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 29, 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.