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.