PROTECTING INNOVATION IN CLOUD COMPUTING

Christopher J. Palermo*

March 22, 2010

Cloud computing, a relatively recent technological innovation, is presently receiving considerable attention among entrepreneurs, technology financiers, and academics. If you have not yet represented a party whose inventions involve or relate to cloud computing, you will soon. But does cloud computing require fundamental changes in the way that practitioners approach patent drafting and claiming, or other issues of innovation or intellectual property protection? This article concludes that the answer is no, but that special sensitivity is needed to the particular technical context of cloud computing inventions in performing the ordinary services of patent counsel.

Let's begin with a brief tutorial on cloud computing technology. In general, cloud computing refers to data processing environments in which processors, operating systems and often applications are located remotely from the user in data centers, which may be private or quasi-public. Typically an end user accesses cloud resources over the Internet using a conventional browser on a PC, laptop or netbook. If the user can access servers, applications or services regularly, reliably and with good performance, then the user may become unconcerned about the physical location of the computers that are providing service; the computers may be at any endpoint in the "cloud" of networks and internetworks that we know as the Internet.

In private cloud computing, a business enterprise owns, operates or controls a data center and all the equipment in it, and delivers services or applications to its employees through secure network connections, or to customers through secure or non-secure connections. In some cases services or applications may be marketed as "software as a service" (SaaS, pronounced "sass") to indicate that the end user or customer does not locally install the software. Examples in the United States include sales force automation applications from Salesforce.com

or consumer-oriented tax preparation software from TurboTax. Indeed, some technologists contend that the application service provider (ASP) services introduced in the late 1990s and early 2000s are indistinguishable from what marketers are now terming "cloud computing."

In quasi-public cloud computing, service providers essentially rent the time of their computers or processors to individuals or companies, who temporarily load and run their own applications on the computers in the cloud, and then relinquish these resources when they are done. In some cases, the service providers operate their computers using multiple virtual machines; this approach can execute multiple unrelated operating systems and applications on the same physical computer, processor or processor core, whilst giving the customer the impression of having exclusive use. The development of reliable, secure virtualization software is responsible, in great part, for the availability and utility of quasi-public cloud computing. The dominant provider of virtualization software is VMWare. An example of a market-based renter of cloud computing resources is Amazon.com. Quasi-public cloud computing can allow an enterprise to temporarily use a large amount of processing power to serve a special need, or can permit a business to offer a flexible amount of service to its customers, so that the amount of processing power that it uses will vary according to customer demand.

How should patent attorneys approach providing effective intellectual property services to clients involved in cloud computing? We now consider and apply the numerous familiar concepts that are highlighted below.

1. **Risk Evaluation.** Many cloud computing businesses are startups or early stage enterprises. Investors and entrepreneurs will want their patent counsel to advise on the risk of infringement involved in starting up these businesses and offering services or applications using a cloud computing model. In most cases, providing an opinion on risk will be difficult to accomplish at reasonable cost. Fundamentally, cloud computing services involve client-server computing, so all patents previously issued that cover client-server inventions may be in play, including those issuing in emerging technology markets, such as Chinese patents. Searching for, collecting

and evaluating the thousands of patents relating to client-server computer may be troublesome at any practical cost. Further, even if all applicable patents could be found, an excessively high royalty load would probably occur if the enterprise sought to obtain licenses to all patents arguably valid and infringed by the enterprise's technology and for which no design-around option existed. Therefore, some form of risk shifting by contract may be necessary. For example, an enterprise that is planning to contract with a third party data center provider should recognize that cloud computing involves the use of certain relatively new virtual machine and application virtualization technologies, which may be covered by relatively recent patents. It may be reasonable to ask the service provider to bear the risk of any infringement of these patents—at least to the extent that the client's particular application is not implicated in infringement. While it is natural for data center provider will want to minimize its own business risk by disclaiming all such liability, it may be reasonable for the new enterprise to ask the provider to "stand behind" its service. A complete discussion of all issues involved in contracting for cloud computing services is beyond the scope of this article, but many legal questions of that context are basically the same as those encountered in other kinds of independent contractor agreements, or even in the "service bureau" agreements that originated in the 1960s.

2. **Divided Infringement and Extraterritoriality.** Avoiding patent claims that cause divided infringement, at least in those jurisdictions known to lack legal remedies for it, will be a paramount concern in drafting patents for inventions relating to cloud computing. By divided infringement, we mean a situation in which a claim mandates action by different, unrelated parties for at least two steps of a process claim or two elements of an apparatus claim.[1] In this situation, in some jurisdictions an infringement claim is impossible because of the legal axiom that a single party must make, use, sell, or import all elements of the claim for infringement to arise.[2] When a

claim is possible, the patent owner must establish that the defendant exercises control over a third party so that the third party's acts should be attributed to the defendant.[3] For example, a process patent claim that recited steps performed by a JavaScript program executed in the end user's browser, and steps performed by the server application in the cloud, or even steps of the internetworking appliances that carry packets between client and server, may have no enforcement value because no single party uses all such steps, or makes or sells an apparatus that can be made to perform all such steps in ordinary operation. In the United States, this effect can be mitigated in some cases by drafting "system" or "apparatus" claims. Because the basic US infringement statute implicates "use" of a patented apparatus, a claim that recites multiple elements that are made or sold by two or more parties could be valuable if infringed by a third party who makes use of all the elements for profit, as revealed in the *BlackBerry* cases.[4]

3. **Knowing the Target and Detecting Infringement.** Drafting effective, valuable claims for cloud computing inventions also will require conscious definition of the parties who are likely to infringe, and focusing the claims on their conduct. For example, most cloud computing innovations will be found in the data processing logic involved in the server-side application, some will be found in the logic involved in client-side code that is transmitted to and executed in the browser, and perhaps a few will be found in new kinds of protocols or interactions between client and server, or between server and internetworking devices such as cloud routers and switches. Patent claims should be drafted so that they will be infringed by the appropriate competitor or other third party. For example, if the "point of novelty" is found in server-side logic, then steps or elements of the network infrastructure of the data center or the Internet should not be recited. If the key innovation lies in a new snippet of JavaScript that produces an unusual browser interaction once downloaded and executed, then the claim may have to be drafted in terms of causing an effect

upon execution, or in terms of the structure of the JavaScript. Thus, most claims will relate to pre-processing steps, or post-processing steps, without reciting acts that occur within the cloud. These claims should be "tested" by re-reading them and asking, which party will infringe? If the answer is "the end user operating a browser" or "the Internet service provider" then the value of the claims could be called into question, as these parties may be undesirable to sue for infringement. Moreover, counsel should consider whether it will be possible to determine whether any other party is actually infringing—that is, whether infringement will be detectible. In many cases, claims that exclusively read on processing steps performed "in the cloud" will be impossible to detect in third-party cloud-based systems.

4. **Inventive Step: Leapfrogging *Leapfrog*.** Claims that pass the test posited in the preceding paragraph also must be novel and possess inventive step with respect to the prior art. In the United States and many other jurisdictions, merely "cloudifying" a previously known process will not confer inventive step. In the United States in particular, the Court of Appeals for the Federal Circuit has held that merely applying computer automation to a previously known process will not defeat a finding of non-obviousness.[5] Therefore, at the time that an invention is disclosed or identified, patent attorneys and agents will need to help clients identify a point of novelty or inventive step that resides in the substantive data processing or machine configuration involved in the invention, and not merely in the idea that known steps or apparatus have been moved "into the cloud."

5. ***Macrossan-Aerotel* and *Bilski*: The Usual Suspects.** Many inventions arising from cloud computing will be realized in software. Therefore, the disclosure as a whole and the claims must be drafted with sensitivity to the four-part *Macrossan-Aerotel* test, and the two-part *Bilski* test as presently applied. If the disclosure is likely to be filed in the European Patent Office after a first filing in the UKIPO or the USPTO, then Article 52 and applicable case law must be considered. The disclosure

should be sprinkled with information that will satisfy applicable judicial *dicta* in post-*Macrossan-Aerotel* cases. In the United States, at present the claims must be "tied to a particular machine" or involved in a transformation of an article. If the only applicable "machine" is in the cloud, satisfying the *Bilski* test whilst drafting a claim that avoids divided infringement and covers the detectible acts of a third party in a valuable way may be troublesome.

6. **Knowledge of Foundation Technologies.** Cloud computing relies on the integration and interplay of several technologies that have been applied in other contexts for many years. Patent attorneys who have not previously worked with these technologies may wish to consider reading tutorial matter to establish a solid foundation for understanding and advising on cloud computing inventions. Example foundation technologies include public key encryption, virtual machines and program virtualization, storage virtualization, content delivery networks (CDNs), internetworking protocols for managing autonomous network domains (e.g., Border Gateway Protocol [BGP]), browser-side scripting and automation using JavaScript and AJAX, re-imaging of operating systems and applications, automated bootstrap loading and shutdown, and parameterization of universal resource locators (URLs).
7. **Privacy and Data Protection.** If the services or applications of a cloud computing enterprise will store personal information, financial data or healthcare data in cloud-based storage systems or other resources, then myriad privacy and data protection laws of Britain, the European Union, the United States and other jurisdictions are implicated. Germany, in particular, has some of the most restrictive and intractable laws relating to protection of consumer data. Indeed, commentators have observed that cloud computing may be fundamentally incompatible with EU data protection directives and therefore a cloud computing ecosystem may be impossible to develop in Europe.[6] Compliance with these laws is beyond the scope of this article. However, awareness of privacy and data protection concerns is useful, because

some clients may be unaware of their obligations and patent counsel may need to spot such cross-over issues and recommend the involvement of knowledgeable solicitors or regulatory consultants.

Cloud computing involves fascinating technology and holds the promise of providing effective, reliable, always-available new services to consumers and enterprises, without burdening enterprises with the intensive capital costs of building out a data center for each newly conceived service or application. Many familiar legal issues will be involved in drafting valuable patents for cloud computing inventions. Better practitioners will review these issues and consider how to apply them intelligently given the special technical context of cloud computing environments.

---

[1] Mark A. Lemley, "Divided Infringement Claims," American Intellectual Property Law Association Quarterly Journal, Vol. 33, 255, 2005.

[2] *Id*.

[3] *BMC Resources, Inc. v. Paymentech, L.P.*, 498 F.3d 1373 (Fed. Cir. 2007).

[4] *NTP v. Research in Motion, Inc.*, 418 F.3d 1282 (Fed. Cir. 2005).

[5] *Leapfrog Enterprises Inc. v. Fisher-Price Inc.*, 485 F.3d 1157 (Fed. Cir. 2007).

[6] Remarks, Thomas Fetzer, Univ. of Mannheim Law School, at "Emerging Law & Policy Issues in Cloud Computing," University of California Boalt Hall School of Law, International House, Berkeley, California, March 12, 2010.

* Christopher J. Palermo is a co-founder and partner in Hickman Palermo Truong & Becker LLP, San Jose, California, and is a Foreign Member of CIPA. Perhaps taking the cloud computing metaphor too literally, the author wrote this article at 39,000 feet during a flight between Chicago and San Jose.