WRITTEN STATEMENT OF

MR. SAFWAT FAHMY,

CEO AND FOUNDER, SAFEMEDIA CORPORATION

FOR THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

HEARING ON "USING TECHNOLOGY TO REDUCE DIGITAL COPYRIGHT VIOLATIONS ON CAMPUS"

JUNE 5, 2007, 2:00 P.M.

ROOM 2318

RAYBURN HOUSE OFFICE BUILDING

Chairman Gordon, Ranking Member Hall, I want to commend you and your committee for calling this important hearing on "Using Technology to Reduce Digital Copyright Violations on Campus."

My name is Safwat Fahmy, and I am the CEO and Founder of SafeMedia Corporation. Prior to founding SafeMedia, I spent more than 30 years in computer architecture design and software product development. I founded and served as the Chairman of the Board for WIZNET, a business to business ("B2B") e-Commerce content firm and have developed GIS systems for federal and local governments and IBM's IPCS/MAPICS.

My testimony addresses two issues: (1) the privacy risks and other dangers to consumers, students and other users posed by many popular P2P file-sharing programs as outlined by a recent report issued by the United States Patent and Trademark Office; and (2) technology developed by my company to address illegal sharing of copyrighted materials on P2P networks. While I understand that the former is not the focus of today's hearing, I believe it is vitally important that the committee better understands how many popular P2P programs operate as you examine how technology can be used to reduce digital copyright violations on campus.

SafeMedia's mission is to provide an effective, cost-efficient and easily implemented solution for preventing illegal transfers of copyrighted digital material via peer-to-peer networks, and to restore and preserve copyright holders' asset value.

As you know, since 2002, numerous Congressional Committees have addressed illegal piracy on college campuses through peer to peer (P2P) filesharing and the serious privacy and security risks posed by many popular P2P filesharing programs. As early as September of 2002, Congressman Robert Wexler, my home-district Congressman, stated at a hearing before the House Judiciary Subcommittee on Courts, Intellectual Property and the Internet that *2.6 billion songs and 12 to 18 million movies were being downloaded illegally every month.* Perhaps as important as the loss of economic value, is the attendant loss of moral leadership and cultural degradation when intellectual property theft is ignored or even defended.

Starting in March of 2003, the House Government Reform and Oversight Committee held a series of hearings on the threats to privacy and security on filesharing networks. Later that year, the House passed legislation authored by Representatives

Henry Waxman and Tom Davis requiring Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by P2P filesharing. Among Congress' findings in the Waxman/Davis legislation were the following:

> "Peer to peer file sharing can pose security and privacy threats to computers and networks by –
>
> - Exposing classified and sensitive information that are stored on computers or networks;
> - Acting as a point of entry for viruses and other malicious programs;
> - Consuming network resources, which may result in a degradation of network performance; and
> - Exposing identifying information about host computers that can be used by hackers to select potential targets."

The reality and severity of these risks, to those inside and outside of government, remain today and were most recently documented in a U.S. Patent and Trademark Office ("USPTO") report released last month entitled, *Filesharing Programs and "Technological Features to Induce Users to Share"*.[1] Researchers analyzed more than six years of data, claims and counterclaims of five popular file sharing programs. The report addressed whether filesharing programs "deployed features that had a known or obvious propensity to trick users into uploading infringing files inadvertently." The study painstakingly examined "technological features" that "induce" users to "share" copyrighted material. In addition to features such as "share-folder", "search wizard" and "partial-uninstall," such coercive features include: (1) redistribution by default – which causes users to "share" all files that they downloaded; and (2) forced-sharing – which

[1] http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf

compels users to store and share their private folders and documents. which may include copyrighted material such as personal audio files from paid downloads or purchased CD's as well as sensitive personal information located in consumers' "My Documents" folders.

The report also noted that even if a user is sophisticated enough to understand that he or she has become an unwitting participant in pirating, disabling the features is no simple process. In fact, the report warned that software distributors create, "technological barriers" to ensure that "Disabling file sharing…can be very difficult and perhaps an impossible task for all but the most expert computer users."

The Report exhaustively examines how these features were designed and deployed primarily during the period from 2003 to 2006, well after legal actions were being initiated against users. Users, young or older, naïve or experienced, are literally laying open their networks and files once they install a P2P file sharing program. The Report also recounts mounting evidence from security companies, government agencies, and television network investigations, demonstrating the serious security and privacy risks posed by P2P filesharing networks. In one example, "a woman's credit-card information was found in such disparate places as Troy, Michigan, Tobago, Slovenia, and a dozen other places. Her music-downloading application was in fact making readily available her entire 'My Documents' folder to that application's entire P2P audience, 24 hours per day." This example and others like it demonstrate why the U.S. Patent and Trademark Office said, "They [file sharing programs] pose a real and documented threat to the security of personal, corporate, and government data."

The Report carefully avoids blaming distributors of P2P software for deceiving consumers, but noted that available public information made clear that their programs utilized such technological features. Incredibly, the companies whose filesharing software USPTO analyzed have not refuted any of the report's allegations. And in the final analysis, does it really matter to P2P networks users whose identity or taxpayer information is stolen or whose legally obtained music has been illegally distributed without their consent, whether the software designers intentionally meant to harm them or did so by "accident?" The simple fact is that the most popular P2P services cannot thrive without "cooperation" from users sharing their files. If that cooperation cannot be obtained willingly, as the report's analysis shows, it will be obtained through "technological features" that "induce" users to "share."

With my background in computer architecture design and software product development, I became acutely aware of the serious privacy and security risks posed by some P2P filesharing networks and the significant economic losses that are being sustained through illegal file sharing on certain P2P networks. I also recognized that technology could serve as an important part of the solution and so in October of 2003, I came out of retirement to found SafeMedia corporation. I understood that any technological solution had to distinguish between P2P networks that utilize seemingly inadvertent and anonymous file-sharing and services such as BitTorrent which require identification and consent of peers prior to the sharing of files. I set forth a number of additional criteria for a technologically sound solution and determined that any device or program addressing these issues had to:

- protect user privacy,
- provide 100% accuracy with no false positives,
- easily adapt to small or large network environments,
- cause no slowdowns for legitimate network traffic,
- self-correct with no additional administrative burdens to network managers,
- adapt quickly to changes in illegal P2P networks and transmissions,
- install easily, and
- perhaps most important, has to be available at an affordable price.

Mr. Chairman, I am happy to report that after years of hard work, we were able to utilize a combination of breakthrough core technologies to take this effort in a new direction. In fact, our solution will prevent illegal P2P file sharing networks from forming in the first place. We've labeled it "P2P Disaggregator" (P2PD) technology. It can be deployed at end-user sites, either integrated into network devices installed in edge routers/modems or subnet edge routers and concentrators, or as an independent network appliance which I will focus on today.

Our device: "Clouseau" is a network appliance that detects and prohibits illegal P2P traffic while allowing the passage of legal P2P such as BitTorrent and all other internet transmissions. Clouseau is inexpensive and smaller than a phone book – users simply plug it in between the internet and their computer network, and it goes to work. With Clouseau, we have addressed and solved the weaknesses inherent in other technological approaches to this problem:

- No Invasion of User Privacy: Clouseau detection does not invade user privacy, never captures or records user IDs, does not decrypt any traffic, and allows the execution of all current security techniques (Tunneling, SSH etc.). Clouseau never opens packets to determine file legality or illegality. That determination is based solely upon the type of transmission – it never invades user privacy by looking at the content of a file.

- Accuracy: Clouseau is fully effective at forensically discriminating between legal and illegal P2P traffic with no false positives (i.e., identifying another protocol as the targeted protocol) whether encrypted or not. It prohibits sending and receiving all illegal P2P files, and prevents the flow of copyrighted digital files from legal Internet services, DVDs and CDs to P2P networks where they are totally accessible to millions of users to pirate.

- Scalability: With little or no latency and nearly perfect accuracy, Clouseau operates at network speed processing large traffic volumes on the order of several hundred thousands to several million connections at a time (depending on model) with minimal computation expense.

- Robustness: The P2P community is constantly devising new strategies to cloak their activities including launching new protocols, double and triple-layering encryptions, and frequently changing servers. SafeMedia vigilantly monitors all these rapidly changing characteristics. Clouseau is provided with a remotely secure update every three hours ensuring its constant ability to meet these dynamic challenges.

- Network Appliance Advantages: In addition to the above, Clouseau also provides some unique improvements to the appliance model, such as:

  - Lights-Out Management – Clouseau has been designed as a zero-maintenance appliance from the user's perspective. All updates are done automatically and do not require operator/administrative intervention.

  - Network Invisibility – Clouseau operates in a stealth mode when performing P2P filtering. This feature allows the appliance to be completely invisible to attacks that may be launched on the device.

  - Resilient and Self-healing – In the event of physical attack or hardware or software failure, numerous internal fault-tolerant, self-protection measures are in place to protect the device from undesirable changes affecting the appliance's functionality. Should deprecation of the module or corruption of a file system be discovered, Clouseau will self-heal by automatically restoring corrupted files. Clouseau reboots in the event of power loss (in approximately 45 seconds) to ensure system and network security and functionality. Thus, using a combination of resilient operations, self-healing techniques and builtin fail-safes, Clouseau is able to protect itself from multiple types of attacks that may be imposed on it.

- Plug and Play – Clouseau is very easy to install and requires no changes to existing network topology.

How does Clouseau work? I will do my best to explain in layman's terms the following technologies utilized by Clouseau:

- Adaptive Finger Printing and DNA Markers – SafeMedia's filtering system utilizes proprietary finger printing techniques to identify specific P2P clients/protocols. By using these DNA markers, Clouseau® is able to uniquely identify whether a packet is part of a P2P transaction or regular internet traffic. By studying the details in-depth, SafeMedia is able to avoid false-positives.

- Adaptive Network Patterns – Not all protocols can be easily identified with single packets. As such, Clouseau® is able to monitor packet flows and adapt its filtering based on what it has already seen and now sees. This extensible system utilizes a technique called experience libraries.

- Experience Libraries – P2P clients and protocols will change every day. The process of adapting to this change and constantly being updated with the latest knowledge of such clients/protocols is the responsibility of the experience library. SafeMedia's network operations trains these libraries with new patterns and DNA markers and push these new libraries to Clouseau® units out in the field.

- Update – No P2P filtering appliance will function without constant updates. All of the methods described above are constantly evolving and SafeMedia utilizes the Akamai network to push new updates through the internet Using a highly scalable network such as Akamai allows SafeMedia to offload the deployment of updates to a well-established content-distribution network.

Clouseau has been effectively installed for clients in Florida, California, Oklahoma and Texas in a variety of educational and commercial settings. We are currently deployed at Florida Atlantic University. We continue to expand our higher education efforts and hope to announce soon that we will install the product at a number of additional colleges and universities.

As you know some colleges and universities have been reluctant to adopt effective policies to deal with illegal file-sharing. Some cite student privacy as a concern for refusing to stop clearly illegal file sharing, but they need to be challenged with this question: How does it protect student privacy to allow P2P file-sharing services to roam student's computer hard drives for private folders and documents without their explicit permission? I would further ask if there isn't a double standard at work. Colleges and universities fiercely protect their own intellectual property. Why are they so cavalier when it comes to the intellectual property of others?

Mr. Chairman, we welcome the insights and assistance that can be given to this issue by the Science and Technology committee and would be happy to answer any questions you may have regarding Clouseau or the issues that have been raised in my testimony.