

# The Washington Times

Article published Jul 25, 2007

## Internet sharing exposes secrets

July 25, 2007

By Adam Terese - Hundreds of classified documents, including a Pentagon computer network diagram that contained system passwords of defense contractors, have been accidentally leaked on the Internet through peer-to-peer software, lawmakers were told yesterday.

Users of peer-to-peer services such as Kazaa, LimeWire and Morpheus are unknowingly allowing this and other private information, such as bank statements and Social Security numbers, to be shared through the software, experts said at a House Oversight and Government Reform hearing. Peer-to-peer networks can be used to share music, movie and other files.

"It is an urgent problem. We don't know what is already out there," said retired Gen. Wesley Clark, chairman and chief executive of the consulting firm Wesley K. Clark & Associates. Mr. Clark spent 34 years in the U.S. Army and the Department of Defense.

The hearing yesterday was not intended to shut down peer-to-peer networks but rather to examine their threats to national and personal security, said committee Chairman Henry A. Waxman, California Democrat.

The networks get more than 300 million searches each day from users in the U.S. and abroad, while Google gets 130 million, said Robert Boback, chief executive officer of Tiversa Inc., a data security company.

Mr. Boback estimated that MP3 music files make up 38 percent of files found on the networks, while MPEG movie files make up 19 percent.

But some users are deliberately searching for bank statements and credit-card numbers, as well as medical records.

"We are in a wall-less society," he said.

Government and corporate documents can be accessed if they are on the network because certain features of peer-to-peer software have a tendency to cause inadvertent file sharing. One of those allows users to choose a folder to store downloaded files, but it does not warn the users that subfolders also will be shared.

That means someone can work at home and, unaware that a peer-to-peer program is installed, save a file to a shared folder.

In 2003, the House committee's hearings on similar issues resulted in a conduct code for the peer-to-peer industry to help eliminate features in the programs that lead to the accidental sharing.

But in March, the U.S. Patent and Trademark Office released a report suggesting inadvertent file sharing is still a problem. Thomas Sydnor, an attorney for the PTO, said distributors of five peer-to-peer programs continued to include features in their programs that can cause users to

accidentally share sensitive information.

Mark Gorton, chief executive officer of the Lime Group, maker of LimeWire, said he does not know how much classified information is available through LimeWire's network. To protect users from inadvertent sharing, he said warning messages pop up when users try to share folders that may contain sensitive information.

"Clearly, the warnings are not enough," he said. "LimeWire has always tried to make the program clear and easy for users."

The leaked information also is likely to spread since the file name may be associated with other common search terms, said M. Eric Johnson, director of the Center for Digital Strategies at Dartmouth University's Tuck School for Business.

For instance, a search for a music file from rapper PNC may bring up documents for PNC Bank if they are on the network.

"Such digital wind increases the P2P security threat for many organizations," he said.

However, Mary Engle, associate director for advertising practices for the Federal Trade Commission, said the FTC staff found peer-to-peer file-sharing to be a "neutral" technology.

"Its risks result largely from how individuals use the technology rather than being inherent in the technology itself," she said.