Testimony of

The Honorable Orrin Hatch

June 17, 2003

"THE DARK SIDE OF A BRIGHT IDEA:
WILL PERSONAL AND NATIONAL SECURITY RISKS OF P2P NETWORKS COMPROMISE THE PROMISE OF P2P NETWORKS?"

We are here today to explore some potentially troubling aspects of an exciting technology that rightfully has gained the attention and admiration of millions of Americans, and many millions more around the world: peer-to-peer file sharing networks.

Recent developments in peer-to-peer networks have added dramatically to their versatility - and therefore their utility - to many computer users. Napster, the first peer-to-peer system, permitted the sharing of audio files only, but newer generations of this technology permit the sharing of any type of computer file, including audio files, video files, visual images, documents of all kinds and computer programs.

These advances have been accompanied by a soaring increase in the use of peer-to-peer networks. Kazaa, the most popular of these networks, is now the most popular download on the "downloads.com" Internet site - Kazaa and other file-sharing programs have now been downloaded over 400 million times. Kazaa often has over 4 million users connected to its network simultaneously. The demand for other popular P2P programs, such as Grokster and Morpheus, is growing rapidly as well, and mostly among minors. Research shows that about 41% of those who download files over P2P file-sharing networks are between the ages of 12 and 18.

These statistics underscore the great appeal and promise of P2P networks, as well as the potential scale of any problems they create. They permit rapid and broad dissemination of information and ideas; and they have provided a powerful tool to researchers, hobbyists, and interested citizens seeking information and ideas on an array of topics. At the same time, however, they have also opened up our homes, our businesses, and our government agencies to potentially serious security risks that are neither widely recognized nor easily remedied. Recent studies involving some of the more popular P2P networks suggest that a significant number of their users are inadvertently sharing personal and highly sensitive data over these networks, including tax returns, bank account information, personal identifying information, passwords, and e-mail inboxes. While the true scope of this problem is still unknown, studies have shown that potentially malicious parties are searching P2P networks for personal emails and credit card numbers. This alone is disturbing, but in government agencies, employee use of P2P networks could also disclose sensitive government data to the enemies of this country. At this moment in history, the implications of this risk are troubling, to say the least.

I am also troubled that many P2P networks require their users to install so-called "spyware" or "adware" - programs that monitor, collect, and report information about the Internet "browsing" habits of a particular user. Such programs can collect and disseminate information about the Internet use and personal information of anyone using the computer on which a P2P networking program has been installed. The invasion of privacy and potential for identity theft inherent in such programs has already attracted justifiable attention from members of Congress and consumer advocates concerned about the privacy and security implications of such practices. In addition, some of these "spyware" or "adware" programs can also wreak havoc on a user's computers by commandeering their browsers, creating conflicts with other software that can crash a user's computer, and otherwise interfering with users' control over their computers.

Finally, the users of P2P file-sharing networks may also encounter malicious programs - such as viruses, worms and Trojan horses - that have been disguised as popular media files. Indeed, the operators of the most popular file-sharing program recently explained to the House Committee on Government Reform that "when files come from anonymous and uncertified sources, the risk of [those] file[s] containing a virus greatly increases." If the promoters of

these networks acknowledge that their nature increases users' risk of exposure to malicious programs, then they must also recognize their increased duty to protect and educate their users.

I do believe that peer-to-peer file-sharing networks are here to stay. But the problems of data privacy, spyware and viruses should remind all of us that the final role of peer-to-peer file-sharing networks in our culture remains to be seen. This technology has great promise, but some potential pitfalls. If these networks are designed to minimize the risks of file-sharing, then the promise of this technology can become reality. If not, then users, network administrators and others may ultimately conclude that the risks of this technology outweigh its advantages.

I would like to thank all of our witnesses for appearing here today to address these important issues. We are particularly privileged to have with us three of our colleagues whose stellar work in this area has shed much-needed light on the significance of the risks we will discuss in this hearing and their potential consequences: Senator Feinstein and Representatives Tom Davis and Henry Waxman.

# # #