EXHIBIT A-7

does not appear to be true.[36] After a content owner has gone through the process of submitting information about the file he wishes to protect, Lime Wire LLC leaves it up to the user to turn Enable Content Filter on! So no protection is afforded unless the user specifically directs the program to do so. In my experience, moreover, most users will not alter default settings. Thus, Lime Wire LLC's choice to default this filter to "OFF" means that most users will never even enable it.

98. An examination of the LimeWire source code[37] shows that when "Enable Content Filter" is turned on and a download is initiated: (i) a LimeWire file sharing application retrieves the IP address of the machine and the hash of the file to be downloaded, (ii) it then sends a request to a server run by Lime Wire LLC (fserv1.limewire.com located at IP address 76.8.67.4); and (iii) the source code indicates that a response is expected.

99. To test the effectiveness of Lime Wire LLC's Content Filtering system, I ran two experiments, which are described fully in Exhibit C. According to reports in the LimeWire Blog (http://www.limewire.org/blog/?p=206) and in TorrentFreak (http://torrentfreak.com/limewire-to-filter-out-adobe-products/), both published in November on 10-11, 2006, Lime Wire LLC has agreed to filter copies of Adobe products, in particular Adobe Photoshop. Summarizing my experiment, I started a packet sniffer called WireShark on my computer. The packet sniffer monitors network traffic to and from my machine. Next I started LimeWire and set content filtering to ON. I then did a search for Adobe Photoshop, received a set of results, selected several results for downloading, and then installed one fully

[36] See http://www.limewire.com/about/copyright.php.

[37] See https://www.limewire.org/fisheye/browse/limecvs/core/com/limegroup/gnutella/messagehandlers/InspectionRequestHandler.java (v 1.15) and https://www.limewire.org/fisheye/browse/limecvs/core/com/limegroup/gnutella/settings/FilterSettings.java (v 1.20).

downloaded copy of PhotoShop on my machine to verify that the downloaded software was actually Adobe Photoshop, which it was. Examining the WireShark results, I observed that the LimeWire application did contact fserv1.limewire.com:10000 for *each* of the download attempts, and it sent the associated SHA-1 value of the Adobe Photoshop file I was attempting to download, but when I ran this experiment in July 2007 there was no response from fserv1.limewire.com, despite initiating seven downloads. I repeated this experiment multiple times over a period of a month, even for downloaded content other than Adobe Photoshop, with the same results.

100. In February 2008, I re-ran my experiment, searching for copies of the program Adobe PhotoShop, and I observed a response from fserv1.limewire.com for each download. The second part of Exhibit C shows the results. Of the five downloads that I attempted, three were successful, but two were blocked by LimeWire using the message "Content Removed." The experiment also points out, however, the ineffectiveness of using the SHA-1 value to determine if a file is authorized as the filtering failed to eliminate the three successful downloads.

101. A hash is a property of a particular digital file, not of a work. When a master copy of a music file is created by the content owner, that file may be used to create the commercially sold CDs. However, anyone may "rip" the music off of the CD, and depending upon the ripping software and various options such as bitrate, a new file *with a new file hash*, is created. As a result, if the content owner submits a master music recording's file hash to a P2P software company for filtering, the file hash of the master recording is not likely to be present on the P2P network. Moreover, there may be many different versions of

the ripped musical work, each with a different hash. It is not unusual to find dozens or more different files available in LimeWire search results for a hit single.

102. Restating, the futility of using file hashes to screen for unauthorized content becomes clear when one considers that a single song may have any number of SHA-1 file hashes depending upon how the song's file was created. To take an example, I selected the song entitled "Californication" from the album (CD) of the same name of an album that I own by the Red Hot Chili Peppers.[38] Using an Apple MacBook Pro running Mac OS X and a Toshiba laptop running Windows XP, I ripped the song off of the CD. I varied the bitrate and computed the resulting SHA-1 file hashes. The table below summarizes the results.

Platform	Rip Application	Codec	BitRate	File Size	File Hash[39]
Mac OS X	iTunes 7.4.2	AAC	128kbps	5MB	YP2NE2REOBQRJOJZADDS NUNWDLUYAD3B
Mac OS X	iTunes 7.4.2	Apple Lossless	993kbps	32MB	WKZMHCZ2LAYRR3IRNRZ W5SHZ6TDHCGD7
Mac OS X	iTunes 7.4.2	MP3	160kbps	6.2MB	4QYYGII5SRGMFGIPF5G7R VCRP6QQYOQJ
Mac OS X	iTunes 7.4.2	MP3	192kbps	7.4MB	3FQFPSZ3YKZ6V4FFEEUJH2 MH6T66LIFU
Mac OS X	iTunes 7.4.2	MP3	256kbps	9.9MB	IT5D6J6SWFKFWU2XDUKF OSQ5NVUJ7C6M
Windows XP	Win Media 10.0	WMA	128kbps	4.9MB	X2CHSCB4H4AZ52NJR3GMH DTW6NHRRQXR
Windows XP	Win Media 10.0	WMA	192kbps	7.4MB	5O6VUJAW777CPKHIYDYG5 GG3GIO4YY3F
Windows XP	Win Media 10.0	MP3	192kbps	7.3MB	M4PFR2WO6NKMJH2ANUS3 CWYEEUS6S7CV
Windows XP	Win Media 10.0	MP3	256kbps	9.8MB	VJDSVN343ZCGP7JBD3CUK NQOZD675MEZ

Table 2: File Hashes for the Song Californication Produced Using Multiple Methods

[38] See for example http://www.amazon.com/Californication-Red-Hot-Chili-Peppers/dp/B00000J7JO.

[39] The SHA-1 encodings are displayed using Base32 notation, see http://tools.ietf.org/html/rfc4648.

103. As revealed in the table, different methods for producing the file have yielded totally different SHA-1 hash values. Using a file's hash alone as a method of filtering unauthorized works is woefully inadequate.[40] Since LimeWire users can continuously upload new versions of music files, using the file's hash for filtering unauthorized works will inevitably prove to be ineffectual.[41]

E. *Lime Wire LLC has failed to implement an effective filter for unauthorized works*

i. Effective Filtering Methods Currently Exist

104. Other P2P companies, such as iMesh and Kazaa, have implemented effective filters for unauthorized works without negatively affecting performance. These filters rely primarily on acoustic fingerprinting and are supplemented by hash and keyword filtering.

105. Content-recognition filtering is based on recognizing the unique content of an underlying audio-visual work and detecting and preventing copying of that content no matter how the file containing the content was created (e.g. whether the file was ripped from a CD, DVD, or recorded from a radio or television, etc.). Commercial vendors now offer services and/or software that identify files according to a database of unauthorized

---

[40] Notably, Lime Wire LLC itself appears unwilling to rely on its hash-based filtering system to protect its content. Recently LimeWire LLC has opened up an online store they call LimeWire Store, located at http://www.store.limewire.com/store/app/pages/Home . The website claims that all songs for sale are Digital Rights Management (DRM)-free and in mp3 format. According to testimony by Sam Berlin [252:4-5, 257:9-261:18], LimeWire is branding all music purchased at the store with an indicator of its own creation, called the magic string. The presence of the magic string causes the mp3 file to be logically placed in a separate folder that makes the file non-sharable by the LimeWire file sharing application.

[41] Moreover, even if a content owner were to attempt to locate and notify Lime Wire LLC of all unauthorized copies, there would still be a period of time during which those copies would not be blocked.

content, e.g. Audible Magic (http://www.audiblemagic.com/index.asp) and Gracenote (http://www.gracenote.com/).

106. One salient feature of content-recognition filtering is its accuracy – it works by identifying only those specific works whose fingerprints have been stored in a database. It does not attempt to block any other works. Moreover, content recognition filtering does not rely on what a user has chosen to name a file, or the bitrate at which the file has been encoded – the underlying content is examined. Audible Magic claims a correct identification rate of unauthorized audio files of above 99% for its content recognition filter that relies on digital fingerprinting.[42]

107. Audible Magic offers to license its software to P2P developers. It provides an SDK (software development kit) that

> "enables P2P software networks to quickly and accurately generate information needed to lookup the identity of the content in an Audible Magic central server. The solution consists of a software API library, content identification and link services, and an information data service. The approach is highly accurate and requires no dependence on metadata, watermarks or file hashes."[43]

108. Acoustic fingerprinting can be – and is – used to filter unauthorized audio files, by peer-to-peer systems like iMesh and Kazaa. In declarations, Benjamin Sorensen and Talmon Marco, both submitted in *MGM v. Grokster*, CV 01-08541, state that Audible Magic's acoustic filtering software has been successfully applied. Sorenson discusses the experience of the Kazaa software, saying, "the Audible Magic technology can

---

[42] See http://www.audiblemagic.com/products-services/replicheck/why.asp and Declaration of Vance Ikezoye, *MGM v. Grokster*, CV 01-08541.

[43] See http://www.audiblemagic.com/products-services/custom/ and http://www.audiblemagic.com/products-services/contentsvcs/.