

Testimony of

Mr. Alan Morris

September 9, 2003

Statement of Mr. Alan Morris, Executive Vice President,
Sharman Networks Limited
Before the
Senate Judiciary Committee
Regarding
"Pornography, Technology and Process: Problems and Solutions on
Peer-to-Peer Networks"
Washington, DC
September 9, 2003

Chairman Hatch and members of the Committee, thank you for this opportunity to again share the views of Sharman Networks Limited (SNL) regarding peer-to-peer (P2P) technology. I am Sharman's Executive Vice President and, as it is a global business, I am responsible for supervising the enterprise from London whilst our Sydney headquarters is off-line at night. I also have specific responsibility for developing the promotion and distribution of licensed content in conjunction with Altnet, our Los Angeles-based U.S. business partner. The Altnet service is available to all users of the Kazaa Media Desktop (KMD) software. Altnet is the largest distributor in the world of licensed and protected media files, as well as the leading purveyor of files utilizing Microsoft Windows Media digital rights management (DRM) technology.

Since its creation, SNL has been dedicated to two principal goals. The first goal is to fully exploit the potential for P2P software to enrich society and the creators of intellectual property through the development of this most efficient means for the commercial distribution of copyrighted material. The second is to provide consumers with the most secure and best functioning P2P software available anywhere; we are the industry leader and consumers have validated our efforts by making the Kazaa Media Desktop (KMD) the most popular P2P application. So, we have built the technology platform for achieving our premier goal, and will be announcing a series of exciting new ventures with content providers throughout the world in coming months. Our greatest disappointment in this regard is that major U.S. content providers have yet to acknowledge that P2P is not the problem but the solution to their digital dilemma and license their copyrighted material for paid distribution to KMD users.

P2P Misinformation

Unfortunately, certain Hollywood interests have not just failed to acknowledge the positive role that P2P can play in solving their online distribution challenge, but have embarked on a deliberate campaign to try to smear P2P technology itself. It seems that ever since Federal District Judge Stephen Wilson's April ruling that the distribution of P2P software was a legal activity in the United States under the standard established by the Supreme Court's 1984 "Betamax" decision, entertainment industry lobbyists have accelerated their deliberate campaign of P2P misinformation on Capitol Hill.

When I testified before you in June I took many of those charges head on and, I believe, showed you that the concerns raised were spurious. You learned that KMD includes, at no cost, highly effective anti-virus protection; last month this feature validated P2P as the distribution technology of the future in response to the MSBlast scare by distributing a massive 10 Terabytes of antivirus update files seamlessly over P2P in a single week, with none of the load problems encountered at this time of peak demand by traditional anti-virus distribution. We also apprised you of SNL's firm "no spyware" policy. And we described the

extensive changes we had made to the KMD user interface and installation process to eliminate any possibility of identity theft as a result of inadvertent placement of personal information in a user's shared folder, even though the FBI had apprised Congress that it did not know of a single instance of I.D. theft resulting from the use of P2P software. Our testimony also quoted various experts' Congressional testimony that P2P software did not have intrinsic security weaknesses or present different or greater security problems than such common Internet tools as web browsers or e-mail software.

Since we presented that testimony, intervening events have further substantiated our position. Two major electronic virus infestations caused several \$billion in damage to computer systems over the summer, and in both cases the principal means of propagation was the exploitation of known weaknesses in commonly used server and e-mail software, with P2P playing no role - indeed, as I noted, it was a major force in combating it. And, just last week, the Federal Trade Commission released its Identity Theft Survey Report; in recounting the means by which I.D. thieves gain access to the personal information of their victims, P2P does not even get a mention. As the saying goes, while P2P's detractors are entitled to their own opinions, they are not entitled to their own facts.

Zero Tolerance for Child Pornography

Mr. Chairman, there is one allegation being made against P2P software that we find vile and reprehensible. And that is the charge that there is some strong linkage between the use of such software and the propagation of exploitive and illegal child pornography. Let me make Sharman Network's position on such despicable content crystal clear. We utterly abhor child pornography. We do not want our software used to propagate this filth, even if it is in a small way.

Since acquiring the KMD software early in 2002 we have had only a handful of case requests about specific child pornography available through P2P from law enforcement agencies worldwide. In each case we proved willing to immediately work with officers. However, they realized very quickly what their colleagues elsewhere had determined some while before -

? Pedophiles quickly realized, when P2P first appeared, that it was a foolhardy way to pursue their warped ends. To make their "collections" publicly available on P2P is counter to their cloak of secrecy. Law enforcement agencies quickly picked them off and so they retreated back to their sordid encrypted sites, newsgroups and the like.

? The nature of p2p applications, unlike websites with their central servers, means that software developers like SNL have about as much knowledge and control over what individuals choose to share as Microsoft has over what is sent via its e-mail clients!

? The relatively small amount of child pornography circulating on P2P has been hypothesized as being largely the legacy of these early forays rather than the stream of new material that pervades the chosen means of pedophile distribution.

Not satisfied just to see this small amount of material wither away (see chart at end of statement) we are actively working with U.S. and international law enforcement authorities, including the FBI, to provide them with a technical understanding of the software and, whilst clarifying the limitations in knowing systemically about files transacted, we have pointed out how they may use readily available technologies to help identify specific users who share illegal pornographic material. Law enforcement agencies, of course, may obtain through appropriate legal process the willing cooperation of ISPs and others in the chain of transmission the necessary proof to pursue and arrest miscreants. In this regard we applaud the actions of Suffolk County police authorities in arresting individuals who have used KMD or other P2P applications to share illegal content and hope other police agencies follow suit. We want pedophiles to quickly get the message that when they make such materials available for other P2P users to find they are also making it quite easy for law enforcement authorities to find them, and then cease to use P2P as a means of propagating child pornography.

In short, Sharman Networks has a zero tolerance policy in regard to child pornography, and we stand ready to take whatever additional feasible steps a software distributor can take to assist in reducing this problem

still further. It should be noted that, while we support user privacy, SNL has not chosen to use methods of providing anonymity to users that could hinder the legitimate quests for purveyors of obscene material by law enforcement agencies.

So, we ask that you put P2P's role in perspective as regards the very real and growing problem of child pornography on the Internet. Based upon the data we have seen, such as that contained in the General Accounting Office's February report on this subject (GAO-03-351) and the chart reproduced below, P2P plays a very minor role in the propagation of child pornography. P2P referrals presently constitute less than two percent of all reports of child pornography submitted to the CyberTipline operated by the National Center for Missing and Exploited Children, while Internet Web sites account for more than seventy seven percent. While any amount of child pornography available via P2P software is unacceptable to us, we know of no instance or charge that there is any commercial or organized distribution of such materials using P2P, while many of the thousands of Web sites hosting child pornography do charge for access to these illegal materials, and newsgroups are actively used for illegal private distribution.

Commercial child pornography Web sites are a rapidly growing problem. Last month, the United Kingdom's National Criminal Intelligence Service released a report stating that Websites containing child pornography had more than doubled in the past year, that more than half of them were hosted in the United States, and that Internet pedophiles were developing more cunning means of avoiding detection. Clearly, any effective law enforcement initiative against the child pornography problem must be primarily directed against these Web sites and coordinated on an international basis

Mr. Chairman, it is clear that the vast majority of the child pornography problem stems from Web sites accessed by Web browser software. Yet we do not see a coordinated campaign to smear Web browsing technology even though it is the primary technological means by which child pornography is accessed, distributed, and sold. Nor do we see such a campaign against instant messaging software, chat rooms or news groups, even though there have been repeated reports of how pedophiles have masqueraded as minors and used these technologies to engage in suggestive conversations with minors, to send pornographic images to minors, and to attempt to set up face to face meetings with minors. And we certainly do not see misguided legislative initiatives, such as a bill recently introduced in the House of Representatives that aims to ban the distribution of P2P technology, directed at these other major technological tools which are commonly subverted by pedophiles for their evil purpose. Nor should we, because we all know that technologies are not inherently good or evil - what's good or bad are the uses that individuals put them to; and what should be pursued are those bad actors that use them for evil ends.

It seems the reason that the entertainment industry has tried to create an unwarranted association between child pornography and P2P is not because P2P software plays a major role in this illicit trade but because they want to create sufficient animosity against this technology to assist in the enactment of new legislation that weakens Betamax standard protection, requires copy control technology, regulates P2P out of existence, or otherwise supports Hollywood's goal of subjugating technology to the needs of their existing business models. This ploy was admitted by unnamed record industry executives in a September 2nd Los Angeles Times article: "Even as the RIAA prepares to seize parents' attention with lawsuits, music executives increasingly have been trying to call attention to the fact that file swapping networks also are frequently used to share child pornography and other X-rated images. Record executives say privately they're also aiming to use the proliferation of pornography as a means of persuading members of Congress and law enforcement officials to take a tougher stance against the file networks."

This may be seen as hypocritical, to say the least, from an industry which quickly wraps itself in your First Amendment whenever the content it produces and the advertising that promotes it are criticized for graphic and gratuitous sex and violence and the promotion of substance abuse. The difference is that the entertainment industry actively markets such fare to kids -- Sharman just provides technology that can be used or misused.

Barring Minors' Access to Legal Adult Content

Most adult content is legal, and its availability in our society is a fact of life, with major corporations engaged in its distribution. It's sold on nearly every newsstand. It's marketed on both a subscription and pay-per-view basis to customers of satellite and cable TV and guests at major hotel chains. The ability to watch X-rated movies in the privacy of one's own home was a driving force in the adoption of the VCR, and this content has migrated onto DVDs as that new technology supplants video tape. And it's well known that access to adult content and sex-oriented chat rooms was an important factor in the growth of now major ISPs, and that the sale of legal adult content is one of the major Internet commerce success stories as well as being touted as the "killer content" for new generation 3G phones.

So it should come as no surprise that one use that individuals make of P2P software is to access adult content. SNL does not distribute any such content. Altnet does have a paid publishing system that allows content owners to publish content into the system. A legal review is always conducted on all such content before publishing takes place. Following the high standards of satellite TV and the cable industry, Altnet does not discriminate against publishers that work within the law and provide technical restrictions to prevent unauthorized distribution of content that may be unsuitable to children. Any adult content published via Altnet is of course only available, through strict credit card verification, to persons over eighteen years of age.

Other individual software users provide the great majority of the adult content available to users of the KMD software. SNL has no direct knowledge of what any particular user is providing, nor do we have any ability to control such distribution or remove a particular piece of content. What we can do, and in fact do, is to provide KMD users, at no charge, with the most comprehensive and effective, password protected, family filter available with any P2P software application.

The extensive availability of offensive materials on popular search engines, such as Yahoo and Google, is a concern for everyone. For instance, a search for the most commonly used adult term on Google will return 43,600,000 results! This does not mean Google is inherently bad. To the contrary, it simply reflects the vast amount of pornography accessible from websites that minors may access in the absence of parental oversight, in contrast to the relatively small amount available from peers' shared folders via P2P.

Like these companies, we are making great efforts to educate users and to aggressively encourage the use of our built in family filter. This filter is set to "on" as the default when the KMD software is first downloaded. Upon acquiring KMD in 2002 we thought it particularly important that such a filter be made an integral part of the software and be turned on as default. This has been validated by the finding of the June 2003 report, "Fast and Present Danger: In-Home Study on Broadband Security Among American Consumers", a study conducted by America Online for the National Cyber Security Alliance, that in 97% of homes with broadband connections parents failed to employ any parental controls to block access to the vast array of adult materials available on tens of thousands of Internet Web sites. Our family filter also provides parents with a password-protected lock so that it cannot be turned off when they are out of the house. We believe it should always be used in households where children may have access to the PC. We also believe filters can never take the place of active and involved parenting.

The KMD filter is based on a confidential list of keywords (unsurprisingly culled from the terms used on the major search engines) associated with adult content and other offensive materials. No adult content filter, no matter how it works, can ever be 100 percent effective at blocking such content. That is particularly true when individuals deliberately create false metatags so that offensive content may be found in a search for innocent material. Similarly some files are salaciously or misleadingly labeled, however innocent or obscene the content might be. There is nothing unique to P2P in this regard. Just last week, the U.S. attorney for the Southern District of New York, in conjunction with the U.S. Postal Inspection Service, made the first arrest under the Truth in Domains Names Act. They charged an individual with creating at least 3,000 misleading domain names, such as dinseyland.com, so that individuals making common typing mistakes, including children, would be connected to advertising sites, including those for pornographic materials, from which they could not easily exit. Announcing the arrest, U.S. Attorney James Comey stated, "The defendant is accused of taking advantage of children's common mistakes, and using that to profit by leading them by the hand into the seediest and most repugnant corners of cyberspace. His alleged actions are not clever but criminal."

We abhor such practices and we welcome any suggestions as to how we might increase the protections against unwanted exposure to adult materials available through the use of P2P technology. But, whether children are using Web browsers, instant messaging software, chat rooms or P2P software, the best means of preventing unwanted exposure to offensive materials is for parents to employ available safeguards such as KMD's family filter, and to actively monitor their children's Internet activities while periodically reviewing both the software and content on their home computer hard drives.

Conclusion

We appreciate this opportunity to share our views regarding pornography and P2P software. We are dedicated to the eradication of child pornography from P2P networks and will continue to cooperate with Congress, law enforcement agencies, and dedicated nongovernmental agencies in support of that shared goal. We are constantly updating the terms blocked by the KMD family filter and will take all other feasible steps to best assure that minors are not inadvertently exposed to adult content when using the KMD software. We have also helped to found a new trade group, the Distributed Computing Industry Association (DCIA), which is designed to bring together all business interests with a stake in P2P technology to collectively address shared challenges, including pornography.

We hope that this Committee and the Congress as a whole will, as they address this issue, keep in mind the many responsible actions that Sharman Networks has taken in regard to adult content, as well as the relatively minor role that P2P plays in the overall availability of such content on the Internet.

I would be pleased to answer your questions.

Source: New York Times, September 7, 2003