

Supreme Court Hears Oral Arguments In In re Bilski Business Methods Patents Case

On November 9, 2009, the Supreme Court heard oral arguments on behalf of the patent applicants and the U.S. Patent Office in *In re Bilski*. At the heart of *In re Bilski* is how a business method may fall within the definition of "process" as it is used in Section 101 of the U.S. Patent Act. Section 101 of the Patent Act broadly defines proper patentable subject matter in the United States as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." Due to the breadth of this definition, it is often left to the courts to render decisions concerning how new technologies or advancements fit within this definition and ultimately left to Congress to enact legislation that further restricts or defines the patentability

of these new technologies or advancements. While the term "process" has an ordinary meaning that is quite broad, the Supreme Court has previously limited the definition to something narrower than its ordinary meaning by concluding that a patent claim covering a "process" is not patent-eligible if it claims "laws of nature, natural phenomena, [or] abstract ideas."

The *Bilski* case stems from an application for patent protection filed by Bernard L. Bilski and Rand A. Warsaw in 1997 and covering a method of hedging risk in the field of commodities trading. The U.S. Patent Office refused Bilski's claims as failing to meet the patent eligibility standard of Section 101. The patent examiner

continued on page 2

Sunrise Registration Period Begins for .PΦ

Russian registrar RU Center has begun accepting applications for domain names under .PΦ, the Cyrillic country-code top-level domain for Russian Federation. Following a four-month sunrise registration period for trademark owners that began on November 25, 2009, registration will open to general public, first through an auction process planned between April and June 2010, and then at a fixed price, beginning July 2010. The domain names will be in the Russian language, using the Cyrillic alphabet. During the sunrise period, instead of granting registrations on a first-come, first-served basis, the registrar will consider applicants' underlying trademark registrations and give priority to holder of the earlier registration. Thus, if there are two identical registrations in different classes, and both owners have applied for the corresponding .PΦ domain name, holder of the earlier-issued registration will prevail. The domain is still pending final approval by ICANN and the delegation is not expected until February 2010 at the earliest.

ACTA's Controversial Internet Provisions

On November 30, 2009, a leaked European Commission document dated October 29, 2009, confirmed suspicions regarding the Anti-Counterfeiting Trade Agreement's controversial Internet chapter. This comes after Round Six of ACTA negotiations that took place November 4-6, 2009, focusing on enforcement in the digital environment, ramped into controversy in light of a different leaked document, a summary dated September 30, 2009, also drafted by the European Commission. The leaked summary discussed the US Trade Representative's oral briefing on the progress of the proposed Internet Chapter, and led many in the technology industry to fear that ACTA would impose DMCA-like regulations worldwide. The October document leaked on November 30th is the European Commission's analysis of the ACTA Internet Chapter proposed by the United States, and it confirms suspicions that the US is pushing for ACTA to contain DMCA-like provisions, third-party liability, and criminal sanctions.

continued on page 3

Cloud Computing: Potential Benefits Come With Legal Risks

Cloud computing has come to the forefront recently as a means for businesses to reduce costs and create efficiencies for IT departments and company employees in utilizing software, infrastructure, and platform as a service. However, the use of cloud computing also comes with potential legal risks and issues of concern. This brief article will touch on some of the issues that should be considered when moving a company's documents and applications to a "cloud."

Cloud computing refers to computing services provided over the internet. Consumers and businesses have been using cloud computing for years, through services such as web-based email from AOL, Yahoo and Gmail, or social-

continued on page 4

December 10 Landrush for Non-Latin .EU Domain Names

EURid, the European Registry for .EU domain names, has announced that starting December 10, 2009, companies and individuals based in the European Union will be able to register .EU Internationalized Domain Names (IDNs). IDNs are domain names that contain non-Latin characters such as the Swedish å, the German ü, the Romanian ș and characters from the Bulgarian and Greek alphabets as a whole. IDN support will enable companies and individuals to register second-level .EU domain names in any of the 23 official languages, many of which have non-Latin characters in their alphabets. Rather than having a sunrise period for existing registrants, EURid has decided to allow registrations on a landrush, first-come, first-served basis. Any disputes regarding these newly-registered domains will have to be resolved through EURid's Alternative Dispute Resolution process administered by the Prague-based Czech Arbitration Court.

Bilski (continued from page 1)

supported the refusal of all claims in the application stating that “the invention is not implemented on a specific apparatus and merely manipulates [an] abstract idea and solves a purely mathematical problem without any limitation to a practical application, therefore, the invention is not directed to the technological arts.” The applicants appealed the patent examiner’s decision to the Board of Patent Appeals and Interferences at the U.S. Patent Office. While the Board rejected the patent examiner’s reasoning, it did agree that the claimed method was not proper patentable subject matter. Specifically, the Board concluded that the applicants’ claims did not involve any patent-eligible transformation, holding that transformation of “non-physical financial risks and legal liabilities of the commodity provider, the consumer, and the market participants” is not patent-eligible subject matter. The Board also held that Applicants’ claims “preempt[] any and every possible way of performing the steps of the [claimed process], by human or by any kind of machine or by any combination thereof,” and thus concluded that they only claim an abstract idea ineligible for patent protection. Finally, the Board held that Applicants’ process as claimed did not produce a “useful, concrete and tangible result,” and for this reason as well was not drawn to patent-eligible subject matter.

The applicants timely appealed the decision of the Board to the Federal Circuit Court of Appeals. The Federal Circuit, sitting en banc, affirmed the Board’s decision that the applicants’ claims did not meet the patent eligibility standard of Section 101. The Federal Circuit held that a “process” must be tied to a particular machine or apparatus, or must transform a particular article into a different state or thing (the “machine-or-transformation” test), to be eligible for patenting under

Section 101 of the Patent Act. Of particular significance during prosecution of the application, the appeal to the Board and appeal to the Federal Circuit was the admission by the applicants that the claimed “process” was not limited to application on a computer, removing the “machine” portion of the “machine-or-transformation” test from consideration by the Federal Circuit. Because the applicants’ claims do not involve the transformation of any physical object or substance, or an electronic signal representative of any physical object or substance, the Federal Circuit concluded that “transformation” portion of the “machine-or-transformation” test was not met.

The applicants appealed the Federal Circuit’s decision to the Supreme Court, asking the Supreme Court to consider whether the Federal Circuit erred by holding that a “process” must be tied to a particular machine or apparatus, or transform a particular article into a different state or thing (“machine-or-transformation” test), to be eligible for patenting under Section 101 of the Patent Act. The matter was fully briefed on behalf of the applicants and the Patent Office earlier this year. A total of 67 “friends of the court” or *amicus curiae* briefs have been filed by patent owners, bar associations, interested organizations, academics, and individuals, both supporting and refuting the Federal Circuit’s “machine-or-transformation” test. Supportive briefs generally fell in line with the position that the “machine-or-transformation” test would provide meaningful limits to the scope of patent claims as they apply to methods and processes. Briefs refuting the test generally criticize it as being arbitrary, more restrictive than what has been previously applied by the Federal Circuit in similar matters, and in conflict with accepted definitions of statutory terms. Some *amicus curiae* briefs plead

the case of application or non-application of the “machine-or-transformation” test to software patents, clearly requesting the Supreme Court to render a decision beyond the scope of the case at issue.

At oral argument, Justices Sotomayor, Kennedy and Breyer were particularly active, with only slightly lesser participation by Justices Scalia and Ginsburg and Chief Justice Roberts. The Court clearly understood the far reaching implications this decision will have on business methods and methods covering new technologies yet to be developed. During the presentation of the applicants’ argument, the Justices peppered applicants’ counsel with questions on where to establish a limitation on patentable subject matter, should the “machine-or-transformation” test not be accepted. The Justices all appeared concerned of the consequences of setting no limits and affording patent protection to abstract ideas. The Justices appeared equally concerned that the “machine-or-transformation” test could ultimately turn into something too easily applied on a rigid basis. The Solicitor General answered the Justices’ questions by seeking to demonstrate how the “machine-or-transformation” test was a flexible test and a test that would not have changed the result of other seminal cases regarding patentability of processes.

The Supreme Court’s decision is expected in the spring of 2010. The business and legal world alike anxiously await this decision. The Supreme Court may decide the issue without much analysis beyond the specific circumstances at hand, leaving open the possibility for more arguments and analysis as new issues arise, or the Supreme Court may decide to render a broad reaching decision that could extend to cover a host of issues concerning methods and processes.

ACTA (continued from page 1)

ACTA is a proposed agreement between the United States, the European Union, Australia, Canada, Japan, Singapore, Morocco, Mexico, the Republic of Korea, New Zealand and Switzerland to address global counterfeiting and piracy. The idea was launched by the United States and Japan in 2006; thus far, ACTA has been negotiated to cover a broad scope of infringements related to intellectual property and their consequences, including (1) depriving legitimate businesses and their workers of income; (2) discouraging innovation and creativity; (3) threatening consumer health and safety; (4) providing an easy source of revenue for organized crime; and (5) causing a loss of tax revenue. The aim is to enhance international co-operation and to create worldwide standards for enforcing intellectual property rights. Negotiations began in June 2008 and are set to be completed in 2010.

The leaked October document titled "European Union's Comments to the US Proposal" confirms the suspicions generated by the previously leaked September document, in which the EU summarized the USTR's briefing on its progress in drafting the Internet Provisions for ACTA. Taken together, these documents confirm that the US is pushing to model ACTA's Internet Chapter generally on the respective Internet section of the recently completed US-Korea Free Trade Agreement (KORUS), which was based on Section 512 of the Digital Millennium Copyright Act (DMCA).

According to the documents, the US has drafted ACTA's Internet provisions to consist of 7 sections:

Section 1

First section covers general obligations, focusing on "effective enforcement procedures" with language inspired by

article 41 TRIPS. Critics have noted, however, that absent from this language is a statement that the procedures shall be fair, equitable, and/or proportionate, contained in the corresponding sections of TRIPS, the WIPO Copyright Treaty, and Europe's Intellectual Property Rights Enforcement Directive.

Section 2

The real controversy begins with Section 2, which would require ACTA members to provide for third-party liability for copyright infringement. Although this is something that copyright owners have long sought after, it is not required by any of the major international IP treaties, including the 1994 Trade Related Aspects of IP agreement (TRIPS), the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty. Opponents are concerned that this section focuses solely on copyright, and that it may incorporate US "contributory copyright infringement" standards, including the "inducement" standard from the Grokster case which would significantly change the law in many countries.

Section 3

Perhaps the most controversial, Section 3 discusses limitations on third-party liability, laying out the conditions under which an ISP could qualify for safe-harbors. The section is reported to require ISPs to adopt and reasonably implement a policy "to address the unauthorized storage or transmission of materials protected by copyright or related rights" and mandate "broad" provisions regarding notice-and-takedown mechanisms.

The concern here is that the requirement that ISPs must develop and implement a certain policy goes beyond the law already in place in the EU by essentially conditioning the application of the liability limitations on an ISP actively policing

its content. An example of a reasonable policy is explained in footnote 6 which discusses requiring ISPs to terminate subscriptions. This is highly controversial as the issue of whether such an account can be terminated without court decision is still subject to negotiation between the European Parliament and the Council of Telecoms Ministers.

Further, the leaked September document mentioned the following:

"to benefit from safe-harbours, ISPs need to put in place policies to deter unauthorized storage and transmission of IP infringing content (ex. Clauses in customer's contracts allowing, *inter alia*, a graduated response)"

Opponents are concerned that the "graduated response" language may imply that negotiators are considering a sort of "three-strikes" policy under which ISPs would be required to terminate a customer upon repeated allegations of copyright infringement, or the ISP could be vulnerable to liability. The Three Strikes/Graduated Response has been sought by the entertainment industry since the European office of the Motion Picture Association began advertising the Three Strikes policy as an ISP "best practice" in 2005. Those in the technology and telecom industries are concerned that requirements of this type will make it too costly to successfully operate online enterprises such as Flickr or YouTube.

Such Three Strikes regime has previously been rejected by the European Parliament and in several ACTA-negotiating countries, and has never been proposed by US legislators. Opponents argue that even the suggestion of such a policy is contrary to the USTR's own statement that ACTA will not change US law. The current safe harbors under the US DMCA require ISPs

continued on page 4

ACTA (continued from page 3)

to adopt and reasonably implement a policy for termination of "repeat infringers" "in appropriate circumstances." ISPs are given the flexibility to determine what constitutes "appropriate circumstances." If a Three Strikes policy were adopted, this would change. ISPs would no longer be able to determine "appropriate circumstances," but instead would be required to automatically terminate a customer.

Further, many are concerned that this section's aim at implementing a notice and take down procedure will be at odds with the current European Commission's E-Commerce Directive (2000/31/EC), under which an ISP may adopt such policies, but they are not a requirement to benefiting from liability exemptions.

Section 4

Section 4 of the US proposal focuses on technical protection measures (TPMs, aka DRM), and includes language inspired by the US-Jordan Free Trade Agreement (article 4.13) and WIPO Internet Treaties (articles 11 WCT and 18 WPPT). This section would cover prohibitions on use, manufacture and trafficking in circumvention of access controls and provide both civil and criminal penalties, separate and apart from "general" copyright infringements.

Sections 5, 6 and 7

Section 5 focuses on Civil and Criminal Enforcement of Anti-Circumvention and requires both civil and criminal provisions. These provisions are also reportedly designed to stop efforts towards establishing interoperability requirements (i.e., ability for consumers to play purchased music on different devices).

Finally, Section 6 focuses on Rights' Management, again inspired by the US-

Jordan Free-Trade Agreement and WIPO Internet Treaties and provides for civil and criminal remedies, and Section 7 focuses on the limitations to Rights Management Information protection.

The Good and Bad

The main concern with sections 4, 5, and 6 is that they go beyond current EU law by requiring members to provide for civil and criminal remedies. Under current EU law, member states are merely required to provide "adequate legal protection."

Opponents are concerned that the proposed Internet provisions of ACTA will impede consumer privacy, civil liberties and the free flow of information on the internet. They also fear that many of the provisions may mandate requirements above and beyond, or even in the face of, what is already required under other treaties and/or international law. Because the purpose of ACTA is to create new global standards, many fear that implementation of ACTA by developing countries could become a condition imposed in future free trade agreements and ensure that US' chosen implementation of the WIPO Internet Treaty becomes a global standard, hindering the ability of developing countries (which, opponents argue, are excluded from negotiations) to choose policies best suited for their domestic priorities and economy.

Members of the entertainment and content industries take the position that in light of the substantial technological changes since the drafting of TRIPS nearly 20 years ago and the growth of online theft, new tailored rules are long overdue.

On November 19, the MPAA wrote a letter to Congress expressing its support for a "robust" ACTA and requesting codification of the "best practices" for copyright enforcement (aka "three strikes") in order to protect members of the entertainment

and content industry whose livelihood is dependent on intellectual property. In light of the technological changes that have occurred in the last decade, they argue, internet piracy is the fastest growing threat to their industry and copyright protection needs to be strengthened accordingly. They argue that opponents' view that stronger rules are "anti-innovation" disregards that innovation thrives only with adequate incentive. A number of movie studios, labels, and other copyright-holding companies wrote a similar letter in support of ACTA on the same date also requesting codification of "best practices" for copyright and urging for stronger protections.

Conclusion

Since no official draft has been released, it is yet to be seen how far the Internet provisions may go. In any case, negotiating countries are set to meet again in Morocco in July 2010, and the intention is still to conclude negotiations in 2010.

Cloud Computing (continued from page 1)

networking and information-sharing sites like Twitter, Facebook and WebMD. Generally, third-party service providers supply various software and/or hardware infrastructures on an as-needed "pay as you go" basis, thereby making cloud computing more scalable and flexible to meet a company's changing needs for software, infrastructure or storage. Frequently, these services include software applications that an end user might access for basic functions like email and word processing. Additional services provided by a third-party vendor would be infrastructure such as networking and storage capabilities, and more advanced software applications, which could include custom applications.

Although cloud computing can reduce costs and provide flexibility, there are risks

continued on page 5

Cloud Computing *(continued from page 4)*

that must be assessed and accounted for when moving a company's valuable data, including intellectual property, to a cloud hosted by a third-party. Of prime importance is making sure that a company's assets and data are in a safe environment, protected from theft and modification, while also complying with the laws of the location(s) where the company and the cloud may be located. The risks can be minimized by entering into a detailed agreement dictating the terms relating to security, access, performance, location, management and control of a company's assets in the cloud.

The security of a company's data is a primary concern, as the third-party provider has access to the data which is stored on servers and systems over which the company does not have complete control. While the customer legally owns its data in the cloud, it is important that the customer ensures that the provider is contractually obligated to protect the data on a level that complies with the customer's internal policies. Also of concern is protecting the data in a fashion sufficient to meet the regulatory levels of protection required by the locales of the cloud and the customer. This is of particular importance to companies operating in Europe, Canada, or other foreign locations where data protection, security and privacy obligations may be different. It may therefore be necessary

to specify particular locations for cloud storage, rather than unknowingly run afoul of the law due to the provider's location or movement of the cloud.

Security issues are also of utmost importance when protecting intellectual property, such as undisclosed patents and trade secrets. Since it is not uncommon for third-party providers to store one company's data at a location where data belonging to other companies (potentially including company's competitors) is also stored, proper protocols should be contractually defined to ensure that there is no commingling of data with that of another company. These terms would include protocols for access rights and encryption standards, thereby preventing data from being improperly accessed or removed by an unauthorized user.

Performing due diligence on the service provider, including stability of the service provider as an on-going entity, continuous availability of data, backup contingencies, and ability to retain and transfer data to another provider are also of utmost importance. If entering into an agreement with a service provider, a company should also secure assurances that the service provider has obtained any necessary intellectual property licenses, while also getting indemnification for any potential infringement by the provider. The negotiated contract must also provide for

the safeguarding and transfer of data in the event the provider ceases to exist. Inability to fully control company's data and intellectual property assets on a daily basis, as well as in a force majeure event, including bankruptcy or change of ownership of the third-party provider, can negate potential benefits of using a cloud.

Location of the cloud is important not only in terms of compliance with privacy and security laws. Where the data resides may be a critical factor in determining what law applies to the dispute, and how easy it may be to actually access and control the electronic information. Since data stored in foreign countries may be subject to strict requirements with respect to privacy and security, cross-border litigation can become more complicated. Preservation and record-retention policies, including segregation of privileged, confidential or proprietary information such as intellectual property, must be reviewed in light of compliance with litigation protocols.

While cloud computing can provide financial and scalable benefits to companies and IT departments, potential legal issues and risks that it carries must be carefully assessed, evaluated and contractually provided for in a negotiated agreement before a company's valuable data and intellectual property is moved to the cloud.