Intellectual Property

2011 FALL BULLETIN

MP3.com Redux? Music Venture's Model Survives Copyright Challenge as S.D.N.Y. Provides Guidance for Cloud-Based Services

BY MITCHELL ZIMMERMAN

A decade ago, when what would later be known as "cloud" services began to darken the skies of music copyright-holders, and mobile devices were in their adolescence, entrepreneur Michael Robertson launched a business that provided users with access to "their" music anywhere they could get online. The venture was soon crushed in copyright litigation brought by leading record labels. *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

About five years later, Robertson founded MP3tunes.com, offering a range of services that, similarly, allow end users to access music from anywhere – and to locate and store any "free" music to be found on the Internet. This time around, the same district court has upheld the basic business model of the venture against copyright challenges. The decision in *Capitol Records, Inc. v. MP3tunes LLC*, 07 Civ. 9931, 2011 U.S. Dist. LEXIS 93351 (S.D.N.Y. Aug. 22, 2011), *appears* to provide important guidance and support for other entities seeking to provide cloud services.

MP3.com and MP3tunes used different methods for putting music online. MP3.com ripped songs from tens of thousands of CDs it had purchased, loaded them onto its servers, and then streamed the songs to users who had previously purported to prove they already owned the same CDs by putting a corresponding CD into a computer connected with www.mp3.com. Using different means, MP3tunes lets its users select and store music in the cloud, then play it back or download it wherever they are.

The record labels said it made no difference that MP3tunes used different means for collecting the music its users access. However, in *Capitol Records, Inc. v. MP3tunes, LLC,* the district court, granting in part and denying in part the plaintiffs' and the defendants' cross motions for summary judgment, wound up agreeing with MP3tunes on most of the Digital Millennium Copyright Act (DMCA) safe harbor issues, and particularly on those points critical to the MP3tunes business model. Among the key conclusions that lend further support to the cloud storage model, the court held that the service provider was not liable for copying — at the direction of its users — infringing music files found on third-party sites to its own servers and streaming infringing music to its users, provided it observed the requirements of the safe harbor.

How MP3tunes Works

Music gets stored in an end user's online storage "locker" in one of three ways. First, a user can upload music files from their computer. Second, if the user knows the address of a music file that is available anywhere on the Internet, they can use an MP3tunes feature, known as Webload, to copy the file to their locker. Third, if the user neither possesses a copy of a song on their computer nor knows where it can be found on the Internet, they can search for the song at Sideload.com, another website owned by MP3tunes. With a click, they can send a copy of a song located by the Sideload search engine from the third party site into their locker. Users can also employ a Sideload plug-in to copy into their lockers any

In This Bulletin

MP3.com Redux? Music Venture's Model Survives Copyright Challenge as S.D.N.Y. Provides Guidance for Cloud-Based Services ____ 1

The Stored Communications Act: A Statute Long Overdue for a Tuneup ____ 4

Second Circuit Upholds Gray Market Importation Bar and Negates First-Sale Doctrine for Works of Authorship Made Overseas ____ 7

Quick Updates ____ 9

Judge to Oracle: Bye-Bye Billion ____ 9

ICANN to Make New Internet Domain Namespace Available to Brand Owners ____ 9

Judge Sparks Orders Patent Office to Expedite Reexaminations, but Has a Sudden Change of Heart ____ 10

Posting Trade Secrets ____ 11

Fenwick
FENWICK & WEST LLP

free music file they come across on the Internet without being on the Sideload.com website. MP3tunes keeps track of the specific, sometimes-different sources of each user's copies of stored songs.

Songs from the user's locker can either be played (streamed) or downloaded to the user's Internet-connected computer or mobile device. When different users put an identical music file from the same source into their lockers, it appears that MP3tunes does not permanently store multiple full copies of the same song.

Although the operation of the MP3tunes technology is not entirely clear from the court's discussion, it apparently uses an automated system to create a "hash" tag (a unique, automatically-generated code used to identify a file comprised of specific bits of data). If the hash matches a file already stored by another user, after an automated de-duplication process, the new copy of the earlier-uploaded song is deleted, and the later user's locker is populated with the hash rather than another copy of the same file. When that user requests to play the song, the system generates the version of the song from the hash tag – using the file stored by the first user. Assuming this understanding is correct, the term "locker" would be a metaphor, since MP3tunes does not actually allocate to each user a unique area of server space on which is stored each user's own distinct copy of "their" content, as the defendant did in *Cartoon Networks LP, LLLP v. CSC Holdings, Inc.* 536 F.3d 121 (2nd Cir 2008). (For the sake of simplicity, we will nonetheless refer below to "copies" in end-users' lockers.)

Repeat Infringer Policy Upheld

Leading record companies sued MP3tunes for copyright infringement, and all parties moved for summary judgment. The record labels asserted *inter alia* that MP3tunes was not protected by the safe harbors of the DMCA and was directly and secondarily liable for copyright infringement. The court addressed several key issues under the DMCA, beginning with the repeat infringer policy.

Safe harbor eligibility requires that the website adopt and reasonably implement a policy of terminating the accounts of repeat infringers in appropriate circumstances. 17 U.S.C. § 512(i)(1)(A). In the court's view, the key issues were whether the online service terminates "blatant" infringers, and whether the service purposefully fails to keep adequate records of the identities and activities of its users.

In a novel approach, the court distinguished between the "typical" "blatant infringer" — who knowingly uploads copyrighted matter for the world to copy or use — and lesser infringers who merely copy for their own use:

> There is a difference between users who know they lack authorization and nevertheless upload content to the Internet for the world to experience or copy, and users who download content for their personal use and are otherwise oblivious to the copyrights of others. The former are blatant infringers that Internet service providers are obligated to ban from their websites. The latter, like MP3tunes users who sideload content to their lockers for personal use, do not know for certain whether the material they are downloading [from third party sites] violates the copyrights of others.

Consistent with this distinction, the court approvingly noted that MP3tunes had "terminated the accounts of 153 repeat infringers who violated copyrights by sharing the content of their lockers with other users." The court was silent as to whether there were circumstances requiring that those storing infringing songs for personal use be terminated as repeat infringers.

MP3tunes also did not purposefully blind itself to its users' identities and activities. Rather, the company tracked the source of all sideloaded songs and could identify and terminate repeat infringers. Its implementation of its repeat infringer policy was therefore sufficient for safe harbor eligibility.

Inadequate Compliance with Takedown Notices

Under the DMCA, a request that infringing matter on a web service's website be taken down must identify the infringed work and specify the URL where it can be found on the service's website, so as to enable the service to easily locate the file. The record companies argued that it was sufficient for them to specify the web addresses for the infringing links on Sideload.com, since MP3tunes could then readily identify all the lockers "containing" copies of the infringing work obtained via that link. In a decision of first impression, the court agreed that MP3tunes had to not only disable the infringing links specifically identified as available at Sideload.com, but also delete the copies of the music files made from those links, contained in users' lockers:

> Where service providers... allow users to search for copyrighted works posted to the Internet and to store those works in private accounts,... those

> service providers must (1) keep track of the source and web address of stored copyrighted material, and (2) take content down when copyright owners identify the infringing sources in otherwise compliant notices.

Since, in response to the takedown notices, MP3tunes merely removed the links from Sideload.com, but failed to delete the infringing copies already stored in user lockers, this meant that MP3tunes' response was inadequate for safe harbor protection.

Consistent with prior decisions, the court held this did not mean that MP3tunes was obliged to search for and take down *all* of the record companies' content on the companies' theory that their notices were a representative list. "Absent adequate notice, MP3tunes would need to conduct a burdensome investigation in order to determine whether songs in its users' accounts were unauthorized copies.... [T]he DMCA does not place this burden on service providers."

Actual or "Red Flag" Knowledge

Service providers are also ineligible for the safe harbor if they have actual knowledge of infringing matter on their websites, or are aware of facts and circumstances that make infringement apparent (the "red flag" test), § 512(c)(1)(A) and (d)(1). The court stated that the red flag test is met, precluding safe harbor eligibility, if the web service links to sites "whose illegal purpose is obvious to a reasonable person." Neither MP3tunes nor its executives could be said to have actual or red flag knowledge, since the linked websites that were the source of songs at Sideload.com did not use terms (such as "pirate" or "bootleg") that indicated their illegal purposes and since the illegality was not obvious without investigation. "[T]he DMCA does not place the burden of investigation on the Internet service provider." The court clarified with:

> Put another way, if investigation is required to determine whether material is infringing, then those facts and circumstances are not "red flags".... As other courts have held, that rule makes sense where infringing works might be a small fraction of works posted to a website.

Plaintiffs' complaint alleged that "the vast majority of the music available through the MP3tunes service is infringing," but apparently they were unable to offer proof sufficiently convincing to the court.

Finally, the court held that emails or notices by third parties that do not substantially comply with the DMCA's takedown notice requirements also cannot establish actual or red flag knowledge.

Direct Financial Benefit Bar Not Satisfied

Web services are not eligible for the safe harbor if they have the right and ability to control, and derive direct financial benefit from, infringing activity. The labels contended that MP3tunes benefited financially because infringing activity acts as a draw and increases user traffic to MP3tunes. The court rejected the argument: "While Sideload.com may be used to draw users to MP3tunes.com and drive sales of pay lockers, it has non-infringing uses. Moreover, MP3tunes did not promote infringement." Further, "any link between infringing activity and a direct benefit to MP3tunes is attenuated because sideloaded songs were stored free of charge and infringing and non-infringing users of Sideload.com paid precisely the same or nothing at all, for locker services."

Plaintiffs also failed on the right-and-ability-to-control prong for the safe harbor, which "requires something more than the ability to remove or block access to materials posted on a service provider's website." "[T]he pertinent inquiry is not whether [the service provider] has the right and ability to control its system, but rather, whether it has the right and ability to control the infringing activity." MP3tunes does not select the linked websites containing illegal material; "[a]t worst, MP3tunes set up a fully automated system where users can choose to download infringing content." This lack of control over user conduct is insufficient to bar MP3tunes from being eligible for the safe harbor.

To sum up: MP3tunes' failure to remove from users' lockers previously stored infringing copies, for which the record companies had sent takedown notices, made it ineligible for the safe harbor. But the court essentially validated MP3tunes' business model, since in the future it will theoretically be possible for the service to expeditiously remove infringing music files from its servers upon notice. If this decision is followed by other courts, the issue, as a practical matter, may be whether music copyright-holders can serve takedown notices at such a pace, for a large enough proportion of the music stored in users' lockers, that the takedowns will seriously impair the usefulness of the cloud storage service for end users.

Secondary Liability: Contributory Infringement
Having held that the DMCA safe harbor did not preclude all liability, the court next considered, on summary judgment, MP3tunes' secondary liability for the copies of songs in users' lockers for which it had been denied the safe harbor. The court began by sweeping aside MP3tunes' asserted defenses that plaintiffs' proof of ownership of the copyrights in the songs was defective and that free promotional downloads amounted to abandonment or an implied license for MP3tunes' users to store and use the music at issue. Since this meant that MP3tunes' users were direct infringers, the court turned to MP3tunes' liability for contributory infringement. Contributory infringement liability required proof that MP3tunes knew of the infringing activity, and nonetheless materially contributed to it.

"MP3tunes' knowledge of the unauthorized use of infringing sideloaded material is manifest," the court held, based on plaintiffs' take-down notices that put MP3tunes on notice that the specified music files were infringing copies and based on the fact that MP3tunes had removed the infringing links from Sideload.com. The material contribution element is satisfied when the defendant's contribution is substantial, and "substantial contribution is found where an Internet service provider's servers 'are the sole instrumentality of their subscribers' infringement.'" That was the case here.

MP3tunes asserted finally that it was protected from secondary liability because its service had substantial non-infringing uses. The court rejected this contention on the ground that, in all of the past cases in which this was held a valid defense, the defendants did not have an on-going relationship with the direct infringers, as did MP3tunes.

No Direct Infringement by MP3tunes
The court denied the record companies' summary judgment claim that MP3tunes had directly infringed their copyrights. First, there was a triable issue as to whether the direct infringements of its executives and employees were performed in the course of their employment, and could therefore be attributed to MP3tunes. (However, since Robertson was an individually named defendant, the court found him directly liable for the songs he personally sideloaded from infringing sites.) Second, in a confusing (and perhaps confused) part of its analysis, the court denied summary judgment on the record companies' claim that MP3tunes violated the performance right by streaming music from a "master copy" of each copyrighted music file. The court rejected their position on the factual ground that MP3tunes did not use a "master copy" and on the legal ground that, in any event, the safe harbor applied to the performances at issue.

Conclusion and Comment: Cloud Model Vindicated
Notwithstanding the liability "setback" for MP3tunes itself and for Robertson, the district court decision represents an important (if possibly intermediate) victory for those promoting cloud storage by individual end users. The record companies did not, judging from the complaint and the summary judgment decision, challenge end users' right to upload music from their own computers to their lockers, and the infringement claims largely turned on MP3tunes' easy-to-use systems for locating, storing and playing music files from third-party sites, which plaintiffs alleged were "overwhelmingly" a source of infringing copies. But the district court absolved the service provider of liability for copying to its servers and streaming the infringing music files found on such sites, provided it observes the requirements of the safe harbor.

The district court joined other courts in requiring particularized notices of infringement, and in rejecting copyright holder contentions that it is enough that infringing matter is notoriously present. The court drew an interesting distinction, in the context of "repeat infringement," between users who upload to make music available to others (deemed "blatant infringers") and those who do not. It is not clear from the opinion how those who repeatedly "sideload" music from infringing sites, but solely for their own use, should be treated.

We will not be surprised to see appeals to the Second Circuit by both sides, in the fullness of time, though it is not clear whether plaintiffs will first take the case to trial on the remaining issues, including direct liability and damages due. For now, the cloud computing model finds further legal support.

The Stored Communications Act: A Statute Long Overdue for a Tuneup

BY MICHAEL R. EGGER AND TYLER G. NEWBY

If you are responsible for implementing and policing company policies to protect stored electronic communications or compliance with government requests to disclose such communications, you no doubt are familiar with the Stored Communications Act, as well as its deficiencies. Moreover, if the company is a provider of network services "in the cloud," knowing whether the company is entitled to the protections afforded by the Stored Communications Act is critical. For years, though,

judges, legal scholars, legislators, privacy advocates and Internet and network/communications service providers have complained about the deficiencies of the Stored Communications Act. Many have urged Congress to simplify its complex structure and opaque language and, most importantly, to broaden its scope to clearly address 21st century technology.

Background

The Stored Communications Act (18 U.S.C. §§ 2701-2711) (SCA) was enacted in 1986 as Title II of the Electronic Communications Privacy Act and is the primary federal statute regulating the government's right to obtain stored electronic communications from certain providers of network services. In order to make sense of the SCA and appreciate its deficiencies, it is important to understand the policies on which the SCA is based. Understanding these policies, in turn, requires revisiting the state of technology circa 1986.

Although 1986 was not exactly the "dark ages" for technology, it is unlikely that anyone would dispute that technology has significantly evolved in the past 25 years. Still, by 1986, the use of computers and network-related technology had become more decentralized, reflecting the proliferation of personal computers, both in the office and at home. Individuals increasingly used their personal computers (equipped with a modem) to access proprietary network services, such as America Online or CompuServe, in order to send and receive emails, to post messages on public bulletin board systems and to engage in similar activities.

When Congress enacted the SCA, its primary concern was to encourage and support the growth of companies in the then-emerging Internet and wireless communications industries and to ensure that such growth would not be inhibited by customer concerns regarding the privacy of their communications. (Under then-existing Supreme Court precedent, it was far from clear that the Supreme Court would extend Fourth Amendment protection to these new types of communications.) But, Congress was also concerned with maintaining an appropriate balance between an individual's right to privacy and the government's need to obtain certain information for law enforcement purposes.

Scope and Structure

The SCA regulates and protects only wire and electronic communications stored by providers of electronic communication services (ECS) or remote computing services (RCS). Whether a wire or electronic communication is protected by those portions of the SCA that apply to a provider of an ECS (an "ECS Provider") or to a provider of an RCS (an "RCS Provider") depends on the manner in which a provider handles such a communication. It is possible that a provider may act as both an ECS Provider and an RCS Provider with respect to a single communication. It is also possible that a provider may not be deemed to act as either an ECS Provider or an RCS Provider with respect to a communication, in which case the communication stored will not be protected by the SCA.

Electronic Communication Service The SCA protects wire and electronic communications that are sent or received through an electronic communication service while the communications are in electronic storage (§ 2701). The key definitions are as follows:

- "Electronic communication service" means any service which provides to users thereof the ability to send and receive wire or electronic communications, and
- "Electronic storage" means: (1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) Any storage of such communication by an electronic communication service for purposes of backup protection of such communications.

Remote Computing Service The SCA protects wire and electronic wire communications that are held or maintained in a remote computing service: (1) On behalf of and received by means of an electronic transmission from a customer/subscriber of the remote computing service; and (2) Solely for the purpose of providing storage or computer processing services to such customer/subscriber, if the provider is not authorized to access the content of any such communication for purposes of providing any services other than storage of computer processing (§ 2703). The key definitions are as follows:

- "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system; and
- "Electronic communication system" means any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Compelled Disclosure

The scope of the government's right to compel disclosure of a stored wire or electronic communication depends on: (1) whether the provider is acting as an ECS Provider or an RCS Provider as to the communication, (2) whether the communication constitutes content (e.g., the text of an email) or customer/subscriber records or information; and (3) as to a communication stored by an ECS Provider only, the number of days that the communication has been in electronic storage.

Disclosure of Content by ECS Provider The government must obtain a warrant to compel disclosure of the content of a wire or electronic communication held in electronic storage by an ECS Provider for not more than 180 days (§ 2703(a)). If such communication has been in electronic storage for more than 180 days, the government may use a warrant or a so-called "less process alternative," i.e., an administrative subpoena or court order (a "§ 2703(d) order"), which is issued upon a showing of "specific and articulable facts" (§ 2703(b)). The government must provide the customer/subscriber with prior written notice if it relies on one of the "less process alternatives," but may delay providing notice up to 90 days (and in certain instances may have the notice requirement waived entirely) (§ 2705).

Disclosure of Content by RCS Provider The government may compel disclosure of a wire or electronic communication stored by an RCS Provider in an electronic communication system by obtaining a warrant or by one of the § 2703(b) "less process alternatives" described above.

Disclosures of Records/Information by ECS Provider or RCS Provider As to records or other information pertaining to a customer/subscriber of an ECS Provider or an RCS Provider, the government is required to obtain a warrant, a § 2703(d) order, or the consent of the customer/subscriber (§ 2703(c)(1)). The government is also entitled to compel disclosure of basic customer/subscriber information (e.g., name, contact information, length of service, payment source) by subpoena (§ 2703(c)(2)).

Voluntary Disclosure

The SCA regulates the voluntary disclosure of electronic communications stored by an ECS Provider or an RCS Provider, but only if the provider's service is made available to the public. An ECS Provider is prohibited from knowingly disclosing to a third party the contents of an electronic communication while it is in electronic storage (§ 2702(a)(1)), and an RCS Provider is similarly prohibited from knowingly disclosing to a third party the contents of an electronic communication while it is carried or maintained on the RCS Provider's service (§ 2702(a)(2)). The SCA also prohibits disclosure of customer/subscriber records or information ((§ 2702(c)). However, multiple exceptions to the restrictions on voluntary disclosure exist (§ 2702(b) and(c)).

Deficiencies

Some of the criticisms directed to the SCA's deficiencies arise from structural flaws and substandard drafting that cause the statute to be difficult to understand and interpret. These types of flaws are relatively easy to address. Of far greater concern are the material deficiencies that have become apparent with the widespread adoption of 21st century technology:

Email-related

- Having a lower standard of protection for emails held in electronic storage for longer than 180 days made sense in 1986, as email was available only through proprietary network services, such as America Online, using email was costly because these services charged based on connect time, and storage capacity was limited. Today, as a result of the widespread availability of free Web-based email accounts that offer individuals virtually unlimited storage capacity, individuals routinely store emails (including sensitive professional and personal emails) for longer than 180 days, making the lower standard outdated.
- The standard of protection for unopened emails is unclear as a result of the existence of inconsistent interpretations of the definition of "electronic storage." The U.S. Department of Justice takes the position that only a subpoena is required to compel disclosure of emails that have been opened, on the theory that the "temporary or intermediate storage" prong of the definition of "electronic storage" (§ 2510(17)(A)) is satisfied only for as long as an email remains unopened. Although some courts have adopted this position, a controversial U.S. Court of Appeals, Ninth Circuit case, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), held that an email stored by a network services provider, whether opened or unopened, is subject to the same standard of protection until the email "has expired in the normal course," on the theory that the email is a backup copy under the "backup storage" prong of the definition of "electronic storage" (§ 2510(17)(B)).

Cloud Computing-related Some commentators have taken the position that providers of network services "in

the cloud" do not satisfy the definition of an RCS (and therefore are subject to different protections) because they provide services other than storage or computer processing services, or because they have the right to access the content of a customer's/subscriber's communications for purposes of other services. In 1986, the definition of "remote computing services" contemplated only the provision of data processing/outsourcing services. Consequently, this definition needs to be made current and consistent with the much broader scope of services often provided by network services providers today.

Conclusion

On May 19, 2011, Senator Patrick Leahy introduced the ECPA Amendment Act of 2011, which, among other things, proposes: (1) replacing the so-called "180-day rule" for determining the standard of protection for communications held in electronic storage with a requirement that the government obtain a warrant for any stored electronic communication; and (2) adding "geolocation information services" as a third category of regulated entities to address concerns raised by privacy groups regarding the protection of information available through mobile devices, GPS or other electronic communications devices. Although introduction of this amendment was quickly followed by subcommittee and committee hearings, whether Senator Leahy ultimately will be able to steer it to passage, and the timing of doing so, is uncertain given the economic concerns that continue to take center stage in our government. Stay tuned.

Second Circuit Upholds Gray Market Importation Bar and Negates First-Sale Doctrine for Works of Authorship Made Overseas

BY MITCHELL ZIMMERMAN

The U.S. Court of Appeals, Second Circuit decision in *John Wiley & Sons, Inc. v. Kirtsaeng,* No. 09-4896-cv, 2011 WL 3560003 (2nd Cir. Aug. 15, 2011), represents the latest chapter of a long-running saga that could be titled, "Gray Market Goods Try to Enter the Homeland." In *Kirtsaeng,* a divided panel of the Second Circuit held that the first-sale doctrine of 17 U.S.C. § 109(a) does not apply to works of authorship manufactured outside of the U.S. Hence, owning such a copy bestows no right to resell or distribute. If followed, *Kirtsaeng* would alter established law and practice on resale of new and used works of authorship, allowing copyright holders to control, or prohibit entirely, the resale of books, electronic products and any other works of authorship (or goods containing them) that are made overseas.

Like other manufacturers who price differentially in different markets, publisher John Wiley & Sons designated certain editions of its texts for sale only outside the U.S. and printed them overseas. Friends and family members of Kirtsaeng bought copies in Thailand and shipped them to him in the United States, where he sold them on eBay. Wiley brought an action claiming that Kirtsaeng violated § 602(a)(1) of the Copyright Act, which provides: "Importation into the United States, without the authority of the owner of copyright…, of copies… of a work that have been acquired outside the United States is an infringement of the exclusive right to distribute copies [of the work]."

Kirtsaeng asserted that the first-sale doctrine shielded him from liability. Under § 109(a), the owners of copies "lawfully made under this title" may sell or distribute their copies without the copyright holder's permission. Wiley argued that copies manufactured overseas were not "made under this title."

The Second Circuit noted the tension between § 602(a)(1) and § 109(a) and framed the issue broadly: whether the first-sale doctrine applies at all to copies manufactured abroad. The court found the wording of § 109(a) to be ambiguous and sought an interpretation that comported with the purpose of § 602(a)(1) and with the Supreme Court's decision in *Quality King Distributors, Inc. v. L'anza Research International, Inc.,* 523 U.S. 135 (1998). In that case, the Court held that the first-sale defense does apply to importation claims concerning "round trip" goods – those made in the U.S. and lawfully sold abroad before being sent back into the United States and re-sold by unauthorized third parties.

Thus, the main issue posed by *Kirtsaeng* was whether the first-sale defense applies to importation claims concerning *foreign-made* copies. The *Kirtsaeng* majority noted that § 602(a)(1) is intended to allow manufacturers to control the circumstances in which copies of their works that are manufactured abroad can be brought into the U.S. The court reasoned that the protection to be afforded by the provision would have no force in most cases if the first-sale doctrine was allowed as an exception to § 602(a)(1). The court also deemed its interpretation to be consistent with *dicta* in *Quality King* and held that the first-sale doctrine does not apply to copies manufactured abroad.

The Second Circuit could have framed and decided the issue more narrowly by simply deciding that § 109(a) is not a defense to an unauthorized and unlawful

importation. Instead, the Second Circuit limited the scope of § 109(a) itself by concluding that copies manufactured outside the U.S. are simply not "made under this title." Consequently, § 109(a) is not a defense to the resale of copies of a work that have been imported by or with the copyright holder's consent and there has therefore been *no* violation of § 602(a)(1).

The *Kirtsaeng* majority did not address or suggest any policy reason why Congress might have intended that the first-sale doctrine not apply to goods manufactured outside the U.S. Although the court expressly acknowledged the force of Kirtsaeng's argument that its ruling would provide an incentive for outsourcing production, and could result in the circumvention of the first-sale right, it deemed this consideration irrelevant to its analysis.

In his careful dissent, Judge Murtha focused on a close textual analysis, on the history of the first-sale doctrine, and on the policies underlying it, and reached the opposite conclusion in a set of arguments that the majority did not address.

As the Second Circuit noted, these issues had been addressed by the Ninth Circuit. In *Omega S.A. v. Costco Wholesale Corp.,* 541 F.3d 982 (9th Cir. 2008), *affirmed by 4-4 vote,* 131 S. Ct. 565 (2010), the Ninth Circuit held (as does the Second Circuit in *Kirtsaeng*) that § 109(a) does not protect the unauthorized importer of foreign-made copies. But — unlike *Kirtsaeng* — the Ninth Circuit has opined that the first-sale doctrine *does* apply to items manufactured abroad when they are imported and first sold in the United States by or with the copyright holder's permission. *Parfums Givenchy, Inc. v. Drug Emporium, Inc.,* 38 F.3d 477 (9th Cir. 1994).

It is not clear whether the Supreme Court would perceive the differences in analysis by the two courts as a "circuit split" on the importation right, since the Second and Ninth Circuits both concluded that § 602(a)(1) bars unauthorized importation of foreign-made copies and neither allowed § 109(a) as a defense. But *Kirtsaeng*'s different path to that conclusion would have profound implications for first-sale rights and, if widely accepted or affirmed by the Supreme Court, could alter the terms of sale of a wide range of goods.

While it is not clear which manufacturers would choose to exercise the power that *Kirtsaeng* affirms, an extraordinary range of products could fall within its ruling. In addition to obvious works of authorship, like books, musical recordings, films and computer software, myriad products include works protected by copyright. Virtually all electronic goods include integrated circuits containing copyright-protected software or firmware; so do microwave ovens, washing machines, telephones, blood pressure monitors, "intelligent" electric irons, automobiles and trucks, and probably most machinery. Other products, such as clothing, sheets and pillowcases, kitchen canisters and dishware, are commonly decorated with copyright-protected designs and are therefore within the resale control of the "copyright holder," if made overseas. Yet other goods obviously unprotected by copyright — like the shampoo and hair products in *Quality King* — often bear labels or are sold inside of packaging with copyrightable designs or graphics.

The stocks of some shotguns are decorated with protectable designs; likewise, some coffins. A bicycle probably includes nothing protected as a work of authorship, but if the box containing the bike includes a maintenance manual, it could be an infringement to import the box. A made-in-China picture frame may not be protected by copyright, but the sample photo that is typically in the frame undoubtedly is. For that matter, a watermelon grown in Central America usually has a small label on it; including a copyright-protected graphic is not unimaginable.

You get the picture. Nearly everything that is sold does or can include a work of authorship if it is not one itself. Whether most manufacturers would want to exercise control over resale is not clear. But most goods sold in the United States are imported or could be. *Kirtsaeng* opens a new world of possibly unintended consequences.

At this writing, Kirtsaeng's petition for rehearing *en banc* is pending, and his counsel has advised they will likely file for *certiorari* should rehearing be denied. Since, as mentioned earlier, *Kirtsaeng*'s broad holding conflicts with the reasoning of the Ninth Circuit decision in *Omega,* which the Supreme Court reviewed last year and affirmed on a four-four split, it seems almost inevitable that these issues will again be presented to the high court.

We note that the unauthorized importation of a copyrighted shampoo label and some of the other "tail-wags-dog" instances might also be subject to a fair-use defense. That issue does not appear to have been discussed in the cases addressing § 602(a)(1) and is beyond the scope of this article.

Quick Updates

Judge to Oracle: Bye-Bye Billion

On September 1, 2011, U. S. District Judge Phyllis Hamilton set aside the record-setting $1.3 billion jury verdict in *Oracle USA, Inc. v. SAP AG*, No. C 07-1658, 2011 U.S. Dist. LEXIS 98816 (N.D. Cal. Sept. 1, 2011). Absent proof that Oracle lost an opportunity to license its software to third parties, and absent objective evidence of benchmark transactions, the court held the "hypothetical license fee" used as the jury's measure of damages was subjective and speculative. Oracle's "consolation prize" does not appear shabby by ordinary standards, however. As an alternative to a new trial on actual damages, Oracle can accept a remittitur of $272 million.

Oracle sued SAP in March 2007, alleging infringement of certain Oracle software by the SAP subsidiary, TomorrowNow, and the case was tried before a jury in November 2010. In advance of the trial, SAP admitted liability for the alleged copyright infringement, save for some claims by Oracle that had been dismissed before the trial. The only issue for the jury was therefore the amount of damages. The jury awarded a staggering $1.3 billion to Oracle on the theory that this was the value of the hypothetical license fee that Oracle and SAP would have negotiated if Oracle had granted SAP a license to use the Oracle software in question, even though witnesses for both sides confirmed that such a license would never have existed between Oracle and SAP. This award was the highest ever damages award in a U.S. copyright infringement case.

In 2011, SAP filed a motion for judgment as a matter of law that Oracle was not entitled to damages in the form of a hypothetical license fee because Oracle did not provide sufficient evidence to demonstrate that it would have licensed the software in question to SAP, an Oracle competitor, and because Oracle did not provide objective evidence of a non-speculative value on such a license.

The court granted SAP's motion and overturned the jury award. Judge Hamilton agreed that Oracle did not provide evidence to support its hypothetical license estimates which were presented to the jury. First, Oracle did not show that it had lost an opportunity to license the software to third parties for the same use as the infringing use by SAP. Second, Oracle failed to present non-speculative evidence to support a hypothetical license to SAP. The court indicated it "expected to see objective evidence showing some licensing activity either by Oracle or by some other company in the related industry — if not from Oracle/SAP's prior dealings — and objective evidence of what a willing buyer would have reasonably paid, not simply what Oracle would have demanded."

The court clarified what is required: "An objective, non-speculative [hypothetical] license price is established through objective evidence of benchmark transactions, such as licenses previously negotiated for comparable use of the infringed work, and benchmark licenses for comparable uses of comparable works," the court ruled. "Absent evidence of benchmarks, Oracle cannot recover a lost license fee award…."

Although SAP's motion was granted, the court noted that Oracle is still entitled to some measure of damages given that SAP admitted liability for copyright infringement and consequently Oracle is entitled to recover actual damages in for the form of lost profits/infringers profits. Based on the evidence provided by damages experts for both SAP and Oracle, Judge Hamilton calculated that Oracle's lost profits totaled $272 million, and offered Oracle a choice – take the $272 million or go to trial again to determine lost profits.

ICANN to Make New Internet Domain Namespace Available to Brand Owners

In the more than 13 years since the creation of the Internet Corporation for Assigned Names and Numbers (ICANN), the domain namespace has expanded to only 22 generic top-level domains (gTLDs), including .com, .org, and .net. With approximately 50,000 new domain names coming online every day, ICANN is accommodating for this growth by launching a new program that will unleash a potentially limitless amount of new gTLDs. The new gTLD program will enable corporations, organizations, or other institutions to become registry operators for their own gTLD; new gTLDs can consist of community-based generic terms, such as .shoe or .bank, or specific brand names, such as .nike or .chase.

Beginning January 12, 2012, ICANN will begin accepting applications for new gTLDs; the application window will close on April 12, 2012. Applicants must meet certain criteria, including a background screening for criminal activity or a history of domain name abuse, technical requirements to operate a TLD in a secure and stable manner, financial requirements to support the TLD, and a business plan to set forth the purpose and use of the TLD. The rigorous application evaluation process is expected to take about nine months to complete, with the new gTLDs projected to come online in 2013. The new gTLDs come with a hefty price tag, however. Each application will cost approximately $185,000, and the applicant is solely

responsible for its own business startup and operations costs, which could amount to $2 million, according to the International Trademark Association.

ICANN has implemented several rights protection mechanisms for brand owners throughout the application process. After the application window closes, ICANN will make the applications available to the public, who can comment upon or formally object to any new gTLD that they consider to be offensive or to infringe their rights. Furthermore, ICANN requires applicants to describe how their registries will implement rights protection mechanisms such as the Uniform Domain Name Dispute Resolution Policy (UDRP), the Uniform Rapid Suspension (URS) system, and a Sunrise period for domain name registrants. As an additional security measure, ICANN is implementing a Post Delegation Dispute Resolution Procedure (PDDRP) in which a trademark owner may submit a complaint if it believes that a registry is actively engaging in infringing behavior.

About one hundred different groups have already declared intentions to apply for new gTLDs, including Canon, Inc. for .canon, Hitachi for .hitachi, and Adrenaline TLD for sports domains such as .ski and .bike. Other groups have cited sticker shock for their reluctance to adopt a new gTLD, arguing that arbitrating a dispute over ownership of a particular domain name will be significantly cheaper than preemptively applying for a new gTLD. One thing is for certain: as more domain names come online, brand owners must be more vigilant in policing their marks. The new gTLD Applicant Guidebook is available online at http://www.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.

Judge Sparks Orders Patent Office to Expedite Reexaminations, but Has a Sudden Change of Heart

Judge Sam Sparks of the U.S. District Court for the Western District of Texas recently raised eyebrows and questions by ordering the United States Patent and Trademark Office (PTO) to expedite a reexamination of three patents. In *MONKEYmedia, Inc. v. Apple, Inc.*, 1-10-cv-00319 (W.D. Tex. July 25, 2011), after defendants moved for a stay as to three patents in reexamination proceedings, Judge Sparks responded to plaintiff's arguments that the PTO was "notoriously slow" in reaching decisions in reexamination proceedings by ordering the PTO to expedite the reexamination and to "provide the results of its reexaminations to the parties and the Court" three months after the date of the order. Judge Sparks also ordered the parties to expedite their submissions to the PTO "to facilitate timely reexamination."

Neither party had requested an expedited reexamination. On the contrary, after Judge Sparks' order was issued, plaintiff's counsel advised the court that plaintiff MONKEYmedia, Inc. intended to further slow the pace of the reexamination by filing a request for reconsideration of the PTO's denial of MONKEYmedia's request for an extension of time. Upon learning this news, Judge Sparks stayed the entire matter. The subsequent order quieted the legal blogosphere, but left unanswered the question of whether a federal district court judge has the authority to order the PTO to do anything in a case where the government is not a party.

The issue arose when MONKEYmedia, Inc. filed a complaint asserting three patents against Apple Inc. in May 2010 (later amended to include three additional related patents). Several days before the hearing, defendants informed the court that two of the three related patents were under reexamination, and notified the court that defendants intended to file for a stay if the PTO granted a reexam request for the third patent. The PTO did order reexamination, and the defendants filed a motion to stay only as to the three related patents.

Defendants argued that litigating the three patents under reexamination would be a waste of judicial resources, and that MONKEYmedia would not be unduly prejudiced as it was not in the business of making or selling any products covered by the patents. In its opposition, plaintiff made much of the slow pace of reexaminations, arguing that the reexamination would delay half of the case for approximately 6 ½-8 years. Plaintiff argued that the stay would endanger the very viability of the small company by forcing it to litigate two separate trials back to back.

In a July 25, 2011 Order, Judge Sparks stated he did not wish to stay the trial indefinitely, but noted that a short stay may serve to clarify the issues, "particularly if the parties are as interested in the efficient resolution of this dispute as they both purport to be." By expediting their submissions to the PTO, the parties could facilitate the reexamination and (somehow) shorten a 6 ½-8-year delay to a brief three months. Judge Sparks, perhaps acknowledging that his powers were in fact limited to the parties-in-suit, ordered the parties themselves to advise the PTO of the stay and the order for expedited review. It is unknown whether the order was ever conveyed to the PTO because plaintiff's counsel promptly informed the court of plaintiff's own efforts now to delay the reexamination

proceedings, though plaintiff had argued against delay. In a July 27, 2011 Order, Judge Sparks explained that he had issued the July 25 Order because he "believed all parties would work together to achieve a quick and efficient reexamination of the patents," but in this Order, Judge Sparks decided to stay the entire matter pending final reexamination (even though defendants had requested a stay as to only three of the patents-in-suit).

While the limits of Judge Sparks' power over the PTO remain untested, the lesson could not be clearer: when complaining of the "notoriously slow" pace of the PTO to a court, it is best to not simultaneously use every tool at your disposal to further slow the process. Class dismissed.

Posting Trade Secrets

In August, a district court in New Jersey issued a significant decision addressing the issue of whether, and under what circumstances, the posting of materials on the Internet destroys trade secret status. *SyncSort Inc. v. Innovative Routines, Int'l, Inc.,* Civ. No. 04-3623, 2011 U.S. Dist. LEXIS 92321, (D.N.J. August 18, 2011). Rather than adopting a bright-line rule, the court conducted a more nuanced, fact-specific analysis before ultimately concluding that plaintiff's proprietary UNIX command language was sufficiently "secret" to merit trade secret protection, despite several public disclosures of the command language on the Internet.

Plaintiff, SyncSort Incorporated (SyncSort) and the defendant Innovative Routines International, Inc. (IRI), are competitors who develop and sell data transformation software. SyncSort produces and licenses a data transformation software product called SyncSort UNIX, which relies on the use of a proprietary command language that SyncSort had been developing since the early 1990s. SyncSort took various precautions to ensure that the elements and workings of the command language would not become publicly known, such as requiring all SyncSort employees to enter into confidentiality agreements, and implementing a firewall to prevent outsiders from obtaining access to SyncSort's internal computer network. SyncSort also applied confidentiality labels to all readable materials, including the comprehensive Reference Guide defining the commands, parameters and syntax and formal grammar definitions of the SyncSort UNIX command language.

In 2000, IRI developed a computer program that was capable of translating scripts written in the SyncSort command language into scripts that would be compatible with IRI's competing software product. The creation of this translation program required extensive knowledge of SyncSort's command language. After IRI's launch of the competing product, SyncSort filed suit alleging that IRI developed its translation programs using pilfered scripts from the SyncSort UNIX command language as well as the confidential Reference Guide. In response to the allegations, IRI produced evidence that various snippets of the command language, as well as the Reference Guide in its entirety, had been posted on the Internet and that such public exposure had automatically destroyed the trade secret status of any information contained in those postings.

But the judge declined to adopt this inflexible approach, emphasizing that "publication on the Internet may not destroy a secret if it is 'sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic concern.'" Examining the content and context of each Internet posting, he determined that the publicly posted pieces of command language did not negate trade secret protection because the information contained in those postings was insufficient, either individually or in the aggregate, to develop the translator. Even though the judge acknowledged that the Reference Guide document *would* have provided IRI with sufficient information to develop the translator, the judge pointed to the lack of any evidence that competitors or other unauthorized persons had accessed or even attempted to access the Reference Guide on the two occasions it was posted on third-party foreign websites. The fact that SyncSort had taken measures to promptly remove the postings of the Reference Guide further supported the judge's conclusion that these two isolated postings did not destroy the trade secret status of the information.

SyncSort's rejection of the notion that trade secret status is automatically destroyed by Internet exposure is in line with several other district court decisions in recent years and serves as an important reminder that a well-established protocol for protecting trade secrets and other proprietary information, as well as swift actions to remove any unauthorized Internet postings of such information, may be sufficient to preserve trade secret protection for information that is unexpectedly posted.

Fenwick

FENWICK & WEST LLP

Intellectual Property Bulletin Editorial Staff

Staff Editor	Stuart P. Meyer
Assistant Editors	Antonia L. Sequeira Christopher D. Joslyn
Article Contributors	Michael R. Egger, Katie McKnight, Tyler G. Newby, Jennifer Stanley, Betsy White, Lauren E. Whittemore, Mitchell Zimmerman

Fenwick & West LLP Practice Groups

Intellectual Property

David L. Hayes	*Chair*
Sally M. Abel	*Chair, Trademark Group*
Ralph M. Pais	*Chair, Technology Transactions Group*
Mark S. Ostrau	*Co-Chair, Antitrust and Unfair Competition Group and Co-Chair, Cleantech Group*
John T. McNelis	*Chair, Patent Group*
Mitchell Zimmerman	*Chair, Copyright Group*
Rodger R. Cole	*Chair, Trade Secret Group*
Michael J. Shuster	*Co-Chair, Life Sciences Group*

Litigation

Darryl M. Woo	*Chair*
Tyler A. Baker	*Co-Chair, Antitrust and Unfair Competition Group*
Laurence F. Pulgram	*Chair, Commercial & Copyright Litigation Groups*
Michael A. Sands	*Chair, Electronic Information Management Group*
Kevin P. Muck	*Chair, Securities Litigation Group*
Charlene M. Morrow	*Chair, Patent Litigation Group*
Jedediah Wakefield	*Chair, Trademark Litigation Group*
Rodger R. Cole	*Chair, Trade Secret Litigation Group*
Daniel J. McCoy	*Co-Chair, Employment Practices Group*
Victor Schachter	*Co-Chair, Employment Practices Group*
Christopher J. Steskal	*Chair, White Collar/ Regulatory Group*

Corporate

Richard L. Dickson	*Chair*
Douglas N. Cogen	*Co-Chair, Mergers and Acquisitions Group and Co-Chair, Private Equity Group*
David W. Healy	*Co-Chair, Mergers and Acquisitions Group*
Horace Nash	*Co-Chair, Securities Group*
Jeffrey R. Vetter	*Co-Chair, Securities Group*
Scott P. Spector	*Chair, Executive Compensation and Employee Benefits Group*
Stephen M. Graham	*Co-Chair, Life Sciences Group*
Cynthia Clarfield Hess	*Co-Chair, Start-ups and Venture Capital Group*
Mark A. Leahy	*Co-Chair, Start-ups and Venture Capital Group*
Mark C. Stevens	*Co-Chair, Private Equity Group*
Sayre E. Stevick	*Co-Chair, Cleantech Group*

Tax

David L. Forst	*Chair*
Kenneth B. Clark	*Chair, Tax Litigation Group*

Fenwick & West's Intellectual Property Group offers comprehensive, integrated advice regarding all aspects of the protection and exploitation of intellectual property. From providing legal defense in precedent-setting user interface copyright lawsuits and prosecuting software patents to crafting user distribution arrangements on behalf of high-technology companies and implementing penetrating intellectual property audits, our attorneys' technical skills enable the Firm to render sophisticated legal advice.

Offices

801 California Street
Mountain View, CA 94041
Tel: 650.988.8500

555 California Street, 12th floor
San Francisco, CA 94104
Tel: 415.875.2300

1191 Second Avenue, 10th Floor
Seattle, WA 98101
Tel: 206.389.4510

www.fenwick.com

We appreciate your feedback!

If you have questions, comments, or suggestions for the editors of the IPB, you can e-mail them to IPB@fenwick.com.

For subscription requests and address changes, please e-mail IPB@fenwick.com.