

Music in the Cloud— A Business and Legal Primer

BY DAVID M. GIVEN

WHAT IS CLOUD COMPUTING?

A simple definition of cloud computing is a hosted service providing scalable access by a computer user to personal computer files remotely stored on one or more host servers. The benefit of cloud computing is said to be primarily twofold: First, it allows a user to access files, together with computing resources and information technology (IT) services, without “high demand” on his or her computer’s hardware and software; and second, if the service permits, it allows a user to have access to those files anywhere, anytime, and from any platform device.

As recorded music can, of course, be reproduced and stored in a computer file (MP3 being the most common format for that purpose), the current development of cloud services promises a transformation in the way consumers access music. Portability, accessibility, and interoperability are the touchstones of that expected transformation.

Currently, consumers download music files (lawfully or not) onto their computers or other playback devices, where the file is stored on the device’s hard drive. To transfer the music to another device, the file must either be burned onto a CD, put onto a flash drive, e-mailed, or one device must be synced to the other via a cable or other direct connection.

With cloud music services, entire music libraries can be stored in and mobilized from the cloud (in a variety of fashions, depending on the service), and a user can listen to music in his or her library from any device without performing any syncs or transfers. The cloud therefore promises, among other things, to allow unlimited access to music in the form of on-demand streaming and offline listening, while saving time and computer space.

WHAT ARE THE LEGAL ISSUES?

Music in the cloud will change how the public acquires, stores, and accesses music. Its expected benefits to the consumer pose potential threats to artists and record labels, however. In addition to the potential to further shift public perception away from the idea of music as a good (as opposed to a service), cloud computing raises several distinct legal and public policy issues—among them, copyright infringement, music piracy, user privacy, and system security.

Copyright Infringement

Generally, copying a work without permission violates the exclusive reproduction right of the copyright owner. The transfer of a music file from one device to another may violate that right and also be a violation of the copyright owner’s exclusive right to distribute his or her copyrighted work. The issue here is whether music service providers or users have the right to reproduce owned or licensed content when transferred from its original form to a digital file in the cloud.

Direct Infringement. Music service providers and users may be directly liable for making copies of music files without permission.

Public Performance Rights. Streaming an unauthorized copy of a song using a “master copy” of the song through a device may violate a copyright owner’s exclusive public performance rights. In *Capitol Records, Inc. v. MP3tunes, LLC*, No. 07 Civ. 9931, 2011 WL 5104616 (S.D.N.Y. Oct. 25, 2011), EMI Inc., along with 14 other record companies and music publishers, sued MP3tunes, alleging vicarious, contributory, and direct copyright infringement. With respect to direct infringement, EMI argued that MP3tunes violated its public performance rights by employing a “master copy” to rebroadcast songs to users who uploaded different copies of the same recording. The court, however, found that MP3tunes employed no such master copy and therefore was not found liable for direct infringement.

Reproduction Rights. A copy of the music file is made when it is uploaded into the cloud. Another copy of the music file (arguably, ephemeral) is made when it is downloaded from the cloud. Since the exclusive right of reproduction of a copyrighted work is potentially implicated in both the uploading and downloading of such works, parties who play a role in those transactions (i.e., the users and service providers) may be liable to the copyright owner for infringement where the underlying copy of the work is unauthorized. See *Capitol Records, LLC v. Redigi Inc.*, Southern District of New York Case No. 12-CV-95 (RJS) (preliminary injunction denied; however, finding of likelihood of success in case in which, according to plaintiff, uploading of digital copies constitutes “reproduction” under Copyright Act).

As will be seen below, the Digital Millennium Copyright Act (DMCA) gives protection to certain infringing conduct. However, it is not altogether clear to whom that protection extends, and under what circumstances, in the cloud. A user is probably unprotected, and has liability for direct copyright infringement. A service provider might avail itself of the so-called DMCA “safe harbors,” and therefore insulate itself from damages and other remedies for direct or indirect copyright infringement. But that will be the case only if the service provider carefully considers and implements its policing and other obligations under the DMCA. Moreover, given the newness of the technology, certain uses of it may expose the service provider to liability notwithstanding those statutory safe harbors.

Indirect Infringement. Service providers may be indirectly liable for the direct infringement of a third-party user.

Contributory Infringement. Record labels and music publishers may argue that cloud computing service providers are liable for contributory infringement. A service provider generally will be held liable for contributory infringement if: (1) there was direct infringement by a third party, and (2) the service provider knew of and materially aided the infringement. Accordingly, once a cloud music service is put on notice that its service provides access to unauthorized copies of works, it must disable

access to the material to avoid liability for contributory infringement altogether. The seminal case on the subject remains *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), which held that the sale of copying technology is not contributory infringement if the product sold is capable of substantial noninfringing uses. In that case, Sony was found not liable for copyright infringement because the making of individual copies of complete television shows for the purpose of time-shifting was deemed fair use.

In the *MP3tunes* case, the court granted EMI's motion for summary judgment as to its contributory infringement claim. The court found that MP3tunes knowingly and materially aided its users' copyright infringement by continuing to store such content even after receiving EMI's takedown notices. While MP3tunes did remove the links to infringing content on third-party sites to avoid contributory liability, MP3tunes also needed to delete the actual infringing files from individual users' accounts. The court also rejected MP3tunes' argument that its cloud service was capable of substantial noninfringing uses on the grounds that MP3tunes continued to have an ongoing business relationship with the infringing users even after being made aware of their infringement.

Vicarious Infringement. A cloud service provider will be vicariously liable for the actions of an infringing user when the provider: (1) has the right and ability to control the infringer's acts, and (2) receives a direct financial benefit from the infringement. Unlike contributory liability, the provider need not have knowledge of the infringement. The revenue that the providers receive from users for cloud services will likely be considered a direct financial benefit because consumers may be attracted to the service by the existence and availability of the infringing works.

Inducement. In *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), a peer-to-peer direct file-sharing case, the Supreme Court considered an inducement theory of infringement. The court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties." Cloud service providers that purposefully encourage copyright infringement by promoting the transfer of unauthorized copies of music files may therefore be liable for inducing infringement.

Defenses to Copyright Infringement

Digital Millennium Copyright Act (DMCA). The DMCA provides a safe harbor for service providers. Liability for copyright infringement is limited if: (1) a third party initiates or requests transmission of copyrighted material, (2) the service provider does not select the material, (3) the service provider does not select recipients of the material, (4) the service provider does not retain copies of the material, and (5) the service provider transmits material through its system without modification of its content. In *MP3tunes*, the court found that MP3tunes was protected for the most part under the DMCA. Although the court found that one of the alleged actions (allowing users to "sideload"—i.e., to copy songs directly from a third-party site to the user's MP3tunes locker) was not protected by a DMCA safe harbor, this ruling will likely foster confidence

and encouragement for the cloud as long as cloud music service providers adopt and reasonably implement compliant notice and takedown procedures. If the providers are eligible for immunity, indirect infringement claims will most likely be moot.

Fair Use. In determining whether the use made of a work in any particular case is fair use, the factors to be considered include: (1) the purpose of the use, (2) the nature of the work, (3) the amount and substantiality of the portion used, and (4) the impact of the use on the actual or potential market. Uploading for the purpose of distribution and sale is not defensible as fair use; however, uploading for personal use likely will be. Although the entirety of the music file is copied, the impact of copying for personal use arguably has little to no impact on the market because the user has already purchased the work.

Piracy

The advent of cloud music services has the potential to encourage music piracy by allowing users to upload their entire music libraries, including pirated music, into the cloud. Realistically, many music files probably landed in a user's library through illegal downloading. Cloud music services therefore allow for the transfer of pirated files into the cloud. Apple and other cloud music services that have licensing agreements with record labels have found a way to essentially require users to retroactively pay for their pirated music. With a license agreement in place, record labels receive a percentage of the revenue made from users paying for the cloud service. Users who are willing to pay for space in the cloud are basically paying back record labels for the tracks they have already illegally downloaded.

Licensing

Without licensing agreements, the cloud opens up the possibility of illegal sharing and distribution of music files. The reproduction, distribution, and public performance of unauthorized music could be subject to violation of the copyright holder's exclusive rights. Amazon Cloud Drive allows users to mobilize their music library by uploading their files into the cloud. Amazon first launched its service without obtaining license agreements with record labels. Amazon reasoned that its users already owned the music they stored in their library and there was no need to obtain a license agreement. However, since Amazon makes money from users uploading songs into Cloud Drive, record labels want royalties and will not receive anything without a license agreement. Public reports suggest that Amazon is now working on obtaining retroactive licenses with record labels.

User Privacy

Cloud computing presents potential privacy issues because users generally must consent to the service provider accessing their files. For example, Amazon Cloud Drive Terms of Use section 5.2 "Our Right to Access Your Files" states:

You give us the right to access, retain, use and disclose your account information and Your Files: to provide you with technical support and address technical issues; to investigate compliance with the terms of this Agreement, enforce the terms of this Agreement and protect the Service and its users from fraud or security threats; or as we determine is necessary to provide the Service or comply with applicable law.

What types of cloud music services are available?

Music Service Provider	Platform	Allows User's Own Music	Mobile Offline Listening	Auto Sync	Storage Space	Price
iTunes Match	iOS; Web-based computer with iTunes	Yes	Yes	Yes	25,000 songs	Free for iTunes music; \$24.95/year for non-iTunes music
Amazon Cloud Drive	iOS (via Cloud Player Website); Android; Web-based computer	Yes	Yes (Android only)	Yes	Up to 1000GB	Free for 5GB then \$1/GB/year
Google Music	iOS (Google Music web application); Android; Web-based computer	Yes	Yes (Android only)	No	25,000 songs	Free (while in Beta)
SoundCloud	iOS; Android; Web-based computer	Yes (recording and uploading originally-created music)	Yes (if creator allows his or her sound to be downloaded)	No	Unlimited upload minutes	Free for 120 upload minutes; up to \$740 for unlimited
MP3tunes	iOS; Android; Web-based computer; PlayStation 3; Xbox 360; TiVo	Yes	No	Yes	Up to 200GB (about 40,000 songs)	Free for 2GB (about 400 songs)
Murfie	Web-based computer	Yes (user mails CDs to Murfie to be transferred into the cloud to sell or trade)	Yes	No	1,000 CDs	\$1/CD or \$24/year

As a result, the users of Amazon Cloud Drive potentially may be subject to the exploitation of their personal information by Amazon. A second, more serious, privacy issue presents itself if users are able to access the files of other users. Users' files are uploaded into the cloud where unknown users may potentially have the ability to access personal files. By uploading files into the cloud, users risk the privacy interest in those files.

System Security

Security breaches, glitches, and bugs in electronic services happen. In June 2011, a consumer class action lawsuit was filed against Dropbox when a glitch in the service allowed login access to millions of Dropbox accounts using any password. (On October 18, 2011, the Dropbox litigation was terminated by the filing of a notice of voluntary dismissal. See *Wong v. Dropbox, Inc.*, Northern District of California Case No. 11-CIV-3092.) When uploading personal files into the cloud, users should be willing to risk flaws in security, and should probably be warned accordingly.

International Jurisdiction

By nature, copyright law is territory specific. The cloud reaches globally, and rights in the same work may fall under different jurisdictional laws. For example, as a result of the restrictions of U.S. and international copyright law, Pandora Radio blocks access to non-U.S. listeners. In Canada, Canadian copyright law applies to transmissions that have a "real and substantial connection to Canada." In analyzing copyright issues, the European Union (EU) looks at where the transmissions were emitted and where they were received. Clearance in the EU must be obtained on a territory-by-territory basis via a license from the collective rights management organization of each country. U.S. copyright law may apply as long as either the communication originates in the United States or the content is received in the United States. As a result, without international copyright agreements (or treaties), jurisdictional distinctions of copyright law theoretically prevent music from streaming internationally. (See David M. Given, *A Modern Pandora's Box: Music, the Internet, and the Dilemma of Clearing Public Performance Rights*, 26 Ent. & Sports Law. 1 (2008)).

CONCLUSION

The development of cloud computing will likely be driven by several factors beyond the legal issues discussed here. User preferences and business priorities will greatly influence the evolution of the cloud. The cloud era has and will continue to face challenges in balancing the economic interests of parties involved together with the legal implications of those interests. The law should ultimately adapt to innovations such as cloud computing, but legal precedent can be hard to move sometimes.

The cloud has introduced a new level of convenience, flexibility, and ease of use for the consumer. Delays in adapting current law to the cloud era may impede the success of this technology. Lawyers should therefore be prepared to address these issues. ❖

David M. Given is a partner with Phillips, Erlewine & Given LLP in San Francisco, California. A version of this article was presented at the 2012 South by Southwest Music Conference. He wishes to thank his intern June Quan for her research assistance. Mr. Given can be reached at dmg@phillaw.com.