



Wednesday July 29, 2009

The Honorable Eric H. Holder, Jr., Attorney General, U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

RE: Committee on Oversight and Government Reform hearings into “Inadvertent File Sharing over Peer-to-Peer Networks”

Dear Attorney General Holder,

My name is Bernard Trest and I am the president of ZapShares, a company that offers identity theft and lawsuit protection for Peer-to-Peer (also known as “P2P”) file-sharing software, and also conducts research regarding file-sharing networks and software such as LimeWire. We have been working with members of the Congressional Committee on Oversight and Government Reform, most notably Mr. Steven Rangel, which is conducting hearings into “Inadvertent File-Sharing on Peer-to-Peer Networks.”

I am writing this letter to you concerning the issues we have been addressing with the members of the Committee including file-sharing software, matters of urgent national security involving national defense contractors and countries such as Iran and North Korea, rampant identity theft that continues to occur, the widespread and unrelenting illegal sharing of copyrighted materials, and the continued spread of repulsive child pornography. As discussed during my conference call on June 11, 2009 with members of the Committee, I also want to address with you the blatant lies that were told to Congress by Mr. Mark Gorton, Chairman of Lime Group LLC. which is the maker of the LimeWire file-sharing software, during his testimony to Congress on July 24, 2007, and in his subsequent letter to Congress dated May 1, 2009.

Even though the Committee recently held new hearings regarding the inadvertent file-sharing that occurs over Peer-to-Peer Networks, we wanted to bring this matter directly to your attention as well since we feel that this issue requires further investigation on a much greater scale. We had intended to bring this matter to your attention via a letter we composed to you on Wednesday June 10, 2009; however, by request of the Committee members we postponed sending the original letter to you. Please find copies of the letter we submitted on June 25, 2009 to the Committee attached to this letter. Additionally, we also electronically submitted over 150 pages of evidence pertaining to this matter. For your convenience, we have compiled the evidence we submitted to the Committee into a single PDF document which can be viewed online at www.zapshares.com/ZapShares-Evidence.pdf



As with H.R. 1319, the Informed P2P User Act, we feel that the proposed new bill to ban P2P software from all government and contractor computers and networks will do very little to alleviate the issues with P2P file-sharing software. In many cases P2P file-sharing software is installed by a spouse or child living in a household, and in many cases people are even unaware that someone in the household has installed P2P software on the household computer. In the case of government contractors, which have been the source of previously leaked classified information, the contractors usually bring their work laptops home, at which point a child or spouse in the household installs a P2P file-sharing client and the leaks of classified information occur.

Our company recently conducted research into the national security threat posed by file-sharing software and found that computer systems located in Iran, North Korea, China, and Russia are scouring P2P file-sharing networks for classified information that could place national security at risk. During the course of our research, we found offshore computers searching for, among other things, information pertaining to many principal United States defense contractors, weapons system information, classified government documents, information that could be used to steal the identity of United States citizens, and other data that could place national security at risk. What we found most alarming was the fact that a majority of these searches originated from Iran, North Korea, China, and Russia.

We found hundreds of search terms that could potentially jeopardize national security including:

“lockheed” – Which is a search for Lockheed Martin, the largest defense contractor, responsible for technology such as the Trident missile and F-22 Raptor.

“northcom” – Which is a search for the United States Northern Command, the unified combatant command of the United States Military.

“intelsat” – Which is a search for the world’s largest commercial satellite communications services provider.

Even though there have been reports indicating that data related to the President’s helicopter, Marine One, was leaked to Iran due to P2P file-sharing software, based on our research findings we are certain that other classified information that could place national security at risk has been leaked to countries such as Iran, North Korea, China, and Russia; however the United States government and the general public are simply unaware of other classified information that has been leaked.



The P2P identity theft research we conducted found that many people continue to inadvertently share, among other things, personal tax returns, banking and other financial information, credit card information, and other data that identity thieves could use to steal a person's identity. In fact, the abundant availability of private information on P2P file-sharing networks has now led to identity thieves using tools that automatically scan these networks for private data that can be used for the purposes of identity theft and other malicious purposes. We found identity thieves using these automated scanning tools to troll file-sharing networks for thousands of promising search terms such as "credit," "tax," "password," "bank," and the names of many prominent financial institutions, insurance companies, health care providers, and so forth.

In July 2008 we notified Mr. George Searle, the Chief Executive Officer of LimeWire LLC, via e-mail about our preliminary research findings indicating that identity thieves were now using automated software to scan P2P file-sharing networks for information that could be used for the purpose of identity theft. We informed Mr. Searle that the file-sharing network Gnutella, which is the network that LimeWire connects to, was being inundated with search requests for terms such as "credit card," "password," and so forth. In our e-mail to Mr. Searle we expressed our great concern regarding this matter since LimeWire has tens of millions of users and the potential for widespread identity theft due to this new development was very high. In fact, we told Mr. Searle our assumption that possibly thousands, if not tens of thousands, of users of their LimeWire software may have already been affected and could have already had their credit card numbers, credit reports, and other personal information already stolen due to the use of the LimeWire software. I had a subsequent telephone conversation with Mr. Searle regarding our findings and the e-mail which we sent to him and during our conversation Mr. Searle did not express any concern for the situation.

The Denver District Attorney has already prosecuted two cases involving identity theft that occurred due to people's use of P2P file-sharing software. The United States Department of Justice has prosecuted in the United States District Court in Seattle, Washington, two additional cases involving identity theft that were committed due to the use of file-sharing software. Police in the latter case found that the suspect had in his possession private information such as tax returns and bank statements for more than 120 people across the United States from more than a half dozen states. As in the Denver cases the identities of the victims were stolen due to private information that the victims had inadvertently made available through file-sharing software.

Our company is quite certain that there are potentially thousands or tens of thousands of victims that have had their identity stolen due to the victims' use of file-sharing software.



The key issue with identity theft is that the underlying cause as to what led to the theft of one's identity, financial information, and so forth is quite hard to determine. As such, a majority of victims who have had their identity stolen due to the victim's use of file-sharing software will remain unaware that the use of file-sharing software is what led to the identity theft.

We realize that Congress has placed particular attention on LimeWire software as being the main culprit for cases of P2P identity theft and threats to national security. However, our research indicates that LimeWire LLC is by no means the only company that should be focused on during the course of the Congressional investigation. In fact, contrary to Mr. Gorton's claim, LimeWire is by no means the most popular file-sharing software and has continued to lose market share to software such as Ares. For example, on one popular website where you can download LimeWire, the total number of downloads that all versions of the software have received to date is one hundred and eighty million downloads (183,255,946), whereas Ares on one popular website where you can download Ares has received a total of nearly one hundred and ninety five million downloads (196,456,226).

LimeWire connects to the Gnutella Internet file-sharing network, only one of over a dozen different file-sharing networks that presently exist. Additionally, there are currently well over a hundred software programs similar to LimeWire that connect to either one particular file-sharing network, such as the same network that LimeWire connects to which is the Gnutella network, or have the ability to connect to multiple file-sharing networks at once. During the course of our research we studied dozens of different file-sharing software programs that connect to the various Internet file-sharing networks and found that LimeWire is by no means the only software program and Gnutella is not the only file-sharing network that poses threats to national security and can lead to identity theft.

Please find copies of our press releases and research studies regarding the national security threat and identity theft issues posed by file-sharing software on our website, which can be viewed at www.zapshares.com Our published research findings only show a partial list of the thousands of search terms we found that could place national security at risk and also lead to identity theft. Also please note that searches conducted are in many cases partial match searches. For example, when we found searches for the word "tax" then that would match a file on anyone's computer that had the word "tax" in the name, so anyone having files names such as "taxes," "tax return," and so forth would be considered a match and returned as the person having such a file. As another example, the search term "Lockheed" would yield matches to any file with the name "Lockheed," "Lockheed Martin," and so forth.



On June 16, 2009 we sent a letter to Mr. Steven Rangel of the Committee staff informing him that we found a PDF copy of the NATOPS Flight Manual for the McDonnell Douglas Boeing FA-18E/F fighter aircraft located on P2P file-sharing networks. The document was published in March 2001 and issued by “Authority of Chief of Naval Operations and under the direction of the Commander Naval Air Systems Command.” We feel that the availability of such information on file-sharing networks poses a threat to national security, especially when individuals in foreign countries can gain access to this information. We found the file on the eDonkey P2P file-sharing network and the file can be accessed by anyone that has file-sharing software such as eMule installed on their computer.

We have also found very lengthy operating manuals for the Boeing 777, 767, 747, and 737, along with sections of a Continental Airlines flight manual providing 281 pages containing, among other information, detailed preflight instructions. We also found design specifications and standards information for parts used in Boeing and Bombardier aircraft that appears to be strictly for internal company use.

I also wanted to address the issue that Mr. Mark Gorton, chairman of Lime Group LLC, has constantly lied to Congress and perjured himself on numerous occasions. Mr. Gorton has repeatedly stated throughout his previous testimony and his more recent letters to Congress that LimeWire LLC, “does not host, control or have means to monitor user transactions on any peer-to-peer network,” and further claimed, “It is not possible for LimeWire to monitor user activity.” Any such statements made by Mr. Gorton were a blatant lie and Mr. Gorton has clearly perjured himself before Congress numerous times.

LimeWire LLC has indeed been monitoring and controlling file-sharing network activity conducted over the Gnutella network since at least **May 24, 2007**, which is two months prior to Mr. Gorton’s original testimony to Congress on July 24, 2007. In fact, LimeWire LLC has devoted significant resources towards the monitoring and controlling access to the Gnutella file-sharing network and controlling specific content that is shared over the Gnutella network using the LimeWire software. Mr. Gorton and Mr. Searle however are more concerned and have focused their attention on controlling anti-piracy and advertising efforts of companies on the Gnutella network rather than focusing on controlling the widespread use of the Gnutella network and LimeWire for the rampant illegal distribution of copyrighted materials, and the distribution of child pornography.

During our previously mentioned telephone conversation with Mr. Searle, at one point we discussed LimeWire LLC’s monitoring of the Gnutella network and LimeWire LLC’s blocking of anti-piracy and advertising efforts of any companies other than LimeWire



LLC. Mr. Searle admitted that the blocking technology employed by LimeWire was not perfect, but informed me that LimeWire LLC was indeed monitoring the Gnutella network and blocking the efforts of companies that were engaged in anti-piracy and advertising on the Gnutella network.

There are several companies that have attempted to distribute advertising on the Gnutella network, as well as anti-piracy organizations that have attempted to prevent piracy by distributing fake files that appear to be copyrighted materials. The distribution of these types of files has very quickly been blocked by LimeWire LLC, usually within 24 hours. Since May 24, 2007 LimeWire LLC could have employed the same monitoring technique and blocking technology to block LimeWire user's who are distributing copyrighted materials, child pornography, and other illegal content, however LimeWire LLC has chosen to allow these user's the opportunity to continue their illegal activities.

Every time the LimeWire software is run the software searches the network for a hidden system file created by LimeWire LLC named "simpp.xml," and then downloads the file into memory and onto the LimeWire user's hard drive. Even though the simpp.xml file is distributed across the file-sharing network, the file originates and is updated by LimeWire LLC, by a person employed at LimeWire Inc, and then passed down from LimeWire LLC servers across the file-sharing network to other LimeWire software clients. The simpp.xml file is created by LimeWire LLC and is locked by LimeWire LLC using a digital signing algorithm so only LimeWire LLC has the ability to create and modify the simpp.xml file.

The simpp.xml file contains various software settings that LimeWire LLC has the ability to change remotely. Also within the simpp.xml file and very contrary to Mr. Gorton's testimony and letters to Congress, the simpp.xml file provides LimeWire LLC with a network level filter, which provides LimeWire LLC the ability to block specific computer IP addresses, or range of computer IP addresses, from making files available to users running LimeWire software. The filter is referred to by LimeWire LLC as a "hostile host" filter and contrary to Mr. Gorton's testimony, LimeWire LLC modifies this filter manually. This filter provides LimeWire LLC with the ability to block any computer from making available files to other users of the Gnutella network. LimeWire LLC has the ability to update this filter at any time, and has been aggressive at using this filter to keep advertising and fake files being distributed by anti-piracy companies off the Gnutella network. However, despite the fact that this filter could be easily used to keep illegal materials off the Gnutella network, LimeWire LLC has chosen not to do so.

In the evidence we presented to the Committee we provided them with copies of an Internet discussion forum located on the LimeWire LLC website in which a user asks,



“What is simpp.xml?” In response to the question Sam Berlin, who is the Software Development Director at LimeWire LLC, and Aaron Walkhouse, who is a LimeWire Internet discussion forum moderator, discuss in great detail the function of the simpp.xml file and the “hostile host” filter. You can find the Internet discussion forum concerning the simpp.xml file at

<http://forum.limewire.org/showthread.php?t=2733&highlight=simpp.xml>

In the discussion forum, Mr. Berlin and Mr. Walkhouse discuss that LimeWire LLC has been monitoring and blocking the IP addresses of users on the Gnutella network who they consider to be “bandwidth wasters”, which again include companies that are engaged in advertising and anti-piracy efforts on the Gnutella network. Additionally, Mr. Berlin and Mr. Walkhouse discuss how the simpp.xml file is automatically distributed to all LimeWire users by LimeWire LLC and automatically used by the LimeWire software, and that the simpp.xml file cannot be modified by anyone other than LimeWire LLC.

As Mr. Gorton mentioned in his letter to Congress on May 1, 2009, the LimeWire software also has a “Copyrighted Content Filter,” which when enabled by a LimeWire user prohibits the user from downloading files that match digital signatures of files that copyright holders have requested be removed from the LimeWire software. The content filter was implemented in V4.11.0 of the LimeWire software, which was released on March 10, 2006. LimeWire does not automatically enable the content filter by default, and a user must go through several option screens in order to find and enable the content filter. Since March 10, 2006 LimeWire LLC could have automatically mandated the use of the Copyrighted Content Filter and not allowed LimeWire users to download any copyrighted materials, however LimeWire LLC has chosen to ignore Congress, the law, the FTC, the media industry, and many other organizations that are concerned and affected by the rampant illegal distribution of copyrighted materials over P2P file-sharing networks.

Since November of 2008, LimeWire LLC has also added into the LimeWire software and into the simpp.xml file the automatic blocking of specific files identified by their digital signatures. The automatic blocking of digital signatures works similarly to the Copyrighted Content Filter, however this new filter is enabled by default and cannot be turned off by LimeWire users. Using this filter, LimeWire has had the ability since November of 2008 to stop users from downloading copyrighted materials, since this filter can be used to stop any file from being transferred over the Gnutella network. Once again, instead of using this filter to remove copyrighted materials from the Gnutella network, LimeWire LLC has used the filter solely to remove advertising and fake files distributed by anti-piracy companies from the network.



Mr. Gorton has also attempted to deceive Congress in regards to LimeWire's claimed efforts to curb the rampant national security threat that is posed by the LimeWire software, and the rampant identity theft that continues to occur due to file-sharing software. In the letter Mr. Gorton sent to Congress on May 1, 2009 and in his testimony on July 29, 2009 he stated, "In light of and in lieu of that, Lime Wire does all it can to encourages all users to upgrade to LimeWire 5 as the most effective means of file-sharing while still safeguarding private data. At present, despite having been released only months ago, nearly 50% of LimeWire users have upgraded to LimeWire 5." We strongly dispute Mr. Gorton's claim that 50% of LimeWire users have upgraded to the latest version of the LimeWire software, especially considering that LimeWire LLC has **encouraged** people to either continue using an older version of the LimeWire software or to downgrade to an older version of the software. In fact, LimeWire LLC still makes older versions of the LimeWire software available on their website.

Since the release of V5 of the LimeWire software there have been countless complaints made by the software's users concerning the lack of usability and functionality of the new version. In fact, the LimeWire LLC website has an Internet forum with discussions concerning the LimeWire software, and within the discussion forums there are many topics with subject names such as: "Limewire 5 sucks," and "Please enter my vote for Limewire 5 SUCKS!." Some of the discussion topics have over twenty pages of negative comments concerning the new version of the LimeWire software, and many people have stated that they have reverted back to an older version of the LimeWire software. In response to complaints regarding V5 of the LimeWire software, LimeWire discussion forum moderators have directed people to download and install older versions of the LimeWire software, and one moderator even commented, "LimeWire 4 will be supported for a long time to come. No worries there." Even though Mr. Gorton claimed to Congress that his company is directing all users to V5 of the LimeWire software, the truth is that in many cases LimeWire LLC has encouraged people to continue using older versions of the LimeWire software, or has suggested to people that they downgrade from their upgraded V5 of the LimeWire software to an older version.

Mr. Gorton also continues to downplay the severe national security threat and identity theft that continues to occur due to LimeWire software and other similar file-sharing software. In Mr. Gorton's recent letter to Congress he stated "In short, there is absolutely no way to access a LimeWire 5 user's documents unless that user affirmatively elects to make them available." What Mr. Gorton failed to mention and address is the fact that the LimeWire software by default still automatically starts when a user turns on their computer. The LimeWire software settings, and in fact the settings of any file-sharing software, can also easily be compromised by a virus or trojan, especially considering that



there is no way for anti-virus software to know what program settings a user truly intends for file-sharing software that is installed on the user's computer.

Mr. Gorton also failed to mention that viruses and trojans are still embedded in files disguised as audio or video files, which LimeWire does **not** block by default, allows users to download, and in fact by default automatically shares these files with other users of the file-sharing network. Once the settings of LimeWire or other file-sharing software have been compromised, uninhibited access to a user's entire hard drive can be achieved, which can place national security at risk and lead to issues such as identity theft. Our research indicates that the new version of the LimeWire software has in fact done little to curb the spreading of viruses and trojans through file-sharing networks.

I would like to thank you for taking the time to read this letter and address the issue of inadvertent file-sharing and Mr. Gorton's perjured testimony before Congress. If I can be of any further assistance to you or to the members of the Committee examining these issues then please contact me at (416) 897-5194, or via email at btrest@zapshares.com

Yours Very Truly,

A handwritten signature in black ink, appearing to read 'BTrest'.

Bernard Trest
President
ZapShares
www.zapshares.com

Bernard Trest

From: Bernard Trest [btrest@zapshares.com]
Sent: Thursday, June 25, 2009 12:46 AM
To: ' [REDACTED]@mail.house.gov'
Cc: ' [REDACTED]@mail.house.gov'
Subject: Evidence re: Inadvertent File Sharing on Peer-to-Peer Networks

Mr. Rangel,

We have completed gathering and documenting the evidence that you had requested in regards to the Congressional hearings into the "Inadvertent File Sharing on Peer-to-Peer Networks." The evidence is contained within eleven PDF documents and encompasses a total of 164 pages. Since the combined file size of the documents was quite large, we have Zipped (compressed) all of the files and placed them on our server for you to download. The Zipped documents can be downloaded at:

www.zapshares.com/ZapShares-Bernard Trest-Evidence.zip

The evidence we are presenting to you in this matter is as follows:

- 1) Detailed information pertaining as to how the simpp.xml file functions. As mentioned, LimeWire LLC has been monitoring and controlling content that appears on the Gnutella network since May 24, 2007. This evidence clearly supports the fact that Mr. Mark Gorton, Chairman of LimeGroup LLC, has perjured himself before Congress on numerous occasions. We have documented the "hostile host" filter, the URN filter, and the Copyrighted Content Filter. Any or all of the latter mentioned filters could have been used to remove copyrighted materials from the Gnutella network, greatly reduce the amount of child pornography, and also filter files that could pose national security and identity theft risks.
- 2) Copies of Internet discussion forums in which LimeWire users discuss their dissatisfaction with LimeWire V5 and mention that they have in fact reverted to an older version of the LimeWire software. In nearly all of these cases employees of LimeWire LLC, including several LimeWire LLC developers and Internet discussion forum moderators, have directed LimeWire users to download and install older versions of the LimeWire software.
- 3) Web pages indicating that older versions of the LimeWire software are still available on the LimeWire LLC website. Additionally, LimeWire LLC provides clearly detailed instructions regarding how to access and download the older versions of the LimeWire software.
- 4) Copies of our e-mail communication with Mr. George Searle, the Chief Executive Officer of LimeWire LLC. In this e-mails and during my telephone conversations with Mr. Searle, I discussed with him the fact that LimeWire LLC has been monitoring and blocking the efforts of companies that attempt to conduct anti-piracy and advertising efforts on the Gnutella network. Please note that due to the fact that large parts of the e-mail communications contain information pertaining to business plans and other private company information, we have only included relevant sections from our e-mails to Mr. Searle. The sections themselves were not modified in any way other than the blanking and/or removal of large sections of the original e-mails.
- 5) Copies of Internet discussion forums in which users voice their outrage at the availability of child pornography.

6) Software screenshot captures showing the still abundant availability of private information that could lead to identity theft or pose a risk to national security, the continuing problem of copyrighted materials which still plagues the Gnutella network, and also the continued availability of child pornography. Please note that we use proprietary software for most of our research so for competitive reasons we cannot provide you with screenshots of the internal software that we use.

Please keep in mind that due to the way in which regular P2P file-sharing software functions, regular P2P software is designed to stop a particular search after either a few hundred results are returned, or after a very short specific period of time. An identity thief using regular P2P software can find a few hundred tax returns within 20 seconds, restart the P2P software, conduct the same search, and find another set of a few hundred different tax returns than had been found in the prior search. Within a few minutes an identity thief can gain access to thousands of tax returns and other private information, all without any custom software.

Even though our research has shown that identity thieves are now using propriety automated software to scan P2P networks for personal information, an identity thief does not even necessarily require any special software in order to access personal information. The difference between conducting a search for tax records through LimeWire or through proprietary software is that the custom software would be designed to connect to larger parts of file-sharing networks, so proprietary software conducts a more comprehensive scan for shared files in a shorter period of time.

7) Detailed statistics and software screenshot captures from other file-sharing software showing that other file-sharing software and other file-sharing networks pose the same risk as the LimeWire software in regards to identity theft, risks to national security, the sharing of copyrighted materials, and the availability of child pornography. As mentioned during our conference call, our research clearly indicates that other file-sharing software and other file-sharing networks, which in some cases are even more popular than the LimeWire software and the Gnutella network, are plagued with similar concerns as those expressed in regards to the LimeWire software.

8) Copies of our press releases and studies.

9) Copy of the letter that we intended to send to Congressman Edolphus Towns, Congressman Darrell Issa, Congressman Peter Welch, Congresswoman Mary Bono Mack, The Honorable Attorney General Eric H. Holder, Jr., and also The Honorable FTC Chairman Jon Leibowitz. Please note that this letter contains additional information, evidence, and details that can be used during the course of the hearings into this matter.

Please keep me apprised in regards to the hearings into this matter.

Thank you again.

Yours Very Truly,
Bernard Trest
President
ZapShares
www.zapshares.com