Hearing Summary

HEARING ON PRIVACY AND SECURITY RISKS OF PEER-TO-PEER TECHNOLOGY

Rep. Henry A. Waxman
Chairman, Committee on Oversight and Government Reform

On Tuesday, July 24, 2007, the Committee held a hearing on inadvertent file sharing over peer-to-peer (P2P) networks, the impact of such sharing on consumers, corporations, and government entities, and whether such sharing creates privacy or security risks for users. Witnesses included officials from the Federal Trade Commission (FTC), the U.S. Patent and Trademark Office (PTO), the Department of Transportation (DOT), as well as independent experts experienced in P2P issues.

The PTO Report. In 2003, the Committee held a hearing to investigate and understand the uses and risks of P2P networks, finding that highly personal data such as tax returns and financial information were being shared with millions of computer users without the knowledge of their owners. After the Committee's 2003 hearing, the P2P industry adopted a voluntary Code of Conduct to prevent inadvertent disclosures of sensitive information. In March 2007, however, the PTO released a report suggesting that inadvertent file sharing may still be a serious problem and that the industry might not be living up to its promise to address this issue voluntarily.

The Committee's Findings. In response to the PTO report, the Committee staff conducted its own investigation into the question of whether inadvertent file sharing is still prevalent. Using LimeWire, one of the most popular P2P programs, Committee staff ran a series of common searches during a one month period. The results were alarming: the Committee staff easily obtained personal bank records and tax forms, attorney-client communications, corporate strategy documents for Fortune 500 companies, confidential corporate accounting documents, government emergency response plans, and even military operation orders.

Risks to Consumers, Industry, and Government. At the hearing, government and independent witnesses confirmed that sensitive information like that obtained by the Committee is continuously being released across P2P networks. A professor from Dartmouth University's Tuck School of Business described how information travels over P2P networks, how individuals are constantly searching for valuable information, and how it is virtually impossible to remove exposed items from circulation. Tiversa, Inc., a firm specializing in data security for corporations, conducted a live demonstration that illustrated the broad scope of information available through P2P networks.

Tiversa also provided the Committee with several highly sensitive security-related documents, including a description of the Pentagon's backbone network infrastructure, U.S. soldier names and social security numbers, and physical threat assessments for multiple cities, including diagrams and details regarding specific infrastructure weaknesses.

Mark Gorton, the CEO of LimeWire, expressed surprise at the breadth of sensitive information available through P2P networks. Mr. Gorton suggested that while some people are "not paying attention to our warnings . . . we need to do a better job of making it very, very, very difficult for users to accidentally share files."

The Potential of P2P Technology. At the hearing, Chairman Waxman emphasized that the goal of the hearing was not to shut down P2P networks or otherwise hinder lawful innovation and development in this area.

Additional information, including Chairman Waxman's statement and copies of testimony, is available at www.oversight.house.gov.