# SafeMedia Corp. Tells House Hearing “There Is a Smokescreen of Misinformation About How contaminated P2P Networks Operate”

Submitted by: Mayo Communications
Wednesday, 25 July 2007

---

Washington, DC & Hollywood, Calif. —SafeMedia Corporation CEO and Founder, Safwat Fahmy outlined the dangers and risks of contaminated P2P networks today (Tuesday, July 24, 2007) in his written testimony before the U.S. House Of Representatives Committee On Oversight and Government Reform, at the “Inadvertent Filesharing Over Peer-To-Peer Networks” hearing.

The SafeMedia Chairman focused how P2P networks operate, the features and characteristics of “contaminated” P2P networks. Fahmy also explained in his written testimony how SafeMedia’s technology was developed to address illegal sharing of copyrighted materials on contaminated P2P networks and how it will help to protect consumers, students ,businesses and our national security from the serious privacy, identity theft and security risks.

“In layman’s terms, Peer to Peer networking (P2P) allows individual users to transfer files directly to each other without going through a central server,” Fahmy said. “In the traditional Client/Server model, the client sends requests to the server and the server responds to these requests and acts on them. This is how the popular downloading service “iTunes” operates and this is how "MySpace" and "YouTube" work as well. In contrast, with P2P networks, each computer serves as a peer and functions as a client with a layer of server functionality – the individual peers communicate and exchange files directly with no controls.”

Historically, Fahmy told the Committee hearing, “P2P networks were developed to overcome limitations on bandwidth and processing/storage so arguably there were some benefits to using P2P networking as opposed to the client-server model. But frankly, the historic reasons for developing P2P networks do not exist in today’s world: limitations on bandwidth and processing/storage are easily remedied by clustering many low cost servers and the deployment of wideband fiber to deliver even more powerful performance than P2P networks.”

“P2P technology is clearly a usable, freely available tool for research and education and we support the lawful use of uncontaminated P2P networks,” he said. “The legal and innovative uses of P2P technology highlight the importance of being able to differentiate between legitimate uses of P2P and ‘contaminated’ P2P networks.”

Fahmy also said, “It is no secret that in order to avoid liability for the creation and distribution of a network that allows users to illegally transfer copyrighted material, most popular filesharing networks have no accountability of ownership, contents or participants,”. He pointed to an accurate, in-depth and “no smokescreens” U.S. Patent and Trademark Office (USTPO) report, published in March, which said, “That file sharing programs pose a real and documented threat to the security of personal, corporate, and government data.”
In his closing testimony Fahmy said, “As an experienced computer technologist (35 years), I would never recommend that Congress mandate the adoption of a particular technology to address the vital issues you are examining today. However, I do believe that the only way to protect individuals, companies and the

U.S. economy from the dangers of contaminated P2P including identity theft is for Congress to act decisively on recommending that technical solutions be adopted that eliminate the threat of contaminated P2P."

SafeMedia has developed patent pending business solutions combining P2P Disaggregator technology (http://www.SafeMedia.com) (P2PD (http://www.SafeMedia.com)) and a Digital Internet Distribution Solution (http://www.SafeMedia.com) (DIDS (http://www.SafeMedia.com)) that prevents contaminated P2P networks from indiscriminately accessing users' computers. P2PD is based on many advanced technologies created specifically for network operations, resulting in far higher, scalable processing capacity than the network bandwidth it serves. It utilizes the following technologies:

•Adaptive Fingerprinting and DNA markers: The P2PD library of all P2P clients and protocols is the world's largest and most current library of fingerprints and DNA markers and is updated every 3 hours.

•Adaptive network patterns: Not all protocols can be easily identified with a single set of packets. As such, P2PD is set to monitor packet flows and adapt its technique based on what it has already seen and what it sees now.

•Intelligent libraries: SafeMedia's experience libraries are knowledge-based, created from the actual operations of the subnet, and include specific logic markers in addition to the derived adaptive network pattern analyses.

•Remote update and self-healing: All maintenance actions-updates, integrity checks, sanity validations, system housekeeping, and self-defense are remotely performed through SafeMedia's servers with no delay in network operation.

•No Invasion of User Privacy: P2PD detection does not invade user privacy, does not record and track user IP's, does not decrypt any traffic, and allows the execution of all current security techniques (Tunneling, SSH, etc.).

•Accuracy: P2PD is fully effective at forensically discriminating between contaminated and non-contaminated P2P traffic with no false positives (i.e., identifying another protocol as the targeted protocol) whether encrypted or not.

•Speed: P2PD operates at network speed with little or no latency.

Fahmy also insisted that such solutions would best be achieved without putting any additional burdens on people who use the internet. "At SafeMedia, we believe we have such a solution and I am confident that, in time, the marketplace will show that we have the best technological solution," he said.

--ends--

Editors note:

For media interviews contact George McQuade, MAYO Communications (http://www.mayocommunications.com), 818-340-5300. For more information about SafeMedia Corporation product line visit www.SafeMedia.com or call 561-989-1934.

To hear today's testimony from the U.S. House Of Representatives Committee On Oversight and Government Reform, at the "Inadvertent Filesharing Over Peer-To-Peer Networks" hearing please visit: http://oversight.house.gov/story.asp?ID=1430