want to bring forward a bill to make sure that this is done nationally.

I might say that when it comes to the FEHB, our Federal employees here, until there is some such software in place, given our work force, it tends to be an older work force, I do not see how we could take this very important step that everyone knows needs to be taken in computerizing the records of Federal employees.

Thank you, Mr. Chairman.

Mr. TIERNEY. Thank you, Ms. Norton.

Mr. Bilbray, you are recognized for 5 minutes.

Mr. BILBRAY. Thank you, Mr. Chairman.

Mr. Gorton, I think that historically we have basically felt that it is the obligation of the consumer to protect their own files. That is part of the process that historically we have used. Basically, you have to at least move through the system and keep clicking to move those files across.

What I am really concerned about is that history has proven that this is not just a consumer problem. There is the SWIF example where you had 300 people who are illegally in the country being able to access records and use those records for illegal employment. There are people who are able to use this document for other issues that we don't even know about. National security could be one of them.

This issue is going to be addressed now, not just as an individual's privacy issue but as a national security issue. We need to be more proactive in making sure that this data is not out in the stratosphere. Are you ready to be more aggressive with your industry? Are you ready to be proactive working with this Congress at shutting down this opportunity to breach information systems that can be used as a threat to this country?

Mr. GORTON. Absolutely. We worked with this committee in the past and I hope we have the chance to do so going forward.

Mr. BILBRAY. My question to you is if you were going to legislate from the Federal level, and I know this is counter-intuitive for you to think about, but if you were going to legislate, what would you do to address this problem?

Mr. GORTON. I touched on this earlier in my testimony. There are a number of problems where computers can essentially break the law or have these security issues. The unique point of control for every computer is its ISP. From a legislative point of view, that is

really the only practical place you can attack because—let's say you have a child pornographer. If they are identified, as Mr. Boback's software can easily identify in an automated way many, many people very easily, if there were a quick and effective mechanism where his computer quickly routes a message to an ISP, maybe the child pornographer is cutoff the Internet or law enforcement is notified. Again, you have to come up with reasonable procedures.

You have to ask some hard questions like under what circumstances we cut a computer off from the Internet. If he finds a document that has nuclear secrets, is that enough to shut the computer off first and then go do an investigation after? These are hard questions that need to be answered.

In the first wave of regulations surrounding the Internet, I think there was a lot of euphoria with the Internet. There wasn't as clear of an issue of what the negative consequences of some of these amazing technologies are. We have a clear idea now.

Again, in order to do this, you have to deal with the ISPs, which are basically telecom companies. I am sure you are aware, these are politically quite powerful institutions. But I don't think that it is possible for this country to really wrestle these questions to the ground without having the ISPs play a constructive role in that.

Mr. BILBRAY. Look, we were all enamored, too, with computer training and then we placed restrictions on the application of that technology. My question really gets into the fact, and I guess I would close with a challenge to you, that this isn't just about the technology application by certain agencies or certain companies. It is also a national protocol or procedure that tightens up and makes it more proactive to open up your record files. We need a procedure. We need to be looking at having regulations on this.

You don't have to answer this but the challenge to you is not to be obstructionist. Be proactive at saying, "OK, we have this procedure now." We think this, this, this, and this will make it harder or tougher for people to inadvertently transfer files and will basically make them more responsive. It will be less user friendly at opening up the files but will address the problem.

That challenge of balance, if you want this committee and Congress to do the right thing, then you have to be willing to move from a historical position and be proactive. Take the hit to some degree, inconvenience the consumer to some degree, but address the crisis in a manner that is less obtrusive than what we would propose working from the regulatory side.

I yield back, Mr. Chairman.

Mr. TIERNEY. Thank you, Mr. Bilbray.

I thank all of our witnesses for their testimony here today, and for their time and their expertise. We do appreciate it. I am sure the chairman has further intentions to followup on this issue.

The meeting is adjourned.

[Whereupon, at 11:40 a.m., the committee was adjourned.]

[The prepared statement of Hon. Gerald E. Connolly and additional information submitted for the hearing record follow:]

Statement of Congressman Gerald E. Connolly

Committee on Oversight and Government Reform

"Inadvertent File Sharing Over Peer to Peer Networks"

July 29th, 2009

Thank you, Chairman Towns for following up on a previous Oversight hearing on the topic of inadvertent file sharing. Diligence is required to ensure that peer to peer networks do not endanger the privacy of our constituents who may use them without being aware of the risks.

At a previous hearing two years ago, this Committee learned that tax returns, bank records, health records, and military documents were being shared inadvertently over the LimeWire peer to peer network. Unfortunately it seems that LimeWire has not addressed these security deficiencies, and that LimeWire's failure to secure its' users privacy is typical of peer to peer networks.

There are many policy implications of these findings. I hope the Committee is able to focus on a few of these.

First, we must empower our constituents to protect themselves from inadvertent file sharing. One simple step would be to direct the Federal Trade Commission, which currently has no guidance on peer to peer network security, to provide information to consumers about security risks associated with peer to peer networks. This is a particularly important step because normal firewalls and encryption codes do not protect individuals against inadvertent file sharing over peer to peer networks, and because third parties can expose individual's private files even if those individuals have not used peer to peer networks themselves.

Second, we must consider the impacts of peer to peer networks on business incentives. In 2005 the Supreme Court ruled unanimously that peer to peer networks infringe on copyrights by inducing users to share information that may be under copyright, even if the peer to peer network managers are not aware of each specific instance where copyright infringement occurs. We should build upon this decision and identify steps that can provide greater security of intellectual property, because loss of security undermines the incentive to innovate artistically or technologically.

Finally, we must act quickly to reduce exposure of military files to inadvertent file sharing, and work with Federal contractors to ensure that their sensitive files are secure as well. As the recent leak from a Maryland contractor demonstrates, our enemies may be using peer to peer networks to spy on our defense technology.

Thank you again, Chairman Towns for holding this meeting.

EDOLPHUS TOWNS, NEW YORK
CHAIRMAN

PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERRY E. CONNOLLY, VIRGINIA
MIKE QUIGLEY, ILLINOIS
MARCY KAPTUR, OHIO
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
PATRICK J. KENNEDY, RHODE ISLAND
DANNY K. DAVIS, ILLINOIS
CHRIS VAN HOLLEN, MARYLAND
HENRY CUELLAR, TEXAS
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
PETER WELCH, VERMONT
BILL FOSTER, ILLINOIS
JACKIE SPEER, CALIFORNIA
STEVE DRIEHAUS, OHIO

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5051
FACSIMILE (202) 225-4784
MINORITY (202) 225-5074

www.oversight.house.gov

DARRELL E. ISSA, CALIFORNIA
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. MCHENRY, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
JIM JORDAN, OHIO
JEFF FLAKE, ARIZONA
JEFF FORTENBERRY, NEBRASKA
JASON CHAFFETZ, UTAH
AARON SCHOCK, ILLINOIS
BLAINE LUETKEMEYER, MISSOURI

October 1, 2009

Mr. Mark Gorton
Chairman
The Lime Group
37 7 Broadway, 11th Floor
New York, NY 10013

Dear Mr. Gorton:

I am writing to request information related to an issue raised during our Committee's July 29, 2009 hearing entitled, "Inadvertent File Sharing Over Peer-To-Peer Networks: How it Endangers Citizens and Jeopardizes National Security."

During the hearing, Mr. Robert Boback, CEO of Tiversa, Inc., told the Committee that beginning with LimeWire version 5.0, his company's software was blocked from monitoring LimeWire users.

Mr. Boback testified:

> Our own personal concern with LimeWire 5.0 and up is that for some unexplained reason, Tiversa, which is the only oversight to a number of peer-to-peers, was hard coded in a block so that we would be unable to see every user of 5.0 and up … for some reason our entire IP address range that Tiversa uses to monitor has been hard coded, which means someone literally typed into the LimeWire code to not ever connect to anyone associated with Tiversa.

Later, in response to a question from Rep. John Tierney, you suggested that a possible reason for Tiversa being blocked from monitoring LimeWire versions 5.0 and later is that Tiversa was automatically flagged as a spammer, stating the following:

> We have an automated system which goes and looks for spammers. I believe that his [Boback's] company's systems in

> some way have a profile of a spammer and they were inadvertently flagged as a spammer.

Rep. Tierney then engaged you in the following exchange:

> Mr. TIERNEY: So who in your company do you think had that desire and then physically blocked them?
>
> Mr. GORTON: Like I said, it is an automated system.
>
> Mr. TIERNEY: No, no. Let us back up a second. Somebody had to physically go in and block them out. So who in your company is in charge of doing that?
>
> Mr. GORTON: No. Like I was saying, we have an automated system which identifies IP addresses. There is no human being involved.

Mr. Boback from Tiversa, in response, testified:

> It is clear that we are blocked. We don't spam ... To say that it is automated is not accurate... You can automate a number of things, but literally someone typed in our IP range... That is hard coded into there, which means someone literally did it. I don't know who that was.

Finally, there was an exchange between the two of us regarding this issue:

> Mr. ISSA: Mr. Gorton, in light of this hard coding question that there isn't time to resolve here, will you agree to answer questions we submit and to provide information as to the people who wrote the software and who would directly know how these IP ranges got in?
>
> Mr. GORTON: Yes, we would be happy to help the Committee with that.

I remain interested in reaching a resolution of this matter, and appreciate your stated agreement at the hearing to assist the Committee with its understanding of how Tiversa's IP ranges were blocked.

Following the hearing, Tiversa provided my staff with information gathered from LimeWire's own source code, publicly available at http://cvs.limewire.org, and suggested that on April 29, 2008, a LimeWire code author identified as "sberlin" inserted Tiversa's

IP range, 72.22.0.0/19, into the list of "hostile IPs" that were to be blocked.[1] Based on a search of LimeWire's Web site, we are assuming that "sberlin" is the user name for LimeWire Development Director Sam Berlin. In addition, my staff was told by Tiversa that shortly following the July 29 hearing, Tiversa's IP addresses were unblocked.

To help the Committee understand how LimeWire 5.0 and later versions came to block Tiversa's access, please provide the following information by October 16, 2009:

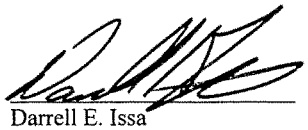
1. The identity of LimeWire code author "sberlin" if someone other than LimeWire Development Director Sam Berlin.

2. An explanation of the actions taken by LimeWire code author "sberlin" on April 29, 2008 that resulted in the inclusion of Tiversa, Inc.'s IP addresses (72.22.0.0/19) in a list of hostile IPs, as well as LimeWire's decision-making process leading to those actions.

3. An explanation of the decision to unblock Tiversa, Inc.'s IP addresses following your participation in the July 29, 2009 Committee hearing on peer-to-peer file sharing.

Thank you for your cooperation in this matter. Should you or your staff have any questions with regard to this request, you may contact Mark Marin or Steve Castor of the Committee staff at (202) 225-5074.

Sincerely,



Darrell E. Issa
Ranking Member

cc: The Honorable Edolphus Towns, Chairman

[1] *See* https://www.limewire.org/fisheye/browse/~author=sberlin/limecvs/components/gnutella-core/src/main/java/com/limegroup/gnutella/simpp/SimppDataProviderImpl.java?r=1.1.

Lime Wire LLC
45 HOWARD · NEW YORK, NY 10013 · TEL: 212.775.3000 · FAX: 212.775.3001

October 14, 2009

Delivered via UPS

Ranking Member Darrell Issa
Congress of the United States
House of Representatives
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Ranking Member Issa:

I write in response to your letter of October 1, 2009 requesting information related to an issue raised during the Committee's July 29, 2009 hearing regarding inadvertent file-sharing. Thank you for giving me the opportunity to be of assistance to the Committee. And, thank you as well for taking advantage of the benefits of open-source software and LimeWire's publically accessible source code and change log. I hope it is proving helpful to the Committee's investigations.

In response to the questions raised in your letter, I offer the following:

1. "sberlin" is Lime Wire LLC Development Director /Client Team Lead, Sam Berlin.

2. To be clear, to the best of its knowledge, Lime Wire has never knowingly treated Tiversa, Inc.'s ("Tiversa") IP address as a "hostile IP" or intentionally included an IP address in any list of hostile IPs because it was Tiversa's IP address.

For background, Lime Wire's standard practice for the distribution of hostile IPs is to distribute them to a LimeWire Gnutella client(s), which client(s) then further distribute the hostile IPs to other LimeWire Gnutella clients. For a period of time beginning on or about April 16, 2008 until August 17, 2008, Lime Wire was restricted in its ability to transmit the hostile IP list to the LimeWire Gnutella clients using its standard practice. To maintain the safety and security of LimeWire users during this time, in lieu of Lime Wire transmitting the hostile IPs to other LimeWire Gnutella clients, on April 16, 2008 Mr. Berlin copied the approximately *22 million* hostile IPs that were distributed to LimeWire version 4.16.6 Gnutella clients (including 72.22.0.0/19) and placed them into the LimeWire version 4.16.7 code as default hostile IPs.

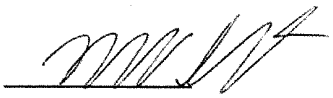
Tiversa's suggestion that Lime Wire intentionally inserted Tiversa's IP address into the LimeWire source code on April 29, 2008 is incorrect.[i]

As of July 14, 2009, the determination and transmission of new hostile IPs is fully automated. IP addresses previously determined to be hostile IPs before the implementation of the automated system are currently under review.

3. There has been no decision within Lime Wire following the July 29, 2009 hearing and concerning the IP address 72.22.0.0/19. According to Lime Wire's records, the IP address 72.22.0.0/19 continues to be blocked.

I thank you again for the opportunity to assist you in this matter. I welcome the opportunity to be of further assistance should you or your staff have any further questions.

Sincerely,



Mark Gorton
Lime Wire LLC

Cc: *The Honorable Edolphus Towns, Chairman*

---

[i] To view the changeset that shows the changes to the LimeWire software code made by Mr. Berlin on April 16, 2008, See https://www.limewire.org/fisheye/changelog/limecvs?cs=MAIN:sberlin:20080416222646.

To view the specific change within the April 16, 2008 changeset that shows Mr. Berlin's addition of the default hostile IP list into the LimeWire software code, See https://www.limewire.org/fisheye/browse/limecvs/components/gnutella-core/src/main/java/com/limegroup/gnutella/simpp/SimppManager.java?r1=1.26&r2=1.27

To view the routine code maintenance that relocated the default hostile IP list code within the LimeWire software from "SimppManager.java" to "SimppManagerImpl.java" on April 28, 2009, See https://www.limewire.org/fisheye/changelog/limecvs?cs=MAIN:sberlin:20080428214048

To view the routine code maintenance that relocated the default hostile IP list code within the LimeWire software from "SimppManagerImpl.java" to "SimppDataProviderImpl.java"on April 29, 2009, See https://www.limewire.org/fisheye/changelog/limecvs?cs=MAIN:sberlin:20080429190007