

Testimony of

Mr. Alan Morris

June 17, 2003

Chairman Hatch and members of the Committee, I want to thank you for this opportunity to share the views of Sharman Networks Limited (SNL) regarding security considerations for 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 whilst Sydney is off-line at night. I also have specific responsibility for developing the promotion and distribution of licensed content in conjunction with Altnet. I am accompanied at the witness table today by Mr. Derek Broes, Executive Vice President of Worldwide Operations for Los Angeles-based Brilliant Digital Entertainment (BDE). BDE's 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. Mr. Broes is a recognized expert on Internet security, and Altnet is now in the process of rolling out a new high-security file-sharing network for users of KMD. He has submitted a formal statement to the Committee that I would ask to be made part of today's official hearing record.

We commend the Committee for scheduling this important hearing. P2P is a natural step in the evolution of the Internet. It is seen by many as a powerful and beneficial technology for maximizing the efficiency of computing and network resources, as well as a medium for making information and media available to a worldwide audience at the lowest conceivable cost. But P2P is hardly the end point of the Internet evolution - it is a way station toward fully distributed computing applications commonly referred to as "grid computing". As described in the article "The Grid: Computing Without Bounds" which appeared in the April 2003 issue of Scientific American, "Grid computing refers to the large-scale integration of computer systems (via high-speed networks) to provide on-demand access to data-crunching capabilities and functions not available to one individual or group of machines...[It] enables large-scale scientific and business collaboration among members of virtual organizations, remote experimentation, and high-performance distributed computing and data analysis."

That same Scientific American article recognized Kazaa's legitimate place among new distributed computing technologies: "The concept of globally virtualized grid computing is a natural extension of today's Internet. The Internet virtualizes communications, permitting any person to connect with any other person or device, regardless of location or the means used to do so. The result has been an explosion of innovative functions: e-mail, the World Wide Web, peer-to-peer applications, including file-sharing systems such as Kazaa, and simple distributed-computing schemes such as SETI@home and the Smallpox Research Grid." (Emphasis added)

SNL's Commitment to User Privacy and Security

From inception, Sharman Networks Limited, owner and operator of the Kazaa Media Desktop (KMD), has taken great care to protect users' privacy and security. As the most popular peer-to-peer application, KMD has consistently lead the field with security enhancements developed specifically for the challenges of this new industry, including peer-to-peer's first anti-virus tool.

Kazaa Media Desktop is the only P2P application that includes specifically designed and fully integrated third party virus protection software. 'BullGuard', one of the most advanced proprietary virus protection technologies available, has been installed free to users of KMD since late 2002 and provides an additional layer of protection over and above any antivirus software users have already installed on their computers.

Sharman Networks takes every opportunity to encourage responsible and safe peer-to-peer usage through user education as well as via the default configuration of the software. The nature of decentralized peer-to-peer technology means that users control the material they choose to share with others. Our goal is to provide users with the tools they need for safe and responsible use, though the decision to share material is always at the users' discretion.

The Kazaa.com website provides users of KMD with extensive information to enable them to achieve desired levels of security. Our Privacy Statement provides clear and extensive disclosure of our consumer-friendly policies regarding information collection, use of "cookies", and opt-out mechanisms. Kazaa has a firm "No Spyware" policy to protect users against software that is either surreptitiously installed or which covertly gathers user information. Our Security and Privacy guide is constantly scrutinized and upgraded in the light of usability trials and third party reports and instructs users on how to engage in safe sharing and protect themselves against computer viruses. Our Setup guide provides detailed information as to how users may disable file sharing and activate our password-protected Family Filter to block the inadvertent download of offensive and adult material, as well as to activate additional filter options that can block file types known to transmit viruses, files that would not be blocked by a firewall, and bogus files. We believe that we have the most extensive and effective protection policies and capabilities of any P2P software available today. But we are not resting, and are continuously testing further improvements consistent with our role as the P2P technology leader.

The availability of offensive materials, in particular any involving children, on every search engine including Yahoo and Google is a great concern of ours. Like those companies mentioned, we are making great efforts to educate and when possible, work with authorities in their efforts to mitigate the problem. We aggressively encourage the use of our built in family filter and 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.

Sharman Networks is committed to the security of its software and has proven that it will take the proactive steps necessary to defend the integrity of Kazaa Media Desktop, including addressing any new malicious viruses that 'freeze', 'silence' or otherwise compromise a user's experience. Sharman continues to maintain its role as market leader and will continue to set best practices and high standards for the burgeoning growth of P2P in general.

Inadvertent Sharing and Identity Theft

Mr. Chairman, identity theft as a byproduct of using P2P software remains a hypothetical threat. Last month James Farnan, the Deputy Assistant Director of the FBI's Cyber Division, told the House Government Reform Committee that "no instances of identity theft have been reported to be associated with P2P networks". Despite the assurance this gives in the short term with regard to the competency of our existing systems, we are never complacent - Sharman will continue to do everything possible to make use of the KMD completely secure by default; with a design so intuitive that users cannot inadvertently share personal files, and so clear in its operation that users can easily ascertain exactly what files they are sharing.

We take responsible critiques of our software very seriously, and we respond to them quickly. We welcome intelligent research such as "Usability and privacy: a study of Kazaa P2P file-sharing" (the "HP study") first published by Nathaniel Good and Aaron Krekelberg last year and updated in April 2003, and we integrate such thinking into our product development plans. As soon as we received that study we compared its findings with the focus group user sessions we have conducted by independent third parties. Version 2.5 of KMD, now in beta release and soon to go public, incorporates a variety of security changes to prevent inadvertent file sharing during KMD installation, prevent a change in the location of the "My Shared Folder" that might lead to accidental sharing of preexisting folders, and make it far easier for users to determine what they are sharing. In particular, any user who attempts to share an entire drive, including their hard drive, now receives a very strong warning against doing so. Users are more definitively encouraged to maintain the KMD default settings, which designate the My Shared Folder as the only shareable location. The "Participation Level" portion of our online guide makes clear that preferential queuing for a requested file depends on the ratio of uploaded to downloaded megabytes and not upon the total megabytes available for sharing. In other words, making lots of files available, that others are not likely to be interested in, provides no benefit. Users are likewise rewarded for rating the integrity of files. The goal of our participation level policy is to maximize the functionality and integrity of the Kazaa P2P experience.

We would note that, in testimony before the Government Reform Committee last month, the authors of the HP study stated, "The problems we discovered with the Kazaa interface are not intrinsic to P2P in general, nor are they a reflection of an underlying security weakness in P2P systems... [They] can be adequately addressed by educating users about P2P and networking in general, and more importantly, improving the user interface." As noted, we took their study seriously and have made the recommended upgrades.

P2P in Perspective - User Education Needs

Mr. Chairman, while some entertainment industry executives have embarked upon a campaign to demonize P2P, the risks associated with this digital technology are neither unique nor exceptional. Jeffrey Schiller, Network Manager and Security Architect for MIT, testified before the House Government Reform Committee last month that, "In some ways they [P2P programs] are more secure than E-mail...File-sharing programs, as viewed by the end-user are no more or less secure than other common Internet applications such as web browsing or reading E-mail...The risks are slightly different, but the magnitude of danger is about the same." (Emphasis added)

Indeed, Congress could keep itself very busy holding hearings on the security flaws of all sorts of well known, branded digital software. In just the past few weeks, the press has carried reports that:

- ? Vulnerability in the Microsoft Windows Media Player could enable an attacker to execute an attack on the computer of a user who downloads a new "skin" for the player.
- ? The latest version of America Online's ICQ instant messaging software contains a flaw that could allow an online attacker to take control of a user's computer.
- ? Microsoft acknowledged a security flaw in its popular Internet Passport service that left 200 million users vulnerable to hackers and thieves, and that may have been in violation of an FTC consent order regarding the veracity of its claims for Passport's security and privacy protections.

These are just a few of many possible examples. Certainly, any software flaw that has the potential to let a third party take over one's computer is the ultimate security risk and the most egregious form of digital identity theft. What is required in response to such reports is not accusation and vilification, but immediate remedial actions combined with a long-term commitment to improving basic education on security risks for all computer users. We cannot overemphasize the need for improved user education, especially as we move into an "always on" world of broadband connectivity through both wired and wireless access. While one must undergo extensive training and obtain a driver's license to cruise the interstate highways, absolutely no such prerequisites apply to surfing the information highway. We are hardly about to suggest that government impose a licensing requirement for Internet use, but government should promote the need for a greater level of public understanding of the risks of all forms of public Internet activity and the ways that they can be effectively managed.

The pressing need for such education was brought home by last week's release of "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 study revealed that for broadband users in general:

- ? 97% of broadband parents do not use parental controls
- ? 67% of users do not have properly and securely configured firewalls
- ? 62% do not regularly update anti-virus software
- ? Despite vulnerabilities, 86% keep sensitive information on their home computer

The adoption of broadband is both inevitable and desirable. For years policymakers in Washington and other capitals have debated how to best encourage more rapid adoption of broadband to create the infrastructure for the long promised wide range of innovative new products and services. Commentators, telecommunications companies and service providers all agree that P2P is the "killer app" that has finally given the public the incentive to acquire broadband and so drive the development of the many societal and commercial opportunities created by a high speed wired world. But the public and private sectors must do far more to help educate users about the inherent risks of fast connectivity, as well as the available and effective means for ameliorating them.

External Threats to P2P Security

Mr. Chairman, Sharman Networks is committed to continually improving security and privacy safeguards for the tens of millions of users of Kazaa Media Desktop worldwide. Indeed, much like companies such as Microsoft and AOL in other Internet sectors, Sharman has set standards for security in P2P. However, real threats to the security of the computers of millions of P2P users around the world arise from the activities of those who seek to portray themselves as being impacted negatively by P2Ps existence. From its inception, Sharman Networks has been dedicated to legitimate and licensed uses of P2P technology that compensate copyright owners and reward creators. But content

industries have yet to fully understand and embrace the commercial benefits available to them through P2P. As Michael J. Wolf, Managing Partner of McKinsey & Company's Media and Entertainment Practice wrote in a May 1, 2003 Wall Street Journal opinion piece on digital music services: "But what's missing from the equation are the file-sharing services themselves, sites like Morpheus, Kazaa and Grokster, which attract 30 million consumers every month. These are the killer apps of the broadband computing world, and one presumes they'd rather attract revenues than lawsuits."

Indeed, we would much prefer to enter into mutually beneficial agreements that serve artists and the public. But the entertainment sector does not seem to be ready to admit that P2P can be their path to prosperity. Until they realize that, some of their current tactics constitute a clear and present danger to the privacy and security of P2P users

In this regard, we recommend that this Committee should overview the "software bullet" technology initiatives being funded by the entertainment industry. A front page story in the May 4, 2003 New York Times reported that, "Some of the world's biggest record companies, facing rampant online piracy, are quietly financing the development and testing of software programs that would sabotage the computers and Internet connections of people who download pirated music, according to industry executives...The covert campaign, parts of which may never be carried out because they could be illegal under state and federal wiretap laws, is being developed and tested by a cadre of small technology companies, the executives said." Among the technologies reportedly being tested and developed are those that lock up computers for hours, delete files from hard drives, and disrupt Internet connections. Such technologies pose a grave threat to both individual users and to ISPs. As Stanford Law School Professor Lawrence Lessig noted, "Freezing people's computers is not within the scope of copyright laws." Hard questions need to be asked about why public companies are investing in the development of technologies that are illegal to implement. Congress also has a right to know what precautions are being taken to make sure that these malicious viruses do not "escape from the lab", and what steps the financiers and developers of these dangerous technologies will take to admit responsibility and advise the public of effective countermeasures in such a situation. Otherwise, there is a distinct possibility of extreme disruption of computer networks and substantial economic loss to their users occurring without public awareness of the source of the infestation.

Further, the activities of the Entertainment industry in pursuing their ends are seen by many observers to constitute a real threat to public privacy: As former Clinton Administration chief privacy officer Peter Swire commented; "The RIAA's position (on gaining subscriber identities from ISPs..) would make it trivially easy to learn the name, address and phone number of anyone who sends e-mail or visits a website".

Conclusion

Mr. Chairman, thank you again for providing this opportunity to discuss privacy and security considerations related to P2P software. While P2P is not without risks neither is any Internet experience, and its present and potential benefits far outweigh them. We at Sharman Networks will continue to make improvements that reduce the chances of inadvertent sharing of sensitive files, and to educate our users regarding the basics of online protection. And we stand ready to work with this Committee, other agencies of government, enterprise and public interest organizations toward shared goals of educating and protecting consumers.

I would be pleased to answer any questions you may have.