

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
750 FIRST STREET NE SUITE 1100
WASHINGTON, D.C. 20002
(202) 326-6016
(202) 349-1921
<http://www.naag.org>

LYNNE M. ROSS
Executive Director

August 5, 2004

PRESIDENT
WILLIAM H. SORRELL
Attorney General of Vermont

PRESIDENT-ELECT
STEPHEN CARTER
Attorney General of Indiana

VICE PRESIDENT
THURBERT BAKER
Attorney General of Georgia

IMMEDIATE PAST PRESIDENT
BILL LOCKYER
Attorney General of California

Adam Eisgrau, Executive Director
P2P United
c/o Flanagan Consulting LLC
1317 F Street, N.W., Suite 800
Washington, D.C. 20004

Re: Peer-to-Peer Software

Dear Mr. Eisgrau:

We are writing to encourage your companies to take concrete and meaningful steps to address the serious risks posed to the consumers of our States by your company's peer-to-peer ("P2P") file-sharing technology. By addressing such problems today as the use of P2P networks to disseminate pornography, invade privacy and infringe copyrights, P2P software may one day realize its potential as a means for facilitating a wide range of collaborative, project management, business planning, and academic/education activities. At present, P2P software has too many times been hijacked by those who use it for illegal purposes to which the vast majority of our consumers do not wish to be exposed.

We have carefully considered your response to the issues raised by P2P software as presented during the June 15-18, 2004 Summer Meeting of the National Association of Attorneys General and the June 8-9, 2004 National Association of Attorneys General Internet Conference. However, we find that this response fails to address the issues raised by P2P software.

Our consumers need to be provided with the information necessary to understand this technology and to make informed decisions concerning its use. P2P file-sharing technology works by allowing consumers to download free software that enables them to directly share files stored on their hard drive with other users. This type of direct access to one's computer differentiates P2P file-sharing technology from garden-variety e-mail accounts and commercial search engines such as Google and Yahoo.

One substantial and ever-growing use of P2P software is as a method of disseminating pornography, including child pornography. While at least some of your companies do provide “filters” to help screen out unwanted files, including presumably those containing pornography, those filters appear to work by focusing on language in the file’s description or the file’s title rather than on the file’s content. P2P users interested in disseminating and receiving offensive or illegal material, such as child pornography, can simply use an innocuous file title and/or description in order to bypass those filters. Consequently, P2P users need to be made aware that they are exposing themselves, and their children, to widespread availability of pornographic material when they download and install P2P file-sharing programs on their computers.

Furthermore, P2P file-sharing technology can allow its users to access the files of other users, even when the computer is “off” if the computer itself is connected to the Internet via broadband. P2P users, including both home users and small businesses, who do not properly understand this software have inadvertently given other P2P users access to tax returns, medical files, financial records, personal e-mail, and confidential documents stored on their computers. Combating identity theft is one of our priorities, and many of our States have enacted laws to stop it. Consequently, P2P users need to be properly educated so that they will not inadvertently share personal files on their hard drives with other users of your P2P file-sharing technology.¹

The illegal uses of P2P technology are having an adverse impact on our States’ consumers, economies, and general welfare. There are serious concerns that P2P software is replacing Internet chat rooms and e-mail as a medium of choice for the dissemination of pornography, especially child pornography. Market forces and technological limitations of the Internet (e.g., the need to pay for web space and bandwidth) have combined to make peer-to-peer software a more attractive alternative to the Internet as a means of disseminating pornography. Peer-to-peer users and distributors of child pornography particularly believe that their anonymity on P2P networks protects them from detection by law enforcement. According to a January 25, 2004 New York Times Magazine article, “[c]yber networks like KaZaa and Morpheus – have become the Mexican border of virtual sexual exploitation.” The Federal Trade Commission, the United States General Accounting Office, and the Judiciary Committee of the United States Senate, among others, have all taken testimony or issued reports on the increasing use of P2P software to disseminate pornography.

P2P file-sharing programs also are being used to illegally trade copyrighted music, movies, software, and video games, contributing to economic losses. The Business Software Alliance estimates that its members lost \$13 billion in revenue last year due to software piracy. According to a February 20, 2004 CNN article, “U.S. software companies lose up to \$12 billion a year in piracy according to the Software and Information Industry Association. Music companies lost more than \$4.6 billion worldwide last year, according to the RIAA [Recording Industry Association of America] and movie industry officials pegged their annual losses from bootlegged films at more than \$3.5 billion.”

¹ This problem is exacerbated by the default settings that you use as part of the installation process of P2P software. One default setting designates each and every file in a user’s hard drive for sharing with other users of P2P software. A second default setting leaves a user’s computer continuously accessible to the Internet. We would urge your companies not to select such default settings as part of your software installation process.

The article further reveals that “[t]he entertainment and computer industry have tried to stem piracy by making CDs and DVDs harder to duplicate. But the rise of free file-sharing networks on the Internet has made it easy for millions of individuals to distribute songs, movies, and software worldwide.” Similarly, a March 28, 2003 USA Today article described a recent hearing of the California Senate Select Committee on the Entertainment Industry in which “committee chairman Kevin Murray, D-Los Angeles, downloaded the KaZaa media desktop player in under 20 seconds, then downloaded numerous songs and the Oscar-winning movie *Chicago*, which hasn’t been released on DVD.”

Some of your companies have taken initial steps to warn users of P2P software that it may not be employed for illegal ends, which is commendable. However, more needs to be done by your companies to warn your P2P users as to the specific legal and personal risks they face when they use P2P technology for the illegal ends of disseminating pornography and “sharing” copyrighted music, movies, and software.

We have, in the past, initiated Internet-related actions to stop individuals from disseminating unwanted spam, including deceptive e-mail designed to lure unsuspecting adults and children to pornographic web sites. We will, as appropriate, continue to initiate such actions in the future to stop deceptive and illegal practices by users of the Internet, including users of P2P software.

However, the undertaking of enforcement actions against individual users does not excuse your companies from fostering deceptive practices on our consumers that invade their privacy and threaten their security. Nor do they excuse your companies from avoiding software design changes that deliberately prevent law enforcement in our States from prosecuting P2P users for violations of the law.

We view with alarm reports that P2P software is being used by your companies as a means of transmitting unwanted spyware and adware that is bundled with the P2P software. Spyware aids an individual or a corporation in gathering information about P2P users without their consent or in asserting control over P2P users’ computers without their consent. In the past, we have initiated enforcement actions against Internet web sites that, without the knowledge of our consumers, placed “cookies” on their computers designed to track their use of the Internet. We would ask you to take concrete and meaningful steps to avoid the infringement of the privacy and security of our citizens by bundling unwanted spyware and adware with your software.²

We view with equal alarm reports that at least some P2P file-sharing services are adding encryption features to those services. The addition of such encryption features will make it more difficult, if not impossible, for law enforcement to police users of P2P technology in order to prosecute crimes such as child pornography. Encryption only reinforces the perception that P2P technology is being used primarily for illegal ends. Accordingly, we would ask you to refrain from making design changes to your software that prevent law enforcement in our States from investigating and enforcing the law.

² It also has come to our attention that P2P file-sharing technology is being used as a means of transmitting computer viruses and worms because conventional virus protection programs, such as those marketed by Novell, do not scan files exchanged via such technology. If such is the case, then it would be incumbent upon your companies to warn your users of this risk.

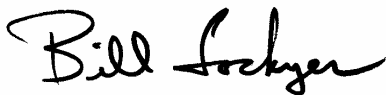
Finally, we are concerned that the filters currently in use are inadequate as a means of protecting P2P users, and their children, from unwanted and offensive materials, such as child pornography. We believe that meaningful steps can and should be taken by the industry to develop more adequate filters capable of better protecting P2P parents and children from unwanted or offensive material. Not warning parents about the presence of, and then reasonably providing them with the ability to block or remove, obscene and illegal materials from their computers is a serious threat to the health and safety of children and families in our States.

We take seriously our responsibility to protect our citizens from misleading or deceptive practices, and to ensure that our citizens are given the information necessary to making an informed decision. And, we take seriously the need to investigate and prosecute violations of our laws wherever they may be taking place – on the Internet, in the brick and mortar world, or on P2P networks.

We believe that it is in no one's interest for P2P technology to be used in order to promote unlawful or deceptive activities. Rather, we believe that concrete and meaningful steps can and should be taken to address the problems we have raised in this letter. It is only by taking such steps that P2P networks will be able to realize their innovative potential as a 21st century virtual collaboration and project management tool for regional or nationwide academic, business, home, and governmental activities.

We look forward to working closely with you to proactively address these problems.

Sincerely,



BILL LOCKYER
Attorney General of California



GREG ABBOTT
Attorney General of Texas



CHARLIE CRIST
Attorney General of Florida



TROY KING
Attorney General of Alabama



TERRY GODDARD
Attorney General of Arizona



MIKE BEEBE
Attorney General of Arkansas



KEN SALAZAR
Attorney General of Colorado



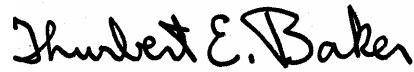
RICHARD BLUMENTHAL
Attorney General of Connecticut



M. JANE BRADY
Attorney General of Delaware



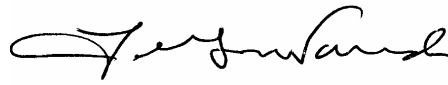
ROBERT J. SPAGNOLETTI
Attorney General of the District of Columbia



THURBERT BAKER
Attorney General of Georgia



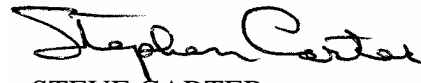
MARK J. BENNETT
Attorney General of Hawaii



LAWRENCE WASDEN
Attorney General of IDADHO



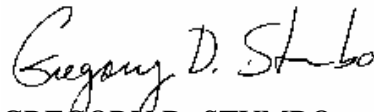
LISA MADIGAN
Attorney General of Illinois



STEVE CARTER
Attorney General of Indiana



TOM MILLER
Attorney General of Iowa



GREGORY D. STUMBO.
Attorney General of Kentucky



CHARLES C. FOTI JR.
Attorney General of Louisiana



STEVE ROWE
Attorney General of Maine



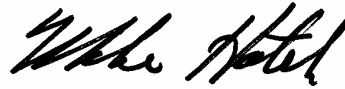
J. JOSEPH CURRAN JR.
Attorney General of Maryland



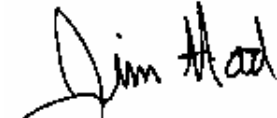
THOMAS F. REILLY
Attorney General of Massachusetts



MICHAEL COX
Attorney General of Michigan



MIKE HATCH
Attorney General of Minnesota



JIM HOOD
Attorney General of Mississippi



JEREMIAH W. NIXON
Attorney General of Missouri



MIKE MCGRATH
Attorney General of Montana



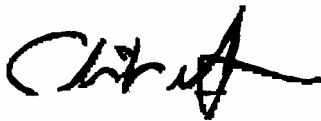
BRIAN SANDOVAL
Attorney General of Nevada



PETER C. HARVEY
Attorney General of New Jersey



PATRICIA MADRID
Attorney General of New Mexico



ELIOT SPITZER
Attorney General of New York



ROY COOPER
Attorney General of North Carolina



WAYNE STENEHJEM
Attorney General of North Dakota



JIM PETRO
Attorney General of Ohio



W.A. DREW EDMONDSON
Attorney General of Oklahoma



HARDY MYERS
Attorney General of Oregon



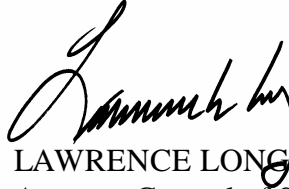
GERALD J. PAPPERT
Attorney General of Pennsylvania



PATRICK LYNCH
Attorney General of Rhode Island



HENRY MCMASTER
Attorney General of South Carolina



LAWRENCE LONG
Attorney General of South Dakota



PAUL SUMMERS
Attorney General of Tennessee



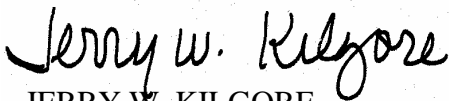
MARK SHURTLEFF
Attorney General of Utah



WILLIAM H. SORRELL
Attorney General of Vermont



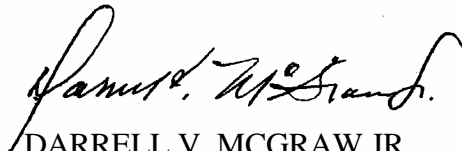
IVER STRIDIRON
Attorney General of the Virgin Islands



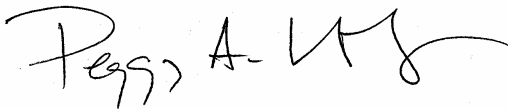
JERRY W. KILGORE
Attorney General of Virginia



CHRISTINE O. GREGOIRE
Attorney General of Washington



DARRELL V. MCGRAW JR.
Attorney General of West Virginia



PEGGY A. LAUTENSCHLAGER
Attorney General of Wisconsin

