

Testimony of
The Honorable Patrick Leahy

September 9, 2003

Statement of Senator Patrick Leahy
Senate Committee on the Judiciary
Hearing on "Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks"
September 9, 2003

At the first Committee hearing on peer-to-peer networks in June, we considered the significant dangers that file sharing can pose to users' privacy and to the security of their computers. Today, we will begin to explore possible solutions to some of the problems raised by peer-to-peer networks and online file sharing. Unless some solutions are found, peer-to-peer will never realize its enormous potential to build on-line communities, to enhance networked learning, and to make unprecedented amounts of material, educational and entertaining, available worldwide.

I believe that peer-to-peer has the potential to revolutionize the way people share all sorts of information. But as with any technology, it can be abused. Peer-to-peer networks can be used to delve into people's private records, or illegally to share copyrighted material. Most disturbingly, peer-to-peer networks can be used to distribute child pornography, and to make all sorts of pornography available to unsuspecting children. If peer-to-peer networks are going to find a useful place in our culture, they must respond to these problems. And we certainly cannot allow those who purposefully exploit network file-sharing to the detriment of children to go unpunished.

As a father and grandfather, I find child pornography despicable. I know my colleagues agree with me. This Committee and the Senate as a whole have taken strong steps to protect our children from pornography, and we will continue to do everything possible to combat child pornography. As a former prosecutor, I want to see that law enforcement has effective tools for the identification and prosecution of the individuals who make, use, and traffic in this material. Pornography, and child pornography in particular, is prevalent on peer-to-peer networks. According to recent reports, as much as 42 percent of peer-to-peer requests are for pornography. A recent GAO study was a wake-up call for America. It found that simple keyword searches on a peer-to-peer network turned up hundreds of pornographic images of children. In fact, child pornography constituted 40 percent of the returns to those searches. The National Center for Missing and Exploited Children, which continues to do outstanding and inspirational work to protect all of our children, reports that there has been a fourfold increase in pornography on peer-to-peer networks in just one year. Moreover, peer-to-peer networks don't simply allow the distribution of child pornography. Through the use of instant messaging, they can be used to lure children into meeting with sexual predators.

So far the peer-to-peer networks are not only turning a blind eye to this problem; in many cases they are specifically designed so that parents are unable to keep their children off the network with a traditional firewall. In addition, what few protections are available are designed so that

they can be easily circumvented by a child, regardless of their parent's intentions.

More disturbingly, the networks are actively hindering law enforcement efforts to crack down on child pornography. Although pornography on peer-to-peer has risen fourfold between 2001 and 2002, arrests for child pornography have dropped dramatically in recent years. We have heard that one, and perhaps the only, reason for this is that peer-to-peer networks have changed their systems to allow their users to remain anonymous. In their zeal to allow illegal file sharing, the networks have made it far too difficult for law enforcement to track down child pornographers. This must stop.

I look forward to hearing from the outstanding group of experts that we have assembled here today about what steps can be taken to stop child pornography. This problem is best solved by the people who understand it best, and deal with it on a daily basis. I am eager to work with those involved as they craft a private-sector solution to this very serious problem, but make no mistake: This must stop.

The second panel today will look at one of the solutions to online file sharing that we enacted five years ago as part of the Digital Millennium Copyright Act. The DMCA gave law enforcement and copyright holders powerful new tools to use in the fight against online copyright infringement.

At the time we were drafting the DMCA, the recording industry, the internet service providers, and others said they were having trouble identifying individuals who might be illegally sharing copyrighted materials online. The parties came together and determined that the best solution was to allow copyright holders to subpoena the information. The subpoena would go to the internet service provider, and would seek the identity of someone the individual believed to be sharing copyrighted material on that ISP's system or network. Section 512(h) of the DMCA codified this solution.

I understand that this section is now being used to subpoena information about individual users who may be sharing copyrighted material, but who are not using the ISP's system or network to store the copyrighted material. In short, it is being used to combat the anonymous use of peer-to-peer networks. There can be little doubt that the use of the 512(h) subpoena raises legitimate concerns for some, such as notice to the end user, oversight of the subpoena process, and the cost of responding to the subpoenas. As before, I believe that these problems are best solved by the groups most closely involved. I look forward to hearing what collaborative steps are being taken to address these concerns, and to make the 512(h) subpoena the fair, but strong tool we intended it to be.

#####