c|net NEWS.COM http://www.news.com/

Congress: P2P networks harm national security

By Anne Broache
http://news.com.com/Congress+P2P+networks+harm+national+security/2100-1029_3-6198585.html

Story last modified Tue Jul 24 16:22:23 PDT 2007

WASHINGTON--Politicians charged on Tuesday that peer-to-peer networks can pose a "national security threat" because they enable federal employees to share sensitive or classified documents accidentally from their computers.

At a hearing on the topic, Government Reform Committee Chairman Henry Waxman (D-Calif.) said, without offering details, that he is considering new laws aimed at addressing the problem. He said he was troubled by the possibility that foreign governments, terrorists or organized crime could gain access to documents that reveal national secrets.

Also at the hearing, Mark Gorton, the chairman of Lime Wire, which makes the peer-to-peer software LimeWire, was assailed for allegedly harming national security through offering his product.

The documents at risk of exposure supposedly include classified government military orders, confidential corporate-accounting documents, localized terrorist threat assessments, as well as personal information such as federal workers' credit card numbers, bank statements, tax returns and medical records, according to recent studies by the U.S. House of Representatives Committee on Oversight and Government Reform, the U.S. Patent and Trademark Office, and private researchers.

Evidence that sensitive information is accessible through peer-to-peer networks illustrates "the importance of strengthening the laws and rules protecting personal information held by federal agencies" and other organizations, said Rep. Tom Davis (R-Va.), the committee's ranking member, who has sponsored a bill that would impose new requirements on government agencies that discover security breaches. "We need to do this quickly."

The politicians present Tuesday generally said they believe that there are benefits to peer-to-peer technology but that it will imperil national security, intrude on personal privacy and violate copyright law, if not properly restricted. Both Waxman and Rep. Paul Hodes (D-N.H.) dubbed P2P networks ongoing national security threats.

Congressional gripes about P2P networks are hardly new, and in the past, they have reinforced concerns raised by the Motion Picture Association of America and the Recording Industry Association of America. Four years ago, the same committee held a pair of hearings that condemned pornography sharing on P2P networks and also explored leaks of sensitive information. And throughout 2004, Congress considered multiple proposals that would have restricted--or effectively banned--many popular file-swapping networks. Waxman noted that he was not seeking to ban peer-to-peer networks this time around but rather to "achieve a balance that protects sensitive government, personal and corporate information and copyright laws."

To be sure, the kind of information leaks that alarmed politicians at Tuesday's hearing are most likely already against the law or federal policy. It is illegal for government employees to leak certain types of classified documents without approval, either electronically or through traditional paper means.

Mary Koelbel Engle, the associate director for advertising practices in the Federal Trade Commission's Bureau of Consumer Protection, said her agency has found in its studies of peer-to-peer network use that risks to sensitive information "stem largely from how individuals use the technology rather than being inherent in the technology itself."

Some politicians nonetheless lashed out at the sole representative from a peer-to-peer software company at Tuesday's hearing: Lime Wire's Gorton, who is also CEO of parent company Lime Group.

The most scathing criticism came from Rep. Jim Cooper (D-Tenn.), who launched into a lengthy monologue in which he deemed Gorton "one of the most naive chairmen and CEOs I've ever run across," and accused his company of making the "skeleton keys" that grant access to material harmful to U.S. national security.

"I'd feel more than a shade of guilt at this point, having made the laptop a dangerous weapon against the security of the United States," Cooper said. "Mr. Gorton, you seem to lack imagination about how your product can be deliberately misused by evildoers against this country." (Cooper also, at one point, claimed that Gorton's own home computer was probably leaking sensitive documents.)

Rep. Darrell Issa (R-Calif.) warned Gorton that Lime Wire's practices may open the company up to serious legal liability.

"Would it surprise you if you have a string of lawsuits for inherent defect in your product if people like Charlie Mueller of Missouri finds out he's lost his IRS filings and feels he's been damaged?" Issa asked.

Gorton repeatedly defended his company's practices and said he wasn't aware of the extent to which national security information was being accessed through his network.

Lime Wire strives to make its product easier to understand and is working on a new version even more tailored to the "neophyte" user, Gorton said. The software incorporates a number of warnings intended to stave off inadvertent file sharing, he added. For instance, pop-up messages appear when users attempt to share folders, such as the all-encompassing "My Documents" folder and the root directory, which are considered likely to contain sensitive

information.

"A lot of the information that gets out there now is because people accidentally share directories that they wouldn't mean to share clearly," Gorton said. "Those warnings are not enough, at least in a handful of cases."

That assertion drew sharp disagreement from Thomas Sydnor, an attorney-advisor in the Patent Office's copyright group. He said peer-to-peer users are being tricked into sharing files they don't intend to make public and claimed that LimeWire's warnings to that effect don't always appear as they should.

In research for a report released in March, the Patent Office found it "stunning to see features that are incredibly easy to misuse," Sydnor said. "You can go to an interface in these programs that looks like you're doing nothing except choosing a place to store files, and you end up sharing recursively all the folders on your computer. It's very easy to make a catastrophic mistake."

Earlier this year, the Department of Transportation experienced an incident in which an employee's daughter installed LimeWire on the home computer that her mother occasionally uses for telework--and misconfigured it in such a way that documents from the department and the National Archives were open to others using the network--including a Fox News reporter. Forensic analysis determined that some of those documents were already publicly accessible and that none of the DOT documents contained sensitive personally identifiable information about anyone other than the employee herself.

The agency's chief information officer, Daniel Mintz, told the committee that his agency already has sufficient authority to combat "inadvertent" file sharing and that it already is required to take such activity into account in its annual information security reports to Congress.

Now on News.com
P2P networks called national security threat Credits roll for Facebook hearing Video: What's to like about TiVo HD Extra: Antique engines inspire nano chip

The key to preventing additional incidents like that one, Mintz told the politicians, is for his agency to step up oversight and "to make sure we're really pushing the policy," which requires written authorization for installation of P2P programs on government machines. That also means beefing up training for its employees and making sure that they're aware of what the limits are, he added.

General Wesley Clark, who now serves on the board of a small company called Tiversa that makes applications designed to monitor peer-to-peer file-sharing activity, called for "some pretty hard-nosed policies by business and government contractors that prevent people from doing government work on computers that have anything to do with the peer-to-peer networks."

"Even when people...are sophisticated with computers, they can still make a mistake, and all that material can be gone in an instant," the former Democratic presidential candidate told the committee.

CNET News.com's Declan McCullagh contributed to this report.