

ONE HUNDRED ELEVENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

Majority (202) 225-5051
Minority (202) 225-5074

April 20, 2009

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Holder:

We have become increasingly concerned about the significant risks posed to American citizens and entities from the accessibility of sensitive private and government information on peer-to-peer file sharing networks (commonly referred to as "P2P"). A number of press reports over the past year underscore the importance of this issue:

- On February 28, 2009, a television station in Pittsburgh reported that the blueprints and avionics package for "Marine One," the President's helicopter, was made available on a P2P network by a defense contractor in Maryland.¹
- On February 26, 2009, the Today Show broadcast a segment on inadvertent P2P file sharing, reporting that social security numbers, more than 150,000 tax returns, 25,800 student loan applications, and nearly 626,000 credit reports were easily accessible on a P2P network.²
- On February 23, 2009, a Dartmouth College professor published a paper reporting that over a two-week period he was able to search a P2P network and uncover tens of thousands of medical files containing names, addresses, and Social Security numbers for patients seeking treatment for conditions such as AIDS, cancer, and mental health

¹ "Navy Releases New Information on Presidential Security Leak," WPXI.com (February 28, 2009).
<http://www.wpxi.com/news/18818589/detail.html>.

² "New Warnings on Cyber Thieves," Today Show, MSNBC, Web video (February 26, 2009).
<http://today.msnbc.msn.com/id/26184891/vp/29405819#29405819>.

problems. The professor found links to four major hospitals and 355 insurance carriers that provided health coverage to 4,029 employers and 266 doctors.³

- On July 9, 2008, the Washington Post reported that an employee of an investment firm who allegedly used LimeWire to trade music or movies inadvertently exposed the names, dates of birth, and social security numbers of about 2,000 of the firm's clients, including Supreme Court Justice Stephen Breyer.⁴
- There have been reports alleging file sharing programs have been used for illegal purposes, such as to steal others' identities.⁵

We are hereby requesting that you provide the Committee staff with a full briefing on the Department's role in protecting Americans from the dangers associated with P2P networks. We are particularly interested in learning the extent to which federal law enforcement action may be taken to protect private citizens, commercial entities, and government agencies from the security risks posed by P2P networks such as LimeWire.

Please have your staff contact Steven Rangel with the committee staff at (202) 225-5051 to arrange the briefing.

Sincerely,



Edolphus Towns
Chairman



Darrell Issa
Ranking Member



The Honorable Peter Welch
Member of Congress

³ See "Academic Claims to Find Sensitive Medical Info Exposed on Peer-to-Peer Networks," Wired.com (March 2, 2009). <http://blog.wired.com/27bstroke6/2009/03/p2p-networks-le.html> .
⁴ See "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing," WashingtonPost.com (July 9, 2008). <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html> .
⁵ See "Seattle Man Accused of Using Software to Hack into Victim's Computers," Seattle Times.com (March 5, 2009). http://seattletimes.nwsourc.com/html/nationworld/2008818184_webtheft05m.html (personal information used to forge checks).