

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

|  |   |                     |
|--|---|---------------------|
| Public Notices                           | ) |                     |
|  | ) |                     |
| Comment Sought on Petition               | ) |                     |
| For Declaratory Ruling Regarding         | ) |                     |
| Internet Management Policies             | ) |                     |
|  | ) |                     |
| and                                      | ) | WC Docket No. 07-52 |
|  | ) |                     |
| Comment Sought on Petition               | ) |                     |
| For Rulemaking to Establish Rules        | ) |                     |
| Governing Network Management             | ) |                     |
| Practices by Broadband Network Operators | ) |                     |

**COMMENTS OF SAFEMEDIA CORPORATION**

SafeMedia Corporation ("SafeMedia") hereby respectfully submits these comments in response to two *Public Notices* regarding a Petition for Declaratory Ruling Regarding Internet Management Policies and a Petition for Rulemaking to Establish Rules Governing Network Management Practices by Broadband Network Operators.

SafeMedia is a global technology company that provides effective, cost-efficient and easily implemented network security solutions. SafeMedia's vision is to provide a safe and secure internet experience for all users free from the dangers associated with peer-to-peer (P2P) networks. SafeMedia's network management tools prevent the illegal distribution of copyrighted information and theft of proprietary information over P2P networks. This technology protects the property of copyright content owners while thwarting individual identity theft. The FCC should ensure that broadband network operators have all the tools they need to provide the fastest, safest, and most reliable internet possible without invading a user's privacy.

The internet is a versatile and powerful tool that has revolutionized daily life. The virtually unlimited applications of the internet provide a platform for innovation across today's

economy. While the internet serves as a helpful resource, it is also increasingly a source of dangerous and sometimes criminal activity which can have a significant financial, legal and national security impact on internet users. One such source of danger arises from the use of certain P2P networks.

P2P networks are a product of the late 1990's. Despite the fall of the dot.com era and the demise of Napster, the number of P2P networks and the size of their libraries continue to grow. Researchers from the Tuck School of Business at Dartmouth College estimate that at any given time P2P networks host nearly ten million users worldwide which is double the number of users as were present three years ago.<sup>1</sup> These estimates do not reflect those users who engage in P2P over BitTorrent networks for which data is difficult to obtain.<sup>2</sup> P2P users are not limited to individuals of any particular income, race, sex, or nationality, but are commonly young (29 and under), technologically adept, and interested in music.<sup>3</sup> P2P users are located in small towns or international cities, the living room or the board room, and in the college classroom or governmental offices.

While some P2P users are aware that there are legal concerns associated with unauthorized file sharing, few users know about the additional dangers posed by P2P networks. In 2007, the United States Patent and Trademark Office (USPTO) released a report entitled *Filesharing Programs and "Technological Features to Induce Users to Share."*<sup>4</sup> Jon Dudas, the Under Secretary of Commerce for Intellectual Property, opened the report with the following statement:

---

<sup>1</sup> M. Eric Johnson *et al.* *The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users*, IEEE Computer Society, p. 2 (Jan.7, 2008) (Proceedings of the 41st Annual Hawaii International Conference on System Sciences) available at <http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750383.pdf>

<sup>2</sup> *Id.*

<sup>3</sup> *Id.* at 5.

<sup>4</sup> Thomas D. Sydnor II *et al.* *Filesharing Programs and "Technological Features to Induce Users to Share,"* United States Patent and Trademark Office (November, 2006), available at [http://www.uspto.gov/web/offices/dcom/olia/copyright/oir\\_report\\_on\\_inadvertent\\_sharing\\_v1012.pdf](http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf).

Filesharing programs threaten more than just the copyrights that have made the United States the world's leading creator and exporter of expression and innovation: They also pose a real and documented threat to the security of personal, corporate, and governmental data.<sup>5</sup>

This report found that five of the most popular P2P programs included a combination of up to five features that induced P2P users to share documents - often without the users explicit knowledge.<sup>6</sup> Despite scrutiny of these features by governmental agencies and independent researchers and the adoption of the "Code of Conduct"<sup>7</sup> by P2P networks, little has changed to limit the vulnerability of P2P networks and the amount of illegal activities they generate.

The 2007 USPTO report was more than a mere intellectual exercise. Software designs incorporated into P2P software that promote file sharing have made P2P networks an attractive financial environment for criminal activity. By inducing (or "duping") users into sharing files inadvertently, P2P networks create the capability for confidential and proprietary information to find its way onto the network. Once the information is leaked onto P2P networks, it is available for anyone to download and can never be recovered or removed. The vulnerability of P2P networks became apparent in November, 2006 when eight individuals were indicted in Denver, Colorado for stealing the identity of P2P users over the popular network LimeWire.<sup>8</sup> These individuals were able to secure over \$70,000 which was used to purchase methamphetamines and retail goods for personal use.<sup>9</sup> Then again in September, 2007, when a Seattle, Washington man was indicted for individual identity theft after stealing personal identification information from tax returns inadvertently shared without the user's knowledge or permission on P2P

---

<sup>5</sup> *Id.* at i.

<sup>6</sup> *Id.* at 1-4.

<sup>7</sup> Available at <http://wiki.morpheus.com/~p2punitied/code.php>.

<sup>8</sup> Press Release, Denver District Attorney Mitchell R. Morrissey, *Id Thieves Charged in 115-Count Indictment* (Nov. 30, 2006) available at [http://www.denverda.org/News\\_Release/Releases/2006%20Release/Sarrasin,%20Adams%20and%20Stesney%20in%20dictment.pdf](http://www.denverda.org/News_Release/Releases/2006%20Release/Sarrasin,%20Adams%20and%20Stesney%20in%20dictment.pdf).

<sup>9</sup> *Id.*

networks.<sup>10</sup> To test the vulnerability of a P2P network, the Tuck School of Business researchers placed actual credit card and phone card information on a P2P network to track the use of confidential information shared via P2P.<sup>11</sup> Within one week, the balance on the credit card was fully depleted and within two weeks the phone card minutes was depleted on internationally based phone calls.<sup>12</sup> Because it is often difficult to determine the exactly where proprietary information is taken, it is likely that the theft of such information over P2P networks is even more widespread than is currently known.

A broadband network operator has a significant obligation to provide its users with the fastest, safest, and most reliable internet possible. In doing so, the broadband network operator should never invade a user's privacy by engaging in deep packet or deep flow inspection. Each broadband network is designed differently and requires broadband management tools that are tailored to its network. For instance, the Federal government must have the ability to share documents efficiently amongst governmental units while, in many cases, strictly prohibiting access from any other party. Similarly, businesses must be equipped to promote coordination amongst its units, but often may engage in close inspection of the content of material that comes in or out of its network. Alternatively, universities typically manage their network to promote the free exchange of ideas, but will often monitor the way its bandwidth is distributed to best manage its allocation to where there is the most need.

Additionally, internet service providers (ISPs) have a significant broadband traffic management issue that requires unique management tools to ensure each consumer is adequately serviced. ISPs generally use a border gateway protocol (BGP) to manage traffic on their

---

<sup>10</sup> Indictment, United States District Court for the Western District of Washington at Seattle, *United States v. Gregory Thomas Kopiloff* (Sept. 5, 2006) available at <http://seattlepi.nwsource.com/dayart/pdf/kopiloffindictment.pdf>.

<sup>11</sup> M. Eric Johnson *et al*, *supra* note 1, at 7.

<sup>12</sup> *Id.*

network. Most P2P systems, however, implement their own routing on top of the Internet in the form of an overlay network. In most cases P2P routing is no longer done on a BGP basis; rather queries are disseminated by flooding, random walks in unstructured P2P networks, or a distributed hash tables (DHT)-based routing system. This creates two independent routing systems: the P2P overlay and the ISP's routing system. If the ISP changes its routing (e.g. for traffic engineering reasons) the P2P system may in turn adapt its overlay, thereby changing the assumptions underlying the traffic engineering decisions. If the P2P overlay changes its network, it impacts the traffic flow, which may cause the ISP to change its routing, which in turn may cause the P2P overlay to change its network yet again. Hence, the two routing systems currently can be viewed as competitors.<sup>13</sup> Each of these broadband networks has unique concerns about the risks and liabilities created by the use of P2P networks on their system. SafeMedia technology assists broadband network operators and users of the internet to successfully manage those risks.

SafeMedia technology is designed to prevent harmful applications on a covered network. SafeMedia technology blocks only P2P applications that engage in the unauthorized transfer of copyrighted information or are designed in a way that "dupes" the user by undermining their or the network operator's intent. SafeMedia protects the value of copyrighted data by preventing P2P networks that engaged in the unauthorized exchange of copyrighted materials. Several common P2P programming designs, like automatic redistribution, coerce users to inadvertently share files without notice to the user through features. These files may contain copyrighted, confidential, or classified information. Additionally, the use of overlay routing by P2P networks

---

<sup>13</sup> John Kubiawicz, *Extracting Guarantees from Chaos*, Communications of the ACM, Vol 46, No. 2, at 33-38 (Feb. 2003) available at <http://oceanstore.cs.berkeley.edu/publications/papers/pdf/CACM-kubiawicz.pdf>; Thomas Karagiannis et al., *Transport Layer Identification of P2P Traffic*, Microsoft Research Program (Oct. 25-27, 2004) available at <http://research.microsoft.com/%7Eethomkar/papers/imc04.pdf>; Norton, William B., *The Evolution of the U.S. Internet Peering Ecosystem* (Nov. 19, 2003) available at <http://www.equinix.com/pdf/whitepapers/PeeringEcosystem.pdf>.

can frustrate traditional BGP routing on a network, slow the network and increase the costs to the ISP and end users. SafeMedia technology blocks these P2P networks without engaging in deep packet or deep flow inspection or invading user privacy. SafeMedia's network management systems are currently deployed and operating successfully in schools such as Pine Crest Preparatory School, law offices such as Kain & Valisky, PA, and in public accounting firms such as KMC in Fort Lauderdale, FL.

In consideration of the significant dangers posed by the internet and the unique interests of broadband network, the FCC should ensure that its actions give broadband network operators access to the broadest range of management tools. At the same time, the FCC should ensure that broadband network operators maintain user's privacy by not engaging in deep packet or deep flow inspection. This will allow broadband network operators to provide the fastest, safest, and most reliable internet possible without sacrificing the privacy of its users.

Thank you for your consideration of our comments to these two Public Notices.

Respectfully submitted,

SAFEMEDIA CORPORATION

\_\_\_\_\_/S/\_\_\_\_\_

Safwat Fahmy  
SafeMedia Corporation  
6531 Park of Commerce  
Suite 180  
Boca Raton, FL 33487  
Tel: (561) 989-1934  
E-mail: safwat.fahmy@safemedia.com