



# First lady's safe house location leaked on P2P

[Angela Moscaritolo](#)

July 29 2009

A recent high-profile breach that illustrates the continuing risk of peer-to-peer (P2P) file sharing programs has exposed a document revealing the location of the first lady's safe house.

The persistent vulnerabilities of P2P networks and the document were topics of discussion during a hearing Wednesday before the U.S. House of Representatives Committee on Oversight and Government Reform. The U.S. Secret Service document, which was leaked on a P2P network, detailed the route to transport the first lady when and if the White House needs to be evacuated, according to Robert Boback, chief executive officer at P2P monitoring vendor Tiversa, who spoke at the hearing which was organized to review national security, consumer identity theft and corporate data leakage risks posed by P2P networks.

P2P networks are commonly used for music sharing, but users often do not realize that once a P2P network is downloaded, it opens up all the contents of a user's hard drive to others, Boback said. The issue of inadvertent file sharing on P2P networks was first brought up to the Committee on Oversight and Government Reform nine years ago, Chairman Edolphus Towns (D-NY) said in his opening remarks Wednesday. Two years ago, file-sharing vendors agreed to self-regulate and address the problem of inadvertent file sharing, but their efforts have failed, Towns added.

"As far as I am concerned, the days of self-regulation should be over for the file-sharing industry," Towns said.

Another document recently found on P2P networks provides the location of every nuclear facility in the U.S., Boback said. The document, dated July 5, 2009, and labeled highly confidential, has President Obama's signature on its cover page.

"Clearly there is a problem," Boback said. "A number of government agencies are exposing information."

And from an identity theft perspective, the losses of personal information on P2P networks are staggering, Boback said. A U.S. military roster containing the Social Security numbers and other personal information of hundreds of thousands of troops was found. Another document containing approximately 20,000 patients'

health care records -- including names, addresses, phone numbers and Social Security numbers -- was also found. All of these documents were discovered within the past few months and many of them still can be found on P2P networks, Boback said.

"Why would you ever dive in a dumpster?" Boback asked.

In addition, Boback provided examples of tax returns from individuals in New York, Arizona, Vermont and Maryland located on P2P networks, but said he could have provided thousands more representing every state. In an example to illustrate exposures of corporations' confidential data, Boback called out a file that was found containing the email archive of a mergers and acquisitions executive at a major, publicly traded company. Ironically, another document available on a P2P network outlined a company's IT policy about how P2P networks were not allowed, Boback said.

At the hearing, Mark Gorton, creator of LimeWire, a popular P2P software company, came under fire for failing to protect users from inadvertent exposure of sensitive documents. Gorton admitted that LimeWire is "not perfect," but said the newest version (5.0) no longer inadvertently share files.

"The LimeWire team has put a huge amount of time to eliminating this problem," Gorton said. "The current version doesn't share any documents by default."

Gorton further explained that LimeWire, as just one file-sharing program out of hundreds, is trying to set an example for others to follow so that the data exposure issue is rectified. But, Chairman Towns said that he heard similar statements from Gorton two years ago, and the problem still persists.

Thomas Sydnor II, senior fellow and director at the Center for the Study of Digital Property at the Progress & Freedom Foundation, who was a witness at the hearing, said that over the past two years LimeWire has put additional security measures in place. He said, however, that the problem is not completely fixed, adding that the current version of the software is "dangerously unpredictable."

"It is clearly not fixed entirely in the most current version," Boback agreed.