Testimony of

The Honorable Patrick Leahy

June 17, 2003

Statement of Senator Patrick Leahy
Hearing Before the U.S. Senate Committee on the Judiciary
"The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-peer File Sharing Networks?"
June 17, 2003

Today's hearing will, I hope, mark the beginning of the Judiciary Committee's serious investigation of the enormous potential of peer-to-peer networks, as well as some of the risks posed when this technology, like so many others, is misused. I cannot overstate my interest in the topic of this hearing, nor my conviction that the Committee has a critical role to play in promoting the potential, and policing the problems, associated with peer-to-peer technologies.

I must note at the outset, however, my concern about the process by which we arrived here this morning. It is critically important that we ensure that we are well-prepared to make good use of the expertise and time generously contributed today by the witnesses seated before us. A careful selection of those witnesses, and a thorough study of their written testimony, are absolutely vital to a useful evaluation of the problems associated with peer-to-peer file sharing. The last-minute rush to put this hearing together has meant that, despite the fact that this hearing is supposed to shed light on the important national security issues raised by peer-to-peer networks, there is no witness here from FBI or the Defense Department or the Department of Homeland Security, who can speak to those issues. In the short time leading up to this hearing, I understand that the Committee majority was simply not able to find anyone who was available. As we move forward to explore this important new technology, I am hopeful that we can work in a bipartisan manner and make real progress.

Peer-to-peer file sharing allows people around the world to share information with one another faster and more efficiently than ever before. Individuals with common interests can easily search each others' shared files, and find a wealth of information that they may not even have known existed. They can then download those files directly from each other with remarkable speed and accuracy. Whether you are in rural Vermont or downtown Los Angeles, you - and everyone else with access to the network -- can have all the information you need. And because there is little centralization of the networking process, minimal infrastructure is needed. Thus, peer-to-peer networks can operate in hostile places, without fear that the network will be shut down. In Iraq, for example, peer-to-peer has been used, and is still being used, by humanitarian groups who need to share critical information needed to carry out their missions.

Peer-to-peer has the potential dramatically to change the way we share information, but it is not new to the Internet. In fact, peer-to-peer merely refers to any network that allows users to share information directly with each other, with little or no centralized control. We should not forget that email, and even the world wide web itself, are both types of peer-to-peer networks. When these networks first developed, they also presented serious concerns, and this Committee, both under my leadership and that of Chairman Hatch, correctly took the lead in responding to those concerns. With the expertise and the mandate needed to address these important issues, this Committee has focused on such issues as online privacy, the availability of pornographic materials on the web, computer piracy, and the dangers of computer viruses. By and large, we have responded appropriately to these challenges, by allowing the communities that use these technologies to find the most efficient and effective ways to deal with their concerns. Only where absolutely necessary have we stepped in to regulate in cyberspace. As a result of this careful work, new technologies have developed, with new uses and more powerful abilities -- and they have developed largely without hindrance.

Like email and the world wide web, peer-to-peer file sharing holds simultaneously enormous promise and the danger of harmful misuse. At its core, it has two components. First, it allows a user to search any of millions of computers for a particular file or kind of file. Next, it allows the user to download those files extremely quickly, directly from others on

the network. Despite the promise of these networks, there are problems with some of the ways peer-to-peer is used. Peer-to-peer makes it quite easy to share copyrighted materials. It has also become clear that peer-to-peer networks offer an easy way for people to share pornographic materials, often child pornography, and may allow sexual predators a way to lure their victims into an instant messaging conversation. These are very serious concerns, and I look forward to working with Chairman Hatch and the rest of the Committee to address them. Today's hearing, however, was apparently designed to focus on another important aspect of peer-to-peer networking, the personal and national security problems it may raise.

First, peer-to-peer file sharing can render a user's entire hard drive vulnerable to download by anyone else using the network. This is because the default setting on some of the programs will search your hard drive for any video or audio files, and then make everything in that folder available for download by anyone on the network. Thus, if there is one picture in your "My Documents" folder, the software will recognize it and make all of the "My Documents" folder available for download. You can commonly find personal information like tax returns, credit card information and medical documents on peer-to-peer networks, and many of the users have no idea that they are sharing this information with everyone else on the network. If the user is a government employee and the computer is a government computer, sensitive government information could be made available to those unfriendly to the United States. Here in the Senate, of course, the firewalls installed by the Sergeant at Arms are intended to keep us safe from these dangers by effectively eliminating the possibility of file sharing using Senate computers. But I also understand that not all government offices have such protections in place, which presents the ominous possibility of genuine risks to national security interests.

Second, some peer-to-peer software is designed to circumvent firewalls and other security protections intended to keep peer-to-peer off a computer or network. This prevents parents from protecting their children from adult content, and also prevents network administrators such as universities from keeping unlawful uses of peer-to-peer off their networks. Many networks would choose to preclude peer-to-peer because the software tends to use up a lot of bandwidth. Parents and those who run computer networks should be able to keep peer-to-peer off if they choose to.

Third, certain peer-to-peer programs include "spyware" and "adware." These two types of software track an individual's Internet browsing, and can record any information sent via the Internet, like credit card numbers. They then send that information to marketers, allowing targeted "pop-up" ads and spam. Because they collect personal information, spyware and adware may contribute to identity theft. Spyware and adware often get installed on the user's computer with little or no notice to the user.

These problems are serious ones, but they are not new. In my Privacy Report Card for the 106th Congress, I noted: "Increasingly, personal information such as diaries, finances, and schedules, will not be stored on hard drives, but instead on Internet-based files. Combined with the reality that a substantial amount of our information is being carried over the 'Wireless Web' access to our personal information-by private and by public snoopers-is also growing exponentially." What is new is the public awareness of the risks posed by peer-to-peer, and the urgency we in Congress are feeling about the best ways to address those risks.

And while these problems are serious, they are not insurmountable. The inadvertent sharing of files may well be remedied by improving the instructions and warnings that users are given when they install peer-to-peer software. The software also need not have the ability to circumvent firewalls to work effectively. Finally, peer-to-peer need not insert spyware or adware on a user's computer to work. None of these programs are necessary elements of peer-to-peer technologies. And the problems they raise can be solved, or better yet avoided, if good corporate citizens and good cyber citizens take the responsibility to do the right thing.

I look forward to hearing from our witnesses and to working with all members of the Committee and with the many online communities to help people to solve these problems. We will hear from Senator Feinstein, who has worked so hard to address the problem of identity theft, and Representatives Waxman and Davis, who, as usual, held a very informative hearing on this subject in the House of Representatives last month. I am disappointed that appropriate witnesses from the Administration are not here to discuss the national security aspects of the peer-to-peer problem. We will hear from Chris Murray, the Telecommunications Counsel of Consumer's Union. Mr. Murray has been invaluable in the protection of consumers' interests in the online and telecommunications world. We will also hear from Randy Saaf, the CEO of Media Defender; Alan Morris, the CEO of Kazaa Networks, the most popular peer-to-

peer file sharing program; and Nathaniel Good and Aaron Krekelberg, who have researched the problem of inadvertent sharing of personal information on peer-to-peer networks.

# # # #