MYERS WOLIN
INTELLECTUAL PROPERTY

"We are heading to a cloud revolution, which means a world of innovation that should be protected."

PROTECTING YOUR CLOUD INTELLECTUAL PROPERTY

BY MICHAEL BEN-SHIMON

The power of the cloud is the buzz that's going to drive the IT industry in the years to come. In fact, it is expected that most of the software applications used today will be "cloudified" in the very near future. According to industry data supplied by International Data Corp and Gartner, by 2014 some 70% of software will run in the cloud, with the market for cloud computing projected to be $149 billion. We are heading to a cloud revolution, which means a world of innovation that should be protected.

To understand the challenges in securing your cloud innovation, let's take a closer look at the underlining technology of cloud computing. In a nutshell, cloud computing is an **Internet-based** infrastructure in which information, resources, and software applications are provided and **shared on-demand**.

Michael Ben-Shimon is an Intellectual Property Analyst with Myers Wolin, LLC

Cloud services, a/k/a Saas, PaaS, and IaaS, use the Internet and remote servers to maintain data and applications. This allows consumers and businesses alike to utilize such resources without installation on their own computers; personal files may be accessed from any computer that has Internet capabilities. The hardware (computing) resources of the cloud are typically geographically distributed, which means that a cloud service can virtually run in numerous different locations, including ones that may also cross borders between countries

The underlying architecture of the cloud poses some IP challenges, however. Execution of a "cloud application" is typically distributed, i.e., it can run on multiple servers located in different parts of the world. Furthermore, developers of such applications usually have little information about what happens under the covers. In most cases, the developers do not know who provides the infrastructure and/or platform services. Thus, it would not be apparent and readily recognizable when infringement takes place, nor would the infringer's identity be readily obvious. The question is, how would one who "makes, uses, offers to sell, or sells" or "induces infringement" of a patented invention become liable for infringement under the meaning of *35 USC §271(a)(b)?*

Guidance can be found in the case law on similar issues. The standard for direct infringement was initially set in *NTP Inc. v. Research in Motion Ltd*. (Fed. Cir. 2005), which addressed the issue of whether a distributed wireless email system, is used "within the United States," where components crucial to the system's operation are located outside the United States, under *35 USC §271(a)*. The Court held that for an infringement of method claims, each and every step must be performed in the United States. However, on the other hand, for an infringement of system claims, the US must be the place where control of the system is exercised and beneficial use of the system is obtained. If a user of the system using an element of the claim is in the US, this may be considered beneficial use of the system.

The court continued its discussion of the standard of direct infringement of method claims in *Muniauction v. Thomson Corp. (Fed. Cir, 2008).* Muniauction's patent disclosed a system that let issuers run an auction and bidders submit bids using a web browser. Muniauction's claim required actions by both a bidder and an auction system. The court held that a method claim is directly infringed upon only when a single party can be found to have performed every step of the claim. This could not be found in Muniauction's method claim which required actions by two different parties. The Federal Circuit also affirmed that for a joint infringement, a party may be liable for infringement only if it can be shown that only one party exercises control or direction over the entire process.

In a recent decision, A*kamai v. Limelight (Fed. Cir 2010),* the Federal Circuit expanded its "control or direct" ruling. The Court ruled that a joint infringement requires an agency relationship or a contractual obligation to carry out the relevant steps. The Court did not find Limelight liable under the theory of joint infringement, as one of the method's steps in Akamai's patent was performed by Limelight's clients.

From the above discussion, it can be concluded that it would be far more difficult to establish a joint infringement liability, when multiple parties perform different parts of the claimed invention. Thus, enforcing of method claims, directed to a distributed execution of a software application, may be a challenge in US jurisdiction. System claims, on the other hand, can be enforced by showing that the infringement "is divided" by two parties, where either party exercises part of the claimed invention in service.

In summary, our recommendations when drafting claims related to cloud computing technology are:

A. Avoid method steps performed by end users;
B. Recite only method steps that are performed by a single party; and,
C. Include at least one system claim that recites at least one element that establishes a control and beneficial use of the system.