A Close Look At Cloud Computing Is Essential

The Editor interviews ***Nolan M. Goldberg****, IP & Technology Counsel, Proskauer.*

Editor: Tell us about your practice and role at Proskauer, particularly as a founding member of the Litigation Department's Electronic Discovery Task Force.

Goldberg: I am a patent attorney with an electrical engineering background. My practice is primarily patent and trade secret litigation, with lots of work in the telecommunications, barcode scanner and financial services fields.

Over the past couple of years, advising clients on electronic discovery-related issues, both in the absence of litigation and during litigation, has become a significant part of my practice. Before litigation, for example, I help clients develop information management systems to proactively reign in discovery costs and meet compliance obligations. During litigation, I help clients understand and manage the burden and costs of the process, with the goal being a rational e-discovery expenditure that, while meeting all obligations, minimizes the disruption to my client, and is proportionate to the amount at issue in the litigation. I also consult on the recovery of often-overlooked electronic evidence, such as computer forensics.

Recently I've focused on electronic discovery and alternate dispute resolution, and I am the primary author of the e-discovery section of the International Institute for Conflict Prevention and Resolution's model economical litigation agreement, colloquially known as the "Litigation Prenup."

Editor: "Cloud computing" is a buzzword that's been popping up more frequently than ever. How would you define it?

Goldberg: Cloud computing is a marketing term that covers lots of different technologies and business applications. By way of example, the National Institute of Standards and Technology ("NIST") is now on version 15 of their attempt to define the cloud, with the current definition two pages long, with lots of subparts.

I like the analogy in the book *The Big Switch* by Nicholas Carr for an initial introduction to the cloud concept, which compares the evolution of cloud computing to the transition from individual power generation to modern utilities.

Historically, factories needed to generate their own power. For example, a water wheel may have been built to power a factory's machinery, with the construction of the wheel and its operation and maintenance falling entirely on that business. At some point, these local generators were replaced with centralized power generation, where power was generated remotely, distributed as a utility, and priced based upon consumption. There are many reasons why this development was a good thing. Utilities presumably know how to generate power better because that is their primary business, there are economies of scale, the consumer can ramp up or down its consumption quickly and easily, and the consumer doesn't have to pay for the excess capacity that the consumer does not need.

Nolan M. Goldberg

Cloud computing is very much the same concept. Rather than building and maintaining its own IT infrastructure, an organization can instead purchase the use of a comparable infrastructure as a service, paying for what it consumes, and leaving it free to focus on its primary business. The cloud also supports business agility by allowing for the fast expansion or contraction of IT capabilities.

"Rather than building and maintaining its own IT infrastructure, an organization can instead purchase the use of a comparable infrastructure as a service, paying for what it consumes, and leaving it free to focus on its primary business. The cloud also supports business agility by allowing for the fast expansion or contraction of IT capabilities."

Editor: Why is it important for lawyers, particularly, in-house counsel, to take a closer look at how their companies are implementing this technology?

Goldberg: Cloud computing is an area of technology and a business model whose impact is going to reach across many legal areas, from electronic discovery to compliance to intellectual property. Accordingly, the stakes are very high as companies consider replacing internal systems with externally hosted ones.

Saving money is a common reason why organizations move to a cloud, and it's important to understand whether the organization will actually realize those savings or just end up transferring costs from their IT budget to the legal budget. There are many legal costs that are often overlooked about which in-house counsel will need to be aware. First, there is the cost of a due diligence process, the investigation that takes place before entering into a contract for cloud-based services.

Second, there may be customization costs. If an organization needs to customize the cloud service to make it suitable for a specific need, that may be counter to the economies of scale and will likely involve additional cost.

Finally, I believe the potential change in risk exposure should be taken into account. This may be difficult to quantify as it is a discussion about possibilities and probabilities. For example, would an organization trade some amount in IT savings for an additional percentage chance of a patent litigation? It is going to fall on in-house counsel to help evaluate these risks and to generally make sure that the service will meet business objectives.

Editor: What is the most important legal question for organizations considering moving their data to the cloud?

Goldberg: Because of the many potential variations in the way cloud systems are implemented, technologically, structurally, and contractually, the legal risks are different with each system. The key legal question is whether a given cloud is suitable for a given application. Every cloud has to stand on its own merit and be evaluated separately with reference to the application for which it is intended. For example, you may not want to use the same cloud that you use for your personal emails to hold your corporation's crown jewels.

Editor: What is the difference between public and private clouds, and why is that potentially important?

Goldberg: I mentioned NIST's 15th attempt to define cloud computing earlier. Version 15 defines a private cloud as where the cloud infrastructure is operated solely for an organization and may be managed by the organization or a third party and may exist on premise or off premise. It defines a public cloud as a cloud where the infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

A key distinction between public and private clouds, and one that is important from a legal standpoint, is that public clouds likely have multi-tenancy, or multiple unrelated consumers of the service. With private clouds, analysis of risk may be very different if data isn't being placed into the hands of third parties.

"With regard to contractual standardization, it is well known that there is a lack of standardized terms in cloud computing contracts. Therefore, it is very difficult for in-house counsel to compare a cloud contract from one provider with a cloud contract from a second provider."

Editor: How may standardization activities impact the adoption of cloud computing?

Goldberg: There are two aspects of standardization that are interesting. The first is contractual and the second is technological.

With regard to contractual standardization, it is well known that there is a lack of standardized terms in cloud computing contracts. Therefore, it is very difficult for in-house counsel to compare a cloud contract from one provider with a cloud contract from a second provider.

The Cloud Computing Project at Queen Mary University of London is an interesting attempt to address this issue. Funded by Microsoft, it is reviewing many common cloud contracts. If it is successful, some best practices may emerge. This should make the due diligence process a lot easier on in-house counsel.

The second aspect of standardization is the need for apples-to-apples comparisons of the technological features of clouds. For example, such issues as security and interoperability may be addressed. Standardization in this sense is needed to facilitate third-party technical audits which will, again, take some of the burden off of the customer during the due diligence process and potentially help speed up cloud adoption.

The potential downside to these standardization activities is that they may ultimately define standards of conduct creating risk for those using cloud systems that fall below those standards.

Editor: As an IP litigator, how do you think the use of cloud services will change the risk of patent litigation?

Goldberg: You are going to have a different risk of patent exposure when your service is hosted in the cloud as opposed to an internally hosted solution. The technologies used by a cloud provider to provide the cloud service won't necessarily be the same as those used in an internally hosted version of the product.

Please email the interviewee at ngoldberg@proskauer.com with questions about this interview.

For example, you may need different technologies to support multi-tenancy in the cloud. You will likely have different security concerns and need to deploy different solutions. In an internal system your security typically includes a firewall designed to keep outsiders off of your network and a permission structure designed to limit the access of employees only to information within the network that they need to know. In a public cloud, you are going to have all of that plus technology protecting your information from other customers of the cloud provider and from the cloud provider itself. The ways data moves and is stored in the cloud may also be different. This all contributes to different risks.

"You are going to have a different risk of patent exposure when your service is hosted in the cloud as opposed to an internally hosted solution … For example, you may need different technologies to support multi-tenancy in the cloud. You will likely have different security concerns and need to deploy different solutions."

The structure of the cloud service will also impact risk. One cloud service could have a single provider that provides all of the necessary hardware and software. Another cloud may have multiple providers, where one provides the cloud hardware and the other provides the software. In the first example, the consumer is likely in a direct contractual relationship with the single provider. In the second example, the consumer may only be in a direct contractual relationship with one of the two providers, with the other provider having its own contract with the remaining provider.

For a more extreme example, the hardware provider may itself have contracted with other hardware providers, for example, for surge capacity. The consumer may not know at a given time the identity of all the participants in a cloud system or the location of its data. That is going to change the risk profile.

I would conclude by noting that there are a lot of cloud startup companies right now, and in fact the cloud makes it very easy for startups, because they don't have to build their own hardware infrastructure.

The problem is that over time many or most startups will fail, and this can result in lots of orphaned patents which may ultimately become a burden on the cloud industry. For example, during the dot-com era, when the bubble burst, many startups that failed had patents, which survived and fell into the hands of non-practicing entities, whose business was bringing lawsuits. Likewise, orphaned patents held by failed startup cloud providers can create similar problems.

Editor: How can an organization manage the risk of patent infringement in the cloud?

Goldberg: Organizations could undertake patent clearance projects to try to identify what relevant patents are in the space, who is filing litigations in the space, and which providers already have licenses to patents that are of concern. However, in the cloud, such efforts could be complicated by a lack of transparency in cloud systems. The consumer may not actually even know or be able to learn how the cloud system is actually implemented at any given time.

Further, certain cloud contracts allow for the provider to change the system, sometimes without notice. Accordingly, you could have done a very thorough patent clearance project, but tomorrow the system, and its risk, may be different.

Another way to manage patent risks is through contractual indemnification. One potential problem is that the customer may not be in a direct contractual relationship with all of the providers of the cloud system. Thus, in a system with many providers, it may be difficult to get complete indemnification.

Editor: What other IP issues are concerns?

Goldberg: Protecting trade secrets in the cloud is another concern. Obviously, you have to take reasonable steps to maintain the secrecy of a trade secret in order for it to maintain its value. It is an open question of what is reasonable in the cloud context. Encryption is likely one answer to this problem.

Some cloud contracts may give the cloud provider certain rights in its customer's data, and there is the potential that this could impact the value of that data. It is one thing when the provider gets rights that it needs to operate its systems, for example, the right to copy or move files in certain limited ways. But, there may be more serious ownership concerns that can impact the value of the data when the provider gets rights in its consumer's data for revenue-related purposes, such as targeted advertisements.

Editor: Can you explain why the issue of "control" over the data in the cloud is important?

Goldberg: Electronic discovery obligations extend to documents in an organization's custody or control. By moving documents to the cloud, the documents may no longer be in a litigant's custody, but they may still be under its control. The starting point for analyzing this issue is the cloud contract. If ESI is under control of the litigant, it may fall within the litigant's e-discovery obligations, meaning that it could be the litigant's responsibility to preserve, retrieve and produce those documents in litigation despite the fact that they are not in its custody. Issues of control go beyond just the basic documents and also extend to things like metadata, log files and other associated ESI.

Before data is put on the cloud, it is important for the cloud customer to know how it is going to carry out these basic e-discovery functions, including making sure it has whatever rights and help it needs from the cloud provider. The cloud contract should also provide for how costs will be allocated.

The analysis of control in the cloud may be simple where a litigant has a direct contractual relationship with all the providers of the cloud service. It can be tricky with more complicated systems.

For example, let's assume that the cloud contract provides a consumer with the right to access certain forensics. One of the things that the consumer will want to check during the due diligence process - if it is not in a direct relationship with the hardware provider - is whether the party with which it has contracted itself has the rights under its contract with the hardware provider to meet its obligations to the consumer.

"Electronic discovery obligations extend to documents in an organization's custody or control. By moving documents to the cloud, the documents may no longer be in a litigant's custody, but they may still be under its control."

Editor: Besides issues of control, how can cloud computing impact e-discovery?

Goldberg: Returning to the previous example, let's assume that a log file is relevant to a case, but it is not under the control of the litigant. Does that mean it can't be discovered? The answer to that is potentially "no," as a discovery request could be sent directly to the cloud provider for such data. While these direct requests to the provider may be objectionable where the data is under the litigant's control, here the log files may only be available from the cloud provider. How the provider responds in such cases depends in part on the cloud contract. Therefore, the contract should describe how the customer would like the provider to respond to those requests.

It is also important to note that the Stored Communications Act may also affect the cloud provider's obligations to turn over data.

Editor: What is data persistence and why is it an important issue in the cloud?

Goldberg: Data persistence concerns how data survives in the cloud, in some cases after you expect or want it to be deleted. It is a good idea – and sometimes a necessity if compliance obligations are implicated – for an organization to make sure the cloud that they are contemplating using will comply with their information management system, and any applicable laws, before they move their data to the cloud.

It can be problematic if the cloud service cannot comply with the organization's retention policies. For example, from an e-discovery point of view, it may mean that a litigant has to incur an expense that they could have avoided if the document had been properly deleted. The unexpected retention of the document could also lead to a direct request to the cloud provider for that document in litigation, particularly if it can be argued that the surviving copy is somehow outside of the litigant's control.

From a compliance point of view, the improper retention of information on a cloud can lead to the violation of certain laws. For example the European Union Data Protection Directive specifies limits on how long data can be retained.

Editor: What steps can an organization take to minimize the impact of a cloud service on e-discovery?

Goldberg: Discovery on the cloud can be more complicated than normal discovery because your data is on a network controlled by someone else. Therefore, there may be restrictions on available tools that you can use, you may need to rely heavily on the provider in order to get things done, and you'll have a lot less knowledge about the network than you do with your own network.

The heat of litigation may not be the ideal time to first address these limitations. It's a good idea to identify how data will be collected and preserved before that data is put on the cloud. What the organization could then do is record the results of the due diligence in a data map or other litigation readiness tool and store that along with the contract. Should litigation later arise your organization will be prepared. This may also provide some defensibility should things go unintentionally wrong.

"The due diligence process, and ultimately the decision about whether to go to the cloud, should be an enterprise decision, bringing in the business stakeholders, IT and in-house legal."

Editor: How important is the role of the lawyers?

Goldberg: The due diligence process, and ultimately the decision about whether to go to the cloud, should be an enterprise decision, bringing in the business stakeholders, IT and in-house legal. While the ease of purchasing certain cloud services may support ad hoc adoption, there may be many benefits to making such decisions in a uniform organization-wide manner.