Blue Skies and Stormy Weather: Balancing Risks and Rewards of IP in the Cloud

October 12, 2011

One of the hottest trends in the business world's never-ending quest to cut expenses, cloud computing promises to slash IT operating costs by anywhere from 40-80% according to studies performed by the likes of Merrill Lynch, Booz Allen Hamilton, and Google. But cloud computing raises serious concerns about privacy, security, and liability that are particularly worrisome for companies with substantial intellectual property assets. Before jumping into the cloud, the risks of data loss and security breaches should be weighed carefully against the promised rewards of lower costs. In the wake of breaches suffered by Microsoft, Epsilon, Google's Gmail, and Sony's PlayStation, prospective cloud service users have to look at the issue from both sides now.

On A Clear Day

The concept of cloud computing is alluring, giving users on-demand network access to a shared pool of computing resources via the Internet. Instead of buying its own servers, software, and data storage, a company can essentially rent them from providers like Amazon, IBM, Google, and Joyent, ostensibly at a fraction of the cost.

Cloud computing is not a single type of system, but includes a variety of systems, technologies, service models, and deployment methods. Cloud systems may be deployed at the user's premises, shared by several users, hosted by a provider, or publicly accessible. The cloud system may offer a software application, a mechanism for users to create and operate their own software, or access to computing resources, such as servers or data storage. Providers can combine various forms, systems and technologies to create hybrid systems.

The various cloud environments are typically categorized by service model and deployment method. Service models include:

- **Software-as-a-Service (SaaS)**, providing specific applications (e.g., NetSuite)
- **Platform-as-a-Service (PaaS)**, furnishing a suite of applications, programming languages, and user tools (e.g., Google's App Engine)
- **Infrastructure-as-a-Service (IaaS)**, offering remote data storage networks (e.g., Amazon Web Services)

The four deployment methods are:

- **Private cloud**—dedicated solely for one organization
- **Community cloud**—shared by multiple organizations that typically have shared concerns
- **Public cloud**—available to the general public or large industry group
- **Hybrid cloud**—combining public and private elements

The biggest advantage touted to customers is cost reduction. Other benefits include flexibility, scalability, remote access, automatic updating, and the expertise of skilled vendors. But for all of these advantages, there may be a dramatic downside.

Clouds In My Coffee

Depending on the environment, cloud computing can be like storing your information in a rented filing cabinet located in a remote communal warehouse. You can lock the filing cabinet, but the landlord knows the combination, along with any number of your employees, clients, customers, and others who may need access. What's more, a warehouse full of filing cabinets is a more attractive target to burglars than one filing cabinet sitting alone in your office. You have to ask yourself:

- Is the warehouse secure against theft and destruction?
- Can other warehouse tenants gain access to your filing cabinet?
- Will you have unfettered access to your own filing cabinet at all times, or will there be power outages, jammed locks, and disputes with the landlord?
- If the government or a third party shows up with a subpoena, will the landlord turn over the contents of your filing cabinet?
- Will the landlord indemnify you against losses associated with these kinds of problems?

These risks are very real, and are already becoming the subject of numerous lawsuits like *Wong et al. v. Dropbox Inc.*, filed this summer in California. The plaintiff in *Dropbox* alleges her cloud service provider had a "bug" in its system that allowed users to access data stored in other users' accounts. The suit alleges the company compounded the problem by failing to give its more than 25 million users adequate notice of the breach. The effect of this kind of breach on a business using cloud services could be disastrous.

A company that puts trade secrets on the cloud not only risks loss and/or exposure of the data, but may also be jeopardizing the trade secret status of that information. Courts will not afford information trade secret status—and related protections—unless its owner took reasonable steps to maintain confidentiality and prevent disclosure. Many cloud service providers attempt to disclaim liability for the consequences of security breaches and omit terms from their agreements evidencing a duty of confidentiality. Acceding to such contract terms, and failing to take other appropriate security measures, could harm a company's chances of protecting its confidential information in court if it ever becomes involved in trade secret litigation.

Law firms dealing with their clients' confidential information have to be doubly worried about computing in the cloud: not only do they face fallout from exposure of their own work product and their clients' confidences, but they also run the risk of violating the Rules of Professional Conduct. In January 2011, the Pennsylvania Bar Association issued an informal advisory ethics opinion, No. 2010-060, advising that current rules do not preclude putting clients' confidential information in the cloud. But the opinion reminds attorneys of their duty under Rule 1.6 to protect confidential information, and suggests a variety of safeguards attorneys should consider.

Is It A Big Enough Umbrella?

One way of protecting IP from the threats associated with cloud computing is not to put it on the cloud. Companies should consider using cloud services for some of their more routine computing functions, while keeping research and other highly confidential information off the cloud. Any time a company chooses to use cloud services, careful attention should be paid to key contract terms to make sure the user isn't the one that ends up getting wet.

Cloud computing agreements diverge widely from typical software license and implementation agreements, and from hardware leases and purchase agreements. In addition to understanding unique cloud service contract provisions, attorneys must understand the basic definitions surrounding cloud computing and the due diligence lawyers and their clients must undertake before implementing such systems. Key points to consider include:

- **Security.** Providers generally warrant they maintain commercially reasonable security measures or use best efforts to protect user data. But they almost never assume responsibility for security issues such as data breach, data loss or service interruptions. Users must exercise due diligence to ensure the provider employs adequate security measures. Depending on the nature of the system, security measures should include—at a minimum—transmission encryption and/or storage encryption. There should also be physical security measures at the provider's facility. Providers should be required to notify users immediately in the event of a data breach.

- **Data Preservation.** Users must ensure adequate backup of data in the event of disaster or system failure. Backup can be provided through alternate cloud systems or the user's own local backup. The proper type of backup depends on several factors, including the size and importance of the data.

- **Location of Data.** For legal reasons, many users must control the exact physical location of data in cloud systems. The laws in many countries prohibit the transmission of certain data to specific countries. The location of the data is also important for purposes of ensuring confidentiality and the availability of appropriate legal remedies. Users should restrict by contract the movement of data to different jurisdictions.

- **Confidentiality.** In the cloud system, providers often have free access to user data. Providers should agree not to disclose or use their clients' data under any circumstances, unless mandated by court order or subpoena, and they should be required to notify the client prior to making any such disclosure.

- **Data and System Accessibility.** Providers should commit to uptime percentages for accessibility to the cloud system. However, counsel must understand the unique aspect of uptime percentages in cloud contracts and their impact on users. Uptime percentages often are tied to intervals within certain time periods, and downtimes of five, ten or fifteen minutes may not be considered downtime. Great care needs to be taken in reviewing these covenants and ensuring the user understands their impact. Also, accessibility is often an issue on termination. Users must be concerned that data or software conversion is adequately and practically addressed.

- **Licensing.** Cloud providers should represent and warrant they have appropriately licensed any software they are using to run the cloud and any software the client will use.

Before getting to the point of reviewing and negotiating contract terms, prospective cloud service users should do their due diligence in choosing a provider. The provider manages the cloud and controls access to software and data, so users should consider the provider's reputation, history, and financial viability. Has the provider encountered problems in the past? If so, how did it react? Will the provider stay in business, and can it support and expand the cloud system to meet growing customer requirements? Does the provider employ and update appropriate security and data preservation systems?

Cloud computing is here to stay. But users and their counsel must consider and address the inherent risks. If they're not willing or able to do that, they'd better get off of the cloud.

About the authors:

Susan V. Metcalfe practices in the Litigation, Intellectual Property, and Injunction Practice groups of McNees Wallace & Nurick LLC. A large portion of Susan's practice involves trademark, trade dress, copyright, and trade secret disputes. She also has broad experience in commercial and business litigation, representing clients in contract disputes, product liability actions, sales and warranty disputes under the Uniform Commercial Code, and directors and officers liability litigation.

Michael A. Doctrow is the Chair of the McNees Wallace & Nurick LLC Intellectual Property Practice Group. Mike practices trademark, copyright, trade secret, and advertising law. He regularly assists clients in structuring and negotiating trademark, copyright, patent and software license agreements, technology contracts, franchise and distribution agreements, and advertising agreements.