I.  INTRODUCTION

“Cloud Computing” is a relatively new term used to describe a general approach to providing computing services through a communications network, typically the Internet. Whole sectors of the application service provider industry, both for enterprise-level and consumer-level applications, take advantage of cloud computing resources. Those who provide legal services to either providers of cloud computing services, or consumers of cloud computing services, would be well-advised to understand the technical and business background of cloud computing, how cloud computing can change traditional software services, what some of the major new risk and legal issues are, and how fundamental or traditional legal doctrines can be applied to this new mode of computing. Whether or not an IP attorney has clients directly involved in providing cloud computing services, it appears that IT departments for many companies are exploring the use of cloud computing, and thus companies and entities which have their own IT and MIS needs will at some point will be faced with some cloud computing issues. Accordingly, attorneys who advise companies or entities of any size which have substantial IT needs should have familiarity with this new area of technology. This may be viewed analogously to the situation in the early dot-com era, when companies in traditional industries and their counsel had to adapt and understand legal and technical issues created by the Internet. Accordingly, in the discussion that follows, an introductory overview of legal issues potentially raised by cloud computing will be presented. In this exciting era of increasing development of computing models and the ever-growing computing resources available to companies and enterprises, the changing landscape as legal doctrines

1 Peter Kang is a Partner in the Intellectual Property Litigation practice group and head of the Korea IP Practice, Sidley Austin LLP (Palo Alto, CA office). The materials presented herein are for discussion purposes only, are exclusively those of the author, and do not necessarily reflect the views of the Firm, the Firm’s partners, or any of the Firm’s clients.
and norms should develop concurrently with the development of this sector of the computing and applications industries.

II. Overview of Cloud Computing – Technical Features

What is cloud computing? Why is it called “cloud” computing? What is the “cloud”? According to one source, the first published use of the term “cloud” to describe the Internet was a 1997 paper presented by Sharon Gillett and Mitch Kapor (well-known computer industry figure, and founder of Lotus and the Electronic Frontier Foundation among others) at a 1996 Kennedy School of Government conference on the Internet. See http://www.johnmwillis.com/cloud-computing/who-coined-the-phrase-cloud-computing/ (Dec. 31, 2008) (citing Sharon Gillett and Mitchell Kapor, The Self-governing Internet: Coordination by Design, in Coordination of the Internet (Brian Kahin and James Keller eds., 1997) (available at http://css.mit.edu/papers/CCSWP197/CCSWP197.html). Figure 1 of the Gillett and Kapor paper is reproduced below:

More recently, U.S. Patent No. 7,596,620 appears to be the first issued U.S. patent which states broadly in its first sentence that “[t]he present invention relates to cloud computing.” See U.S. Patent No. 7,596,620 at col. 1:19 (hereafter, “the ‘620 Patent”). The ‘620 patent states that “[i]n general terms,
cloud computing provides a developer (individual or company) to have access to resources for a Web
application, in particular a web site. Various vendors provide cloud computing to the developer
community. Such vendors include JOYENT (see joyent.com), Amazon Web Services (See
amazon.com), Google App Engine (see http://code.google.com/appengine/) and others.” Id. at col. 1:23-
30. The ‘620 Patent provides the following definition of “cloud computing”: “Cloud computing is
generally defined as using computing resources, primarily servers, owned by a third party provider (such
as the AMAZON ELASTIC COMPUTE CLOUD, JOYENT, and GOOGLE APPS) such that the user
does not need to make a substantial investment in computer hardware and scale resources depending on
the user's needs. Cloud computing primarily involves Web applications but can include storage, raw
computing and other specialized services.” Id. at col. 1:59-67. Figure 1 of the ‘620 Patent is reproduced
below:

As the figures and descriptions above make clear, the “cloud” is a conceptual or descriptive term
for describing a set of computing resources which are connected in a communications network such that,
from the consumer standpoint, the hardware and structural details of that network are essentially invisible. The computing resources provided to the user or developer from the “cloud” are managed or provided by a cloud resource provider company.

One technical feature of cloud computing is the lack of geographical or physical information about the actual hardware making up the cloud. Cloud service providers take advantage of large data centers distributed nationwide (and in some cases worldwide) and networked in such a way that it may become difficult to specify "where" data is physically stored at any given point in time. Indeed, data may be dispersed across and stored in multiple data centers all over the world. One of the strengths of using cloud resources is that the “cloud” makes it possible and practical to store multiple copies of data in different physical locations to allow for faster access. Even a "private cloud" that is essentially run by a single entity can still use multiple physically dispersed data centers. Therefore, data in a cloud may be transferred across multiple national borders.

The term “cloud computing” is sufficiently elastic to cover many types of specific services, and thus as the industry develops, it may become important to distinguish between types of services particularly when discussing legal issues.² For example, services that may be available through cloud platforms include:

- Data storage (e.g., infrastructure as a service (IaaS)),

- Application development/deployment (e.g., platform as a service (PaaS))

² Indeed, in 2008 Larry Ellison, CEO of Oracle, colorfully commented as follows upon the lack of specific definition of the term “cloud computing”: “The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?” See http://news.cnet.com/8301-13953_3-10052188-80.html.
• Software hosting (e.g., software as a service (SaaS))

Rather than installing and maintaining data/software on a network or desktop computer, the data/applications are hosted on computers in the “cloud” and available on demand. For example, when buying and using IaaS, instead of storing data on an organization's own computer network, the data is stored on servers "in the cloud" and available on demand by the organization which is the customer of the cloud service provider.

III. Overview of Cloud Computing – Business Features

As shown above, instead of data processing and storage occurring on an individual's laptop or desktop computer (or on a company's internal network), cloud computing uses hardware and software platforms run by third parties as a business in which such third parties act as providers of the computing resources to their customers. This is a growing industry, and current examples of cloud computing service providers include companies such as Google, Amazon, and others. One conceptual representation of the “cloud computing” business as of 2010 is reproduced below:

One apparent driver of the growth of cloud computing is the cost savings touted by service providers. Companies using cloud services need not purchase their own infrastructure or software. See ‘620 Patent at col. 1:59-67 (defining cloud computing “such that the user does not need to make a substantial investment in computer hardware” and cloud computing can “scale resources depending on the user's needs.”). In other words, a customer of a cloud service need not maintain and continuously upgrade the hardware and software of that company’s internal computer network and systems. Moreover, companies using cloud services need not hire people to maintain the internal computer network and software to run that network. Also, companies using cloud services need not regularly update software (or hardware) when necessary – those who work for companies (or law firms) in which versions of word processing programs or email applications are constantly being upgraded for security patches, new revisions issued by the software vendor, and bug fixes, will understand the disruptions that can be caused by such constant upgrades, and can readily appreciate the cost savings possible if such maintenance is outsourced to a vendor like a cloud service provider. Cloud service customers theoretically take advantage of the best and latest technology since they will not have to disassemble and rebuild their entire IT infrastructure in order to upgrade.

Cloud computing service providers also may emphasize that one benefit of cloud computing may be that the model is highly and relatively inexpensively scalable. Typically, corporations must over-invest in their IT infrastructure in order to be able to handle peak computing requirements, since disruption of IT services during high-demand periods can have amplified negative impact on a business. This results in IT resources being under-utilized on average during more “normal” non-peak demand time periods. “Given that many companies over-maintain their IT capacity and usually cannot
effectively use it all, it may be beneficial to purchase ready-to-use IT services from skilled hands and only pay for the usage.” See H. Du and Y. Cong, *Cloud Computing, Accounting, Auditing, and Beyond*, 80 CPA J. 66, 68 (Oct. 2010). The lack of economic efficiency in such over-investment is an argument in favor of cloud computing. Customers of cloud computing services therefore do not need to maintaining an over-capacity of computing power (e.g., extra servers only used for the holiday e-commerce rush). Customers of cloud services have the flexibility to access variable capacity levels to suit their immediate needs using the cloud.

Cloud computing is sometimes described as or referred to in terms of a “utility” model. See D. Wyld, *The Utility of Cloud Computing as a New Pricing – and Consumption – Model for Information Technology*, 1 Int’l J. of Database Mgt. Sys. 1, 4 (2009) (“it has been suggested that the move to the cloud model could make computing the fifth utility (along with water, electricity, gas, and telephone”)”). In this sense, cloud computing can be viewed as being analogous to a grid of utilities like electricity companies and providers. During summer time, for example, a particular electricity company may not be able to generate enough electricity to meet increased peak demand. That utility will then have to purchase electricity from other providers who are not at full capacity. By analogy, in cloud computing, data computing can be viewed like electricity, able to be moved instantaneously to make available servers and computation resources where needed. Thus, one feature of cloud computing is the ability of cloud service providers to access the cloud resources of other cloud services when needed to meet particularly high demand. Indeed, some cloud computing providers charge for use of cloud services in a way similar to the way utilities charge for electricity: based on how much is used (KW/Hour vs. computing cycles).
IV. Cloud Computing and Potential Legal Issues

With the above technical and business features in mind, it becomes apparent that a multitude of potential legal issues can arise in the context of cloud computing. The discussion below is not intended to be exhaustive, but rather illustrative primarily of intellectual property law issues, with an overview of other areas of law potentially impacted by cloud computing. As with this area of technology and business, the legal issues will likely evolve and change as the business and technical models evolve.

A. Cloud Computing and Intellectual Property Law Issues


The spread of cloud computing has potential impacts on patent issues in several ways. As an initial matter, the growth of cloud computing in industry is mirrored in cloud computing’s growth in the patent world. The numbers of patents relating to “cloud computing” is about to undergo dramatic growth – there are currently only ten issued U.S. patents which contain the term “cloud computing” but there are over 750 published U.S. patent applications which contain that same term.3 Thus, as with most new technical areas, companies and their attorneys are rushing to fill in the field of patents relating to cloud computing. Therefore, it is to be anticipated that there will be increasing licensing and litigation

---

3 According to U.S. PTO data, as of January 11, 2011, there are ten (10) issued U.S. patents which contain the term "cloud computing". The earliest such patent is U.S. Patent No. 7,593,935 (issued Sept. 22, 2009) and the patent with apparently the earliest published claim to priority is U.S. Patent No. 7,636,764 (a continuation of a parent application filed on Sept. 29, 2008). As noted above, the ‘620 Patent appears to be the first issued patent to simply state that it relates to “cloud computing.” By contrast, according to U.S. PTO data, as of January 11, 2011, there are over 750 published U.S. Patent Applications which contain the term “cloud computing”. Thus, it is apparent that the number of patents containing the term “cloud computing” has the potential to increase by two orders of magnitude in the foreseeable future.
issues in the future relating to cloud computing technology, as portfolios expand and IP positions among competitors in this field are developed.

Patents have value in part when they can be asserted, and such assertions require investigation and due diligence into the activities of a potential target of such assertion. One of the initial challenges posed by cloud computing is the difficulty in investigating the physical hardware and processes used by cloud resources, in order to perform a reasonable pre-filing investigation into possible infringing activity. See Fed. R. Civ. P. 11. Under Rule 11, “[i]n bringing a claim of infringement, the patent holder, if challenged, must be prepared to demonstrate to both the court and the alleged infringer exactly why it believed before filing the claim that it had a reasonable chance of proving infringement.” View Eng’g, Inc. v. Robotic Vision Sys., 208 F.3d 981, 986 (Fed. Cir. 2000) (applying Ninth Circuit law under Rule 11). Because by definition cloud resource providers utilize private resources for their customers’ uses, there is typically a confidential and certainly non-public relationship between the cloud resource provider and the customer.

Moreover, cloud service providers generally intend for their services to be seamless and essentially invisible infrastructure from the users’ perspective. See Du and Cong at 70 (“The client IT environment in the cloud is drastically different from one on the company’s premises. The computing services are scattered around, perhaps invisible and unreachable in the cloud.”). Thus, there may be no easily publicly accessible method for investigating the processes, software, or physical infrastructure of a cloud service provider’s platform. In addition, cloud service providers have an industry bias towards keeping the details of their data centers secret. See E. Messmer, Cloud computing secrecy raises IT security risks, Network World US, available at http://features.techworld.com/data-centre/3229374/cloud-computing-secrecy raises-it-security-risks/ (July 6, 2010) (“Cloud service providers often cultivate an aura of secrecy about data centres and operations, claiming this stance
improves their security even if it leaves everyone else in the dark…. data centre locations and practices are treated like national security secrets. But public cloud service providers argue their penchant for secrecy is appropriate for the cloud model - and at any rate, everyone's doing it.”). As with internet infrastructure companies, cloud service providers pose challenges to patent owners in terms of making unavailable the kinds of details one might optimally desire to review in examining a system for potential infringement. This, in turn, makes claim drafting for offensive or assertion purposes that much more challenging for patent owners and prosecutors.

Another issue raised by cloud computing is the borderless nature of cloud computing resources. As noted, cloud service providers tend to be fairly secretive about the technical details of their data centers, and this can include even a lack of transparency of the physical location and setup of the data centers. See id. (one cloud service provider “acknowledged that there has been some secrecy about where things are located because ‘we think it’s a security risk.’”). Several cloud service providers do identify to some extent where their data centers are located, and for some of them, those centers are located in jurisdictions outside the United States. See, e.g., J. Peterson, “Data Center in Singapore opened by Salesforce.com”, Top News Singapore, available at http://www.topnews.com.sg/content/270-data-center-singapore-opened-salesforcecom (July 16, 2009).

The lack of concrete information on location, and the fact that some resources are located outside the U.S., can both raise extraterritoriality concerns. Under Section 271(a), U.S. patents are infringed by activity that occurs “within the United States” and there is in general no extra-territorial application of direct infringement assertions of a U.S. patent (although as with many areas of law, there are exceptions relating to indirect infringement issues and issues relating to provisions such as 35 U.S.C. §§ 271(f) and 295). Cf., e.g., Zoltek Corp. v. United States, 442 F.3d 1345, 1364 (Fed. Cir. 2006) (addressing infringement claim against United States arising from Court of Claims involving overseas activity under
35 U.S.C. § 1498(c)). Accordingly, determining and proving whether infringing activity is actually subject to U.S. patent law can be a challenge for patent owners in this technical field.

A patent infringement issue related to the business of cloud service providers potentially impacts both claim drafting and claim interpretation. For cloud services to work in practice, there is of course an end user or customer of the services. Accordingly, in the context of cloud computing, the business model assumes (like the internet) that there is a communication network or path linking the user or customer and the cloud resources. This creates a potential issues for a divided infringement rebuttal to an infringement claim, depending on how a claim is drafted. The Federal Circuit recently held that divided infringement will defeat a claim of patent infringement unless there is an agency relationship between the actors accused of the infringing activity:

It is well settled that direct infringement requires a single party to perform every step of a claimed method. In both *BMC Resources* and *Muniauction* this court confronted the situation in which more than one party is required to perform the steps of a claimed method.… While control or direction is a consideration, as is the extent to which instructions, if any, may be provided, what is essential is not merely the exercise of control or the providing of instructions, but whether the relationship between the parties is such that acts of one may be attributed to the other…. [T]he performance of a method step may be attributed to an accused infringer when the relationship between the accused infringer and another party performing a method step is that of principal and agent, applying generally accepted principles of the law of agency as explicated by the Supreme Court and the Restatement of Agency. The Restatement defines agency as "the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act." For an agency relationship to exist, and thus, for infringement to be found, both parties must consent that the agent is acting on the principal's behalf and subject to the principal's control.… In assessing infringement based on the actions of joint parties, it is not enough to determine for whose benefit the actions serve, for in any relationship there may be benefits that inure in some respects to both parties. This court therefore holds as a matter of Federal Circuit law that there can only be joint infringement when there is an agency relationship between the parties who perform the method steps or when one party is contractually obligated to the other to perform the steps.

Accordingly, prudent patent claim drafting strategies may consider recognizing the risk in including claim limitations, such as in method claims, in which certain process steps are performed by unaffiliated third parties such as end-users.

While acknowledging the difficulty of proving infringement of claims that must be infringed by multiple parties, this court has noted that such concerns ‘can usually be offset by proper claim drafting. A patentee can usually structure a claim to capture infringement by a single party.’... This court also observes that in addition to initially structuring a claim to capture infringement by a single party, patentees may be able to correct a claim that can only be infringed by multiple parties by seeking a reissue patent. *Akamai*, 2010 U.S. App. LEXIS 25825 at 23-24 (internal citations omitted). Avoiding a claim of divided infringement can be important for strengthening patent portfolio development; however, there can be a tension inherent in such claim drafting strategy with the need to draft definite claims in which the essential elements are appropriately interrelated where necessary. See 35 U.S.C. § 112, ¶ 2; MPEP § 2172.01 (“a claim which fails to interrelate essential elements of the invention as defined by applicant(s) in the specification may be rejected under 35 U.S.C. 112, second paragraph, for failure to point out and distinctly claim the invention.”). Prudent counsel would therefore consider taking proper steps to balance these competing interests in developing cloud computing-related claim language appropriately.

Therefore, in light of the developments in cloud computing and the expansion of this technology, patent portfolio managers and their counsel should consider claim drafting strategies for cloud computing related inventions in light of the goals of minimizing or avoiding rejections (or later invalidity findings in litigation) while developing claims which can be properly asserted under U.S. law and which avoid both extraterritorial issues and divided infringement issues.
2. Cloud Computing and Business Methods

As discussed above in the context of infringement related legal issues, cloud computing raises issues for patent prosecution attorneys and agents, as well as portfolio managers. The distributed nature of cloud computing and the technical/business features described above create additional potential challenges and opportunities for strategic patent development. One evolving area of law is the Supreme Court’s recent decision on business method patents. *Bilski v. Kappos*, No. 08-964, 561 U.S. -, 2010 U.S. LEXIS 5521 (June 28, 2010).

Under Section 101, “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” 35 U.S.C. § 101. In *Bilski*, the Court reaffirmed the “three specific exceptions to 101’s broad patent-eligibility principles: ‘laws of nature, physical phenomena, and abstract ideas.’” *Bilski*, slip op. at 5 (recognizing “these exceptions have defined the reach of the statute as a matter of statutory stare decisis going back 150 years.”). The Court first rejected the Federal Circuit’s attempt to require all patentable subject matter to satisfy the so-called “machine or transformation test” under Section 101:

> It is true that patents for inventions that did not satisfy the machine-or-transformation test were rarely granted in earlier eras, especially in the Industrial Age .... The machine-or-transformation test may well provide a sufficient basis for evaluating processes similar to those in the Industrial Age – for example, inventions grounded in a physical or other tangible form. But there are reasons to doubt whether the test should be the sole criterion for determining the patentability of inventions in the Information Age.... [T]he machine-or-transformation test would create uncertainty as to the patentability of software, advanced diagnostic medicine techniques, and inventions based on linear programming, data compression, and the manipulation of digital signals.... The Information Age empowers people with new capacities to perform statistical analyses and mathematical calculations with a speed and sophistication that enable the design of protocols for more efficient performance of a vast number of business tasks. If a high enough bar is not set when considering patent applications of this sort, patent examiners and courts could be flooded with claims that would put a chill on creative endeavor and dynamic change. In
searching for a limiting principle, this Court’s precedents on the unpatentability of abstract ideas provide useful tools.

*Id.* at 8-9, 12 (internal citations omitted).

Next, the Court held that, as a general matter, business methods can be patentable subject matter under Section 101, although such patents must do more than claim abstract ideas or mathematical algorithms. *Id.* at 10-16 (holding claims at issue invalid for improperly attempting to claim abstract idea). In an interesting discussion which appears to apply directly to new developments in cloud computing, the Court also particularly noted the challenges posed by evolving technology:

But times change. Technology and other innovations progress in unexpected ways. For example, it was once forcefully argued that until recent times, “well-established principles of patent law probably would have prevented the issuance of a valid patent on almost any conceivable computer program.” But this fact does not mean that unforeseen innovations such as computer programs are always unpatentable. Section 101 is a “dynamic provision designed to encompass new and unforeseen inventions.”… It is important to emphasize that the Court today is not commenting on the patentability of any particular invention, let alone holding that any of the above-mentioned technologies from the Information Age should or should not receive patent protection. This Age puts the possibility of innovation in the hands of more people and raises new difficulties for the patent law. With ever more people trying to innovate and thus seeking patent protections for their inventions, the patent law faces a great challenge in striking the balance between protecting inventors and not granting monopolies over procedures that others would discovery by independent, creative application of general principles. Nothing in this opinion should be read to take a position on where that balance ought to be struck.

*Id.* at 8-10 (internal citations omitted).

The first post-*Bilski* Federal Circuit opinion provides the following guidelines on patentability of business methods:

In refocusing the eligibility inquiry of the statute, the Supreme Court advised that section 101 eligibility should not become a substitute for a patentability analysis related to prior art, adequate disclosure, or the other conditions and requirements of Title 35. In other words, section 101 does not permit a court to reject subject matter categorically because it finds that a claim is not worthy of a patent…. The parties do not dispute, and this court agrees, that the inventors do not purport to have invented laws of nature or physical phenomena. Indeed, the Supreme Court in *Bilski* refocused this court’s inquiry into processes on the question of whether the subject matter of the invention is abstract. The
Supreme Court did not presume to provide a rigid formula or definition of abstractness. Instead, the Supreme Court invited this court to develop “other limiting criteria that further the purposes of the Patent Act and are not inconsistent with its text.” With that guidance, this court also will not presume to define “abstract” beyond the recognition that this disqualifying characteristic should exhibit itself so manifest as to override the broad statutory categories of eligible subject matter and the statutory context that directs primary attentions on the patentability criteria of the rest of the Patent Act.


In holding the claims at issue patentable subject matter, the Federal Circuit also held that claims which incorporate mathematical algorithms are not invalid for abstractness for that reason alone:

The invention presents functional and palpable applications in the field of computer technology…. Indeed, this court notes that inventions with specific applications or improvements to technologies in the marketplace are not likely to be so abstract that they override the statutory language and framework of the Patent Act. This court also observes that the claimed methods incorporate algorithms and formulas that control the masks and halftoning. These algorithms and formulas, even though admittedly a significant part of the claimed combination, do not bring this invention even close to abstractness that would override the statutory categories and context. The Supreme Court has already made abundantly clear that inventions incorporating and relying upon even "a well known mathematical equation" do not lose eligibility because "several steps of the process [use that] mathematical equation."

*Id.* at 19-20 (internal citations omitted).

As discussed above, much of the development of cloud computing relates not only to technical development of the “cloud” (and methods of communicating and integrating data in and to/from the cloud) but also relates to business models for cloud computing. For example, business models such as PaaS, IaaS, and SaaS have proliferated due to the technology enabled by cloud computing. In light of the developing case law under *Bilski*, it appears that prudent patent attorneys and their clients should take steps to avoid Section 101 issues by tailoring claims appropriately to avoid unduly abstract processes, as well as the other requirements of the Patent Act such as the written description requirement. As the Federal Circuit noted:
this court notes that an invention which is not so manifestly abstract as to over-ride the statutory language of section 101 may nonetheless lack sufficient concrete disclosure to warrant a patent. In section 112, the Patent Act provides powerful tools to weed out claims that may present a vague or indefinite disclosure of the invention. Thus, a patent that presents a process sufficient to pass the coarse eligibility filter may nonetheless be invalid as indefinite because the invention would ‘not provide sufficient particularity and clarity to inform skilled artisans of the bounds of the claim.’ That same subject matter might also be so conceptual that the written description does not enable a person of ordinary skill in the art to replicate the process.

See Research Corp. Techs., slip op. at 16-17) (internal citations omitted).

3. Cloud Computing and Inventorship Issues

Another patent law issue raised by cloud computing stems from the borderless nature of cloud computing. Specifically, the technical nature of cloud computing has potential impact on priority contests under Section 102(g). Under Section 102(g)(2):

A person shall be entitled to a patent unless … before such person’s invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it. In determining priority of invention under this subsection, there shall be considered not only the respective dates of conception and reduction to practice of the invention, but also the reasonable diligence of one who was first to conceive and last to reduce to practice, from a time prior to conception by the other.


Contests to swear behind references under § 102(g)(2) occur commonly in prosecution as well as in litigation contexts. The territorial requirement (“in this country”) of § 102(g)(2) has implications for the borderless cloud computing environment. First, companies may be based in the U.S. but may use cloud resources for computing and documentation purposes, and it is entirely possible that such cloud resources may be located in data centers outside the United States. As discussed above, cloud resource providers have data centers around the world, and when in need, may sub-contract on a temporary basis for use of fourth-party data centers during periods of peak demand and those additional data centers may in turn be located outside the United States. If a particular inventor uses cloud computing resources in
the process of conceiving a particular invention, a question may arise theoretically as to whether that
conception occurred “in this country” or not. See 35 U.S.C. § 102(g)(2).

Moreover, conception must be corroborated by evidence. In re Jolley, 308 F.3d 1317, 1321
(Fed. Cir. 2002) (“Because conception is a mental act, ‘it must be proven by evidence showing what the
inventor has to disclosed to others and what that disclosure means to one of ordinary skill in the art.’”) (internal citations omitted). If the corroborating evidence were contemporaneously created and stored on cloud resources located outside the United States, there exists likewise a theoretical legal question as to whether this evidence qualifies as sufficient corroboration of invention “in this country.”

Moreover, there is a potential legal issue relating to establishing diligence in reduction to practice under § 102(g)(2). Foreign activities may not be relied upon to show diligence under § 102(g)(2). Scott v. Koyama, 281 F.3d 1243, 1247 (Fed. Cir. 2002) (“Reduction to practice in the United States requires that the invention be embodied in tangible form in the United States, not simply reported.”). Thus, if an inventor uses cloud resources located outside the United States to reduce to practice for example an alleged software-related invention, such use of cloud resources extraterritorially

---

4 Under Section 104, “[i]n proceedings in the Patent and Trademark Office, in the courts, and before any other competent authority, an applicant for a patent, or a patentee, may not establish a date of invention by reference to knowledge or use thereof, or other activity with respect thereto, in a foreign country other than a NAFTA country or a WTO member country, except as provided in sections 119 and 365 of this title.” 35 U.S.C. § 104(a)(1). Therefore, in interferences for example, a patentee or applicant in appropriate cases could theoretically rely upon activities in a NAFTA or WTO country to establish an earlier date of invention. This raises potential legal issues for those inventors whose companies use cloud computing resources located in a non-NAFTA and non-WTO country, since such inventors would be theoretically challenged in reliance on evidence of activities using such cloud resources to establish an earlier invention date. Conversely, an inventor who uses cloud resources in a NAFTA or WTO nation could theoretically consider relying upon activities carried out using such cloud resources to establish an earlier invention date, even if for example such inventor were physically located in a non-NAFTA and non-WTO nation.
may be rejected as a basis to show reduction to practice in the United States. In this context, the technical features of cloud computing which enable the development of an alleged invention may also impair the ability to show diligent reduction to practice of that same invention. This issue arises because of the borderless nature of cloud computing.

A similar issue arises for inventors based outside the U.S. who use cloud resources located within the United States. The Federal Circuit has held that conception that occurs overseas may be afforded a U.S. conception date as of the date of a proven communication or disclosure of the conception into the United States. “Thus the inventor of an invention of foreign origin may rely on the date that the invention was disclosed in the United States, as a conception date for priority purposes.” Scott, 281 F.3d at 1247. Thus, there is the possibility that a foreign inventor may consider reliance on the “disclosure” of a conception into the United States by virtue of the use of cloud resources located in the United States, for purposes of establishing a § 102(g)(2) conception date. Moreover, assuming such use of U.S.-located cloud resources qualifies as “in this country” then such overseas inventor could likewise theoretically attempt to rely on work documented on those cloud resources to establish diligent reduction to practice in this country. Scott, 281 F.3d at 1247. Thus, in such situation, an overseas inventor would benefit from the international nature of cloud computing.

In both interference and litigation contexts, there is also potentially a discovery and evidentiary issue raised by the use of cloud resources located outside the United States. There may be issues concerning identifying where the data or evidence is physically located which allegedly shows conception and/or diligent reduction to practice. For example, there may be evidentiary questions on whether that data has been moved from one set of cloud resources (in one nation) to another set of resources (in another nation), or whether it be established that the data is geographically located in the same place now as it was at the relevant time period. With respect to discovery of such information in
the cloud, there may be an issue as to whether a party can take effective third party discovery from the cloud service provider, for example if that provider is not located in a Hague Convention signatory nation.

4. Cloud Computing and Other IP Issues

The discussion above has focused on cloud computing’s potential interplay with certain patent issues. There are potential other intellectual property law issues raised by cloud computing, of course, as with any field of technology. A non-exhaustive overview of such other intellectual property issues includes the following:

The very nature of cloud computing involves the outsourcing of IT infrastructure by the customer to a service provider. Under some service agreements, a cloud service provider may have the option (and indeed may have the need) to use fourth or fifth party service providers in order to meet peak demand for computing resources. This sub-contracting and downstream use of unknown service providers raises potential legal issues. Under the Uniform Trade Secrets Act, a trade secret must be kept secret: “‘Trade secret’ means information … that … is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” Uniform Trade Secrets Act, § 1(4). In the context of trade secret law, there is a potential or theoretical legal issue raised by the sharing or distribution of confidential information to such service providers and their sub-contractors:

Another concern involves data security when proprietary corporate information and confidential customer data are being transmitted, processed, and stored in the cloud. Data confidentiality becomes an issue when data are being stored in a third-party location. Cloud service users may always be haunted by the fear of their data being spied upon by the provider or its employees at its data centers.

See Du and Cong at 68. Thus, a possible legal issue can arise with regard to whether confidentiality of alleged trade secret information has been adequately maintained and preserved, especially in situations
involving sub-contractors who are not in privity with the developer of the confidential information. These legal issues raise obvious concerns about adequacy of security and confidentiality agreements.

Similarly, in the context of patent law, distribution to multiple third parties of confidential information relating to an alleged invention through cloud computing arrangements raises at least a theoretical issue as to whether such distribution though the “cloud” constitutes a form of “public knowledge” prior art. See 35 U.S.C. § 102(a). This can be particularly an issue for consideration in situations in which the developer of the alleged invention is not in direct privity with the sub-contractors of a cloud service provider, and thus has no direct confidentiality relationship with at least some parties with access to the alleged conception or inventive information. The Federal Circuit has held that even a relatively modest disclosure of information by a single person to a relatively small group of third parties, in the absence of affirmative steps to conceal, can lead to an invalidating “public knowledge” under § 102(a). See Ormco Corp. v. Align Tech., Inc., 463 F.3d 1299, 1305-06 (Fed. Cir. 2006) (invalidating patent based on public knowledge from one dentist to his patients and other orthodontists). Thus, in both the trade secret and patent law contexts, there are issues for consideration regarding the distribution of confidential information.

In the context of trademarks, as with patents, there appears to be growth in the number of trademarks which incorporate the term “cloud computing.” The first application for a mark which contains the term “cloud computing” was filed in 1997, but was abandoned. See App. Reg. No. 75291765, filed May 14, 1997 (service word mark for “CLOUD COMPUTING” abandoned April 21, 1999). The first registered mark containing the term “cloud computing” appears to be Serial No. 77762889, filed on June 18, 2009 and registered on January 19, 2010. There appear to be increasing numbers of such registrations, and this will invariably lead to trademark law issues relating to genericness, secondary meaning, and infringement/likely confusion.
Finally, in the context of copyright, cloud computing raises potential legal issues in the area of data stored in the “cloud” such as computer programs. Under the Copyright Act, copyright attaches to a work which is stored in a tangible medium of expression. See 17 U.S.C. § 102(a) (“Copyright protection subsists … in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”). In the cloud computing environment, data and information can be split up and copied in separate locations in the cloud (and redundant copies can be made in multiple locations). See, e.g., Messmer at 1 (“Google’s multi-tenant distributed model entails ‘splicing data across many hard drives’ so that in this ‘hardened Linux stack’ there’s a ‘quick update of all fragments of all files in the hard drives,’ a process he called ‘obfuscated files.’”). If for example data relating to a single work is physically split up and stored in separate locations in the cloud, there is the possibility of questions being raised as to whether the work has been fixed in a tangible medium of expression, since the “cloud” is an undefined set of machines or devices from which the work would need to be perceived, reproduced, or otherwise communicated.

Also, similar to the discussion above concerning patent law, for copyright law there are extraterritoriality issues which can arise. For example, if an accused infringing work, such as a piece of software, has been copied in the cloud or stored on servers overseas, there arises a question as to whether such activity constitutes infringement reachable under U.S. copyright law. See, e.g., Quality King Distrib. v. L’Anza Research Int’l, 523 U.S. 135, 145 and n.14 (1998) (first sale doctrine applies to goods purchased abroad without requiring extraterritorial application of the Copyright Act).

As discussed, there are a multitude of potential legal issues to consider under various intellectual property schemes relating to cloud computing. The same is true with respect to legal issues outside the field of intellectual property law, of course.
B. Cloud Computing and Other Potential Legal Issues

While the focus of this discussion has been on intellectual property legal issues, clearly cloud computing impacts more than just the areas of traditional intellectual property law. A non-exhaustive overview of potential legal issues include the following:

In the area of e-discovery, for example, cloud computing creates potential challenges for companies attempting to comply with e-discovery obligations, since by definition a cloud services customer does not control the preservation, backup, or maintenance of the IT infrastructure and thus the data and metadata relating to potentially discoverable materials. See Fed. R. Civ. P. 26, 34. One issue for customers of cloud services is whether and how that customer, engaged in litigation, can comply with e-discovery obligations when that customer does not control the computing resources:

Several issues are unique with cloud computing. One is data ownership. Although there is little doubt that the cloud client's data belong to the client, the client does not seem to have much control over the data that are stored in a data center in the cloud. Another concern involves system and application ownership, even though it apparently belongs to the cloud computing provider.

See Du and Cong at 68.

For purposes of third-party discovery (such as procedural issues involving the court from which to issue a subpoena), ascertaining the court(s) having proper jurisdiction over data in the cloud or a set of cloud resources may be an issue in a particular case. See Fed. R. Civ. P. 45. If the cloud resources company is not located in the U.S., there arises an issue of how to obtain discovery of such electronic materials through international service of process or other methods. Moreover, in the litigation context, a subpoena directed to a cloud service provider raises potential legal issues with respect to how response will be made to any such subpoena. A cloud service provider having control of electronic data and files of a customer could, theoretically, respond to a subpoena by producing documents, data, and information the disclosure of which the customer legitimately has objected to, and thus the responding
party to the subpoena may risk waiver of objections. Finally, since such cloud services are not controlled by the customer, there are potential legal issues relating to arguments about spoliation, preservation, litigation-hold, and authenticity of potentially discoverable materials – particularly metadata.

Another potential legal issue relating to cloud computing relates to application and preservation of the attorney-client privilege. *See Upjohn Co. v. United States*, 449 U.S. 383, 389-397 (1981) (communications between counsel and “low level” corporate employees are protected by attorney-client privilege). In a cloud computing environment, theoretically it is possible that a customer’s attorney-client communications may be physically or electronically shared with cloud service providers (and their sub-contractors). Thus, there arises a potential legal issue as to whether there may be an argument of a waiver of privilege if such third parties have full or partial access to a customer’s confidential materials. *Cf., e.g., Mohawk Indus. v. Carpenter*, 130 S.Ct. 599, 607 (2009) (pre-trial orders on waiver of attorney-client privilege are not reviewable on collateral appeal). Preservation of the privilege can be of vital importance to companies, as recognized from a policy perspective by the Supreme Court. *Upjohn*, 449 U.S. at 390-93 (“[T]he privilege exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice…. [I]f the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.”).

Because cloud computing can often involve the storage of private data of third-parties (for example, credit card or other information of customers), there is also a potential for regulatory and related legal issues. Security of such confidential data can be of significant concern in an era of hackers
and others motivated by various reasons to try to obtain such data. See M. Kronfeld, “Treasury Dept. has cloud hacked”, Government Security News, available at http://www.gsnmagazine.com/article/20691/treasury_dept_has_cloud_hacked (May 10, 2010) (“The Treasury Department was hacked last week, leaving the Web site for its Bureau of Engraving and Printing – the agency responsible for printing U.S. dollars – down from May 3 to May 7.”). The utility model nature of the cloud can impact a consumer of services in investigating or performing diligence on security measures of those cloud service providers holding or processing confidential or personal information. “To audit cloud computing providers, in addition to the typical areas of concern such as system reliability, integrity, and security of hardware and applications, issues specific to the cloud computing environment can pose legal, regulatory, and compliance challenges to accounting professionals.” See Du and Cong at 70.

There are evolving standards for security, such as the PCI DSS (Payment Card Industry Data Security Standard), and Statement on Auditing Standards (SAS) 70 (to be superceded by Statement on Standards for Attestation Engagements (SSAE) 16 on June 15, 2011). Id. at 69. Thus, standardization and compliance therewith (and representations of compliance with standards) can create potential legal issues relating to consumer protection laws and regulatory requirements. There is at least the potential for legal issues flowing from a security breach in the cloud resulting in identity theft; consumer harms; or loss or theft of confidential, private, or otherwise valuable information, as well as issues arising from technical developments intended to mitigate or prevent such breaches. See R. Ranchal et al., Protection of Identity Information in Cloud Computing without Trusted Third Party, in “SRDS 2010, 2010 29th IEEE Symposium on Reliable Distributed Sys.” (Nov. 2010).

Similarly, cloud computing implicates privacy law and regulatory issues. In light of the international and borderless nature of cloud computing, ascertaining proper jurisdiction over a set of
cloud resources may be difficult to ascertain. Given the distributed / redundant nature of some cloud systems, there may be an issue to determine where a particular set of data actually physically resides. Because different jurisdictions treat data and privacy issues differently, for example, ascertaining proper jurisdiction can be important for regulatory compliance and private warranty issues as set forth in service contracts. “The location of data centres is a big issue in contract negotiations, where legislative and judicial issues abound. For instance, the location of data is an issue under some data-privacy laws, such as those from the European Union.” See Messmer at 1.

Potential legal and compliance issues thus can arise relating to applicable laws such as the EU Data Protection Directive or the Security Rule dealing with Electronic Protected Health Information under the federal Health Insurance Portability and Accountability Act (HIPA). For example, the EU Data Protection Directive prohibits transferring personal information to countries lacking the same level of protection as that which is afforded to EU residents (such as, for example, the United States). Since cloud resources may be used transnationally, there arises potential issues relating to understanding when and how compliance with particular directives is required or not, and if so, how to undertake such compliance in this technical environment (where by definition the cloud takes advantage of the relatively easy transfer of data within the cloud).

Cloud computing also creates potential legal risk management issues. For example, if there is a third party service outage or a financial dissolution which impacts the integrity of data stored in the cloud, legal issues can arise from such service failures:

In addition, Internet reliability is also an issue because this is the way that all services are delivered and accessed. Many potential users ask how hard they will get hit if they run online applications for business processes and the service provider or the Internet go down…. One more key issue yet to be addressed is the going-concern risk of the cloud provider. If a provider goes out of business or ceases to exist, it creates enormous interruption to its users' businesses or even a disruption of their business continuity. Lawyers are working in these areas to specify standard contract terms between the cloud
provider and the client in case of disagreements and disputes. 

*See* Du and Cong at 68. As a matter of contractual law, mitigation of risks and allocation of risk-bearing relating to service failures can create both business and legal issues.

Because cloud computing services are governed by private law, for example by way of Service Level Agreements by which private parties allocate responsibilities and assign risks, the business of cloud computing thus can implicate several contractual legal issues. Many of the issues discussed herein can be considered for inclusion in the allocation of risks and responsibilities in services agreements, and are thus a matter of negotiation and agreement drafting. For an example of an SLA *See*, e.g., City of Los Angeles SLA with Computer Sciences Corporation and Google for SaaS, available at [http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf](http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf). For those representing customers of cloud computing services, SLA’s can raise complex outsourcing legal issues, and legal issues relating to the protection of clients’ interests may be challenging due to shifting business models and downstream service providers becoming unwittingly involved in the provision of services. Thus, transactional attorneys dealing with IT service agreements for their clients will be increasingly impacted by cloud computing issues.

**V. Conclusion**

To some, cloud computing constitutes a paradigm shift in the provision of services both at the enterprise level and at the consumer level. To others, cloud computing constitutes marketing jargon to describe a wide range of IT outsourcing services and other networked computing services. Delivery of services from “the cloud” raises issues in terms of IP ownership, enforcement, and future portfolio development. Cloud computing also raises potential legal issues beyond the IP realm, and understanding applicable legal and regulatory regimes can be important for companies and their counsel. Cloud computing provides technical and business advantages for service providers and service users,
and it can be cautiously expected that legal issues raised by cloud computing are here to stay and are likely to expand as the cloud computing business sector expands.