Understanding the Legal Risks of Cloud Computing

Navigating the Network Security and Data Privacy Issues Associated with Cloud Services

ASPATORE

For customer service inquiries, please e-mail West.customer.service@thomson.com.

If you are interested in purchasing the book this chapter was originally included in, please visit www.west.thomson.com.

Overcoming Security Challenges in Cloud Computing

Robert J. Scott
Managing Partner
Scott & Scott LLP

ASPATORE

Introduction

Business executives recognize the benefits of cloud computing. Low up front and maintenance costs, utility billing, on-demand scalability, and access to enterprise-level software represent clear advantages for any organization.

Cloud computing can deliver greater speed, flexibility, and tangible IT cost savings; three reasons why businesses should not disregard the cloud as hype. But entering into cloud computing contracts without understanding the inherent risks can cripple an otherwise healthy organization. The significant network security and data privacy risks associated with cloud services should be addressed through proper contracting and risk transfer using insurance.

Data Privacy and Security Risks for Cloud Computing Users

The biggest issues with respect to cloud computing are data privacy and security risks. The loss of personally identifiable customer, financial, or health care information can be catastrophic to a business. Related to these concerns are IP and data ownership issues, the right to use data, jurisdiction of stored data and compliance with local law, rights to the data at termination of a contract, and the availability of monetary or other remedies in the event there is a data breach. Before outsourcing application hosting and data storage to a cloud vendor, a customer must be comfortable that the vendor's platform is secure and that the terms of service protect the customer if things do not go as planned.

The main risk that users face when they place their data and applications on centralized servers in a cloud computing environment arises from the loss of physical control of the data. Once data is out of the users' hands and in the hands of another party, all of the issues identified above become risk points for the user. The customer has a non-delegable duty to safeguard their customer information. In cloud contracts, end-users entrust this duty to safeguard the privacy and security of their data to the cloud provider while still remaining legally responsible for any losses that occur during the term of the contract.

The legal risks for a consumer and a business in the cloud computing environment are generally the same, save for two main differentiators:

1. Businesses have the opportunity to negotiate and balance their risk in terms of negotiating the terms and conditions of the contracts under which the services will be offered, while users rarely do; and,
2. Businesses often store their client data in a cloud owned by the cloud vendor. From a practical perspective, the business must be willing to accept that risk and associated liability on behalf of their clients.

Legal Protection for Data Stored in a Cloud Environment

There are some legal protections for data stored in a cloud environment in the form of state and federal law. Forty-six out of fifty states have data protection statutes (none of which are particularly strong), and there are federal statutes such as HIPAA and Sarbanes-Oxley that are applicable to certain businesses operating in specific industries. But the strongest protections, at least for those users with negotiating power, are in the form of contractual provisions regarding data security, insurance requirements, confidentiality, liquidated damages, and service level agreements. Provisions that limit the cloud provider's liability should be edited to make sure that the provider and its insurance carrier will respond to any claims and pay for any damages that arise from the services. Detailed service level agreements should also be negotiated specifying the precise nature of the services that will be provided and detailing the consequences for any failure in service.

The security and reliability of cloud computing services varies. Many cloud providers take commercially acceptable steps to protect user data, while others are not quite as careful. The trick is to be able to tell one type of provider from the other. For most cloud transactions, that means reading the fine print. A good starting point is to check the provider contract to see how much a cloud vendor is willing to represent that it takes that affirmative step to protect user data.

Contract provisions that require the provider to comply with specific industry regulations such as PCI, GLBA, or HIPAA can signal the provider's maturity level regarding network security and data privacy.

If that type of language is missing or infrequent, it probably means that there is not a lot of security happening behind the scenes.

To determine where the information in a cloud server is located and what law governs its protection, the user has to ask questions. The user is generally not going to be given that information up front because many providers consider their network architecture to be confidential, but most reputable cloud vendors will answer that question without hesitation. Once the location of the server is known, it is the attorney's job to understand what law governs the data storage. In some instances, knowing the location, in and of itself, will help the client make a smart choice between vendors because the jurisdictions where data will be stored can increase or decrease privacy and compliance risks due to variations in applicable laws.

The obligations that hosting companies have with respect to data privacy and security, especially in the United States, are primarily contractual. As discussed above, for certain industries (health care is a perfect example), the data and privacy laws (HIPAA) are well-defined. These laws oblige service providers to take specific technical and procedural steps to handle protected information. For hosting companies not governed by these industry-specific statutes, the obligations set by statute are related to handling of a data breach event, not the process by which the data is protected. Again, the best way to protect user data, and obligate a hosting company to meet a certain standard, is to negotiate it into the contract.

Core Components of a Privacy Policy for Cloud Computing Service Providers

Privacy policies for cloud computing service providers are generally going to do the following: establish the physical, administrative, and technical controls that are in place to protect data. They will define how and when the vendor can share data, and what the vendor will do in the event of a data breach. The customer should read, understand, and negotiate changes to the policy, if possible.

It should be noted that a hosting service can limit its liability by way of disclaimers and agreements. There are some statutory prohibitions against this in limited circumstances, but it is important to look at the standard, one-sided hosting agreement end users are most familiar with. These agreements are essentially nothing more than disclaimers and limitations on liability.

The confidentiality of information in the cloud should be carefully defined in the contract. Most cloud contracts have a section dedicated to confidential information. The lawyer's role is to ensure that the definition of confidential information in the contract is consistent with the information that the end user will be sharing with the cloud vendor or uploading into a cloud platform. In the absence of a contract on this issue, confidential information will be determined under state trade secrets laws, which would apply uniformly to both cloud and non-cloud contexts.

Recent Cases Involving Emerging Cloud Computing Concerns

I believe that it is important to think of data privacy in the cloud, not only as implicating the data a person enters into a website, but also data that is stored elsewhere but that originated from those ubiquitous mobile devices we all carry.

Along these lines, there are several lawsuits being filed against the major cell phone carriers and Carrier IQ, a company that sold software to these carriers to integrate into their phones. Carrier IQ developed software that surreptitiously records data from cell phone use, ostensibly to monitor and improve the performance of the phones. In reality, the software can be, and allegedly has been, used to record user interaction with the phone including calls, text messages, and password information. The data is stored in unknown facilities in the cloud. Users allegedly had no idea that this data acquisition and use was a possibility, much less that it was actually happening. These kinds of legal actions are going to continue to push public opinion, and by extension, lawmakers, into action to protect end users in these agreements. Federal and state privacy regulations have been predicated on a notice and choice model and therefore disfavor any technologies that secretly gather or monitor arguably private information.

Misunderstood Aspects of Cloud Computing and Related Legal Issues

I have found that IP, business continuity, data privacy, and risk management are the most commonly misunderstood aspects of cloud computing. IP risks include trade secrets, copyrights, and trademark aspects of cloud contracts. Business continuity involves the availability of the systems during the term of the contract, and the ability to migrate off the cloud platform at the end of the contract term. Data security and privacy and risk management challenges can be solved through specialized insurance products. Vendor-provided contracts rarely adequately address these concerns and end-users rarely have the specialized expertise on staff to negotiate for the inclusion of appropriate contractual protections.

Attorneys unfamiliar with the issues related to cloud computing should attend continuing legal education (CLE) courses that focus on these issues, or read other attorneys' writings on these topics. Given the trend toward cloud computing for everything from cell phones to digital lockers to personal computer backup services, we will all be asked about these issues eventually.

Avoiding Cloud Computing Risks and Litigation

Risks associated with the loss of customer data are obviously high on the list of litigation risks associated with cloud computing, but in addition, unavailability of the service or unrecoverable data can be particularly painful to a client. When the cloud provider is unwilling or unable to remedy the situation, lawsuits arise. Service level agreements with specific remedies such as financial penalties for failure to comply can be effective in preventing lawsuits. To mitigate the risks of a lawsuit, cloud vendors need to have the proper types and limits of insurance coverage. However, all the coverage in the world will not help if it is not contractually available to the client. The best contracts are those that ensure that insurance proceeds are available to the client when the coverage kicks in.

Ultimately, the best security measure a customer can take is to have a great contract. It is important to have cloud agreements reviewed and negotiated by attorneys familiar with the different ways to balance and mitigate risk.

Many times during the course of the negotiation, the attorney will act as a facilitator, engaging both parties in frank and open discussions about the technical limitations of the cloud service. This leads to a client who fully understands his or her risk by seeing the potential for failure inherent to any service agreement. At that point, the client will have a much better idea of whether or not this is a good deal. Clients jumping into cloud agreements without this in-depth analysis are frequently left holding the bag with no recourse when things go wrong.

Protecting IP in the Cloud Computing Environment

The basics of protecting IP in the cloud computing environment are not dissimilar from protecting it elsewhere: 1) register the IP if it can be registered (via copyright, trademark, or patent), 2) monitor its use (there is no policing authority for these property rights—it is up to the client to do the monitoring), and 3) police the user's intellectual property rights through effective monitoring and enforcement programs. Treat confidential information as secret, and implement tools and processes to keep trade secrets confidential. Appropriate confidentiality provisions should be included in all contracts with employees, contractors, and vendors.

Going forward, I believe that the last thing we need is more state privacy and security regulation in relation to cloud computing. Rather, I would like to see a federal standard for privacy and security regulations that pre-empts the current state laws on these topics The current patchwork of regulations makes it extremely difficult for a business to comply with applicable laws. Extending and standardizing the federal rules applicable to health care, financial services, and banking, and expressly pre-empting state laws covering the same issues makes the most sense.

Lawyers advising clients on cloud contracts should focus the client's attention on all the things that can go wrong if things do not go as planned. By systematically addressing risks through negotiation of special contract provisions, the lawyer can play an indispensable role in helping clients achieve a competitive advantage as an early adopter without taking unreasonable risks.

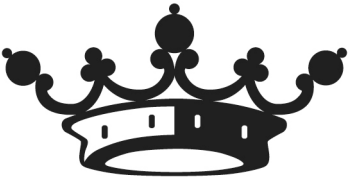
Conclusion

The two important steps to take before entering into any cloud computing agreement is to identify the risks described above to determine the client's comfort level with respect to each and begin the discussion of risk balancing early in the negotiation. Lengthy, unsuccessful negotiations can be avoided if each side is clear as to their "deal-breakers" with respect to these risks up front.

Robert J. Scott is the managing partner of the intellectual property and technology law firm Scott & Scott LLP located in Southlake, Texas. Mr. Scott's practice focuses on areas where law and technology intersect. He is a member of the State Bar of Texas Privacy and Security Committee. He can be reached at rjscott@scottandscottllp.com.

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.



ASPATORE