The Computer & Internet Lawyer

Volume 35 ▲ Number 7 ▲ JULY 2018

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Advising a Client Considering the Cloud

By Drake Mann

Few developments have changed commerce and technology with the speed and scale of cloud computing. An industry now worth around $130 billion barely existed a decade ago. The Internet has enabled computing resources to be gathered into huge datacenters—dense clusters of infrastructure and technical specialization—placed at a distance from the consumer of those computing resources. Efficiencies of scale followed, and the cloud now seems to be both everywhere and nowhere.

The growing ubiquity of cloud computing makes it increasingly relevant to any lawyer whose practice includes reviewing clients' contracts. Cloud computing may seem mysterious or technical, and, too often, businesses move "to the cloud" with little to no thought about the legal consequences the cloud may bring. This article offers some background knowledge a lawyer may find useful in advising clients considering a move to cloud computing.

Drake Mann is shareholder and director of Gill Ragon Owen, P.A., in Little Rock, Arkansas. Mr. Mann is a director of the firm's cybersecurity and privacy practice. He holds FIP, CIPT, CIPM, and CIPP/US designations from the International Association of Privacy Professionals, and an Advanced Professional certification from the Cloud Industry Forum and can be reached at *mann@gill-law.com*.
This article was originally published in the Winter 2018 issue of *The Arkansas Lawyer* magazine and is reprinted here with permission from the Arkansas Bar Association.

What Is the Public Cloud and What Are Its Key Features?

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Its essential characteristics include:

- *Broad Network Access*, which enables customers to access resources whenever and wherever they have access to the Internet, including both workstations and mobile devices;
- *On-demand, Self-service Provisioning* of computing resources by a customer without interaction with the provider's staff;
- *Rapid Elasticity*, which means that computing resources can be rapidly expanded or reduced, in some cases automatically, to match a customer's demand;
- *Measured Service*, meaning metered control, monitoring, reporting, and billing; and
- *Multitenanted Resource Pooling*, whereby efficiencies of scale are gained from gathering computing and

networking infrastructures into large datacenters. Among others, these include efficiencies in purchasing, systems management, physical security, and energy consumption. Software enables physical servers to be joined or divided into virtual servers or other computing abstractions so many customers share resources.[2]

Computing Regarded as a Standardized, Delivered Utility

Cloud computing technologies lead to a conceptual reframing of computing power and how that power is delivered and used. Cloud technologies also alter a chain of legal and commercial relationships in fundamental ways.

Cloud providers can be thought of as delivering units of computing services as standardized commodities, much as public utilities deliver electric power or natural gas. (Consider that the variety of those computing services and how customers use them are potentially as different as electricity is from gas.)

Legal and commercial relationships change in that transactions that were formerly one-time sales contracts for licenses and hardware become periodic contracts for services. Accounting, taxation, and financing changes follow; what were once capital expenses become operating expenses, and startups that could not afford a capital outlay to buy computers might be able to fund monthly outlays for computing power, particularly if its business model matches its cashflow to computing-service costs.

What Commercial Roles Exist in the Cloud?

The parties to cloud computing contracts fall into three broad categories: The cloud-service provider, the cloud-service partner, and the cloud-service customer.[3]

Cloud-Service Providers: The Big Four Providers

There are four large cloud-service providers: Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure, and IBM Cloud Computing. AWS is by far the largest and offers the widest array of services. These providers' business models depend on delivering a high-volume, low-cost, uniform service. There is no cost-effective way for these providers to negotiate special terms for individual members of their large customer base, so click-through terms of service (TOS) are the norm. Lawyers can still serve clients as counselors, calling attention to the more significant risks of the cloud, some of which are discussed further below.

Smaller Providers

There are countless smaller cloud-service providers. Some of these smaller providers may nevertheless be large and substantial enterprises. The services these providers offer vary. Some may merely be regional datacenters providing simple storage, for example. Many, if not most, are Software as a Service (SaaS) providers serving a particular market. Some examples include cloud-based electronic medical records services for healthcare providers, tools for realtors to list properties and manage documents, and cloud-based environments for education.

The relative bargaining power of these smaller providers means that most lawyers' clients can negotiate at least some of the terms of their cloud-service agreements. These providers' service agreements have many features (discussed further below) that are common to the large providers' agreements.

Cloud Providers' Supply Chains

Be aware that, frequently, smaller SaaS providers will buy cloud resources from: (1) one of the big four cloud-service providers; (2) other smaller providers; (3) cloud-service partners; or (4) any combination of them. That is, there may be a long, complex supply chain of cloud providers upstream from the SaaS vendor with which a lawyer's end-user client proposes to contract. For example, a smaller SaaS provider may have developed a cloud-based service that is tailored for a particular market (*e.g.*, orthodontists or car dealers or realtors or law firms). Such a provider might first have designed and tested its software with AWS Developer Tools. It might maintain its database using Microsoft's Azure SQL Database. It might use Google's BigQuery to store and analyze large sets of its customers' data.[4] And it might ultimately conduct all of its operations having no datacenter of its own.

Although the topic is beyond the scope of this article, it is appropriate for a lawyer advising a client considering business-critical cloud services to learn whether the provider itself depends on a cloud-service supply chain, and, if so, what potential impact the TOS at each link along that chain may have on the lawyer's end-user client.

Cloud-Service Partners

Cloud-service partners comprise a range of ancillary service providers, such as auditors and brokers.

Cloud Auditors. Cloud auditors are cloud-service partners that conduct independent assessments of providers' cloud services. If a cloud customer does not have the technical expertise to determine whether a cloud provider is meeting promised performance

metrics under a service level agreement, for example, or if a cloud provider will not grant a customer sufficient access for the customer to assess the provider's security or privacy controls, the customer may use an independent, qualified auditor to evaluate and report on these services.

Cloud Brokers. Cloud brokers manage the use, performance, and delivery of cloud services and may negotiate relationships between cloud providers and cloud customers. Brokers may also participate in a cloud-service transaction in some way. For example, consider a broker that is especially familiar with the service needs and security threats to the healthcare industry. While the big four providers tightly limit liability for their services, a broker in this position might be willing to expose itself to more liability between parties it knows because it is in a better position to manage service needs and to control risks in a way the larger providers cannot. (Of course, a customer relying on a broker's acceptance of this sort of liability would want to know about the broker's financial ability to fulfill its promises.)

Cloud-Service Customers

Given the current state of the industry, most lawyers' clients will be cloud-service customers using SaaS. These services may be offered by one of the big four providers or by a smaller cloud provider. Examples of these cloud-based services include Microsoft's or Google's office suites (word processing, spreadsheet, and presentation tools), Salesforce.com's customer relationship management products, or various industry-specific products, such as those for healthcare providers, lawyers, accountants, realtors, engineers, or educators. If an on-premises software product does not yet have a cloud-based equivalent, it likely soon will. A lawyer tasked with reviewing a SaaS agreement (or any cloud contract) should learn how a typical cloud contract allocates the parties' rights, liabilities, and obligations.

The Shared Responsibility Model

The public cloud alters the underlying commercial framework of computing, as noted above, as well as the framework of responsibilities among the customer, the vendor, and others in the vendor's supply chain. Under what is known as the "shared responsibility model," the parties to a cloud contract are generally responsible for those technologies and services that each party controls.

In a SaaS relationship, the cloud provider is ordinarily responsible for buying, maintaining, and updating computer servers, operating systems, network infrastructures, and end-user software programs. Customers, on the other hand, are only responsible for configuring the software, inputting their data, and managing their access to the Internet. (It is important to note that customers are responsible for maintaining appropriate privacy and security controls within the customer's environment; many customers overlook this fact to their peril.) Cloud providers are responsible for allocating computing resources to meet the cloud customer's needs, keeping the computing infrastructure physically and technically secure, and ensuring customers' data remain available through replication processes and backups. By paying for cloud providers to relieve the customer of these responsibilities, cloud customers can focus on their core businesses.

What Legal Services Do Cloud Clients Need?

Public-cloud-service relationships share many basic premises, features, and risks. Some familiarity with them is useful whether negotiating terms for a cloud customer with enough relative bargaining power to do so or advising a client considering whether to accept any cloud provider's click-through TOS.

Preliminary Matters

Before approaching the nitty gritty of the agreement itself, the lawyer should consider discussing the client's business processes and its use of computing resources. Every client—especially one proposing to use cloud computing—should take time to inventory its data, map data and business-process flows, and reflect on dependencies in its prospective cloud supply chain, such as the reliability and availability of the client's Internet connection. The lawyer should ask whether the client has a written data-security policy; if the client does not have one, the lawyer should advise the client to create one. (The National Institute of Standards and Technology publishes valuable guidance for best practices in cybersecurity.)

If advising a smaller cloud-service provider, the lawyer should help the client account for its own cloud-based dependences. These can include upstream suppliers of cloud services; the size, experience, and abilities of their staff and management; virtualization software providers; and datacenter security and vulnerabilities, including power supplies and backup systems, exposure to natural disasters, and the capacities of their network suppliers. The lawyer should discuss with a cloud-provider client the risks in failing to make realistic commitments.

Both cloud customers and cloud providers should consider that, as a new industry, cloud computing presents the potential for informational asymmetry and related incentives for silence in contracting. That is, as the cloud industry matures, parties' experiences and

their litigated disputes will likely lead to more express terms.

Common Risks for Cloud Customers

Lock In. A lawyer should discuss with a client the termination of a cloud-service contract. Clients should consider that the time may come when they no longer want the cloud service. Some services convert customers' data into a proprietary format that is costly to reverse engineer. Clients would therefore be well-advised to consider that risk before entering a cloud-service agreement. Clients should also review what services they might need from the provider to retrieve their data. Often, cloud providers offer, free of charge, generous customer assistance for on-boarding customer data, but either will provide little to no assistance in returning a customer's data on termination or will require payment for that assistance.

Hidden Costs. In addition to unanticipated data-migration costs at termination, a lawyer should help a client thoroughly analyze the life-cycle cost of cloud services. What looks like savings in the short term may result in undesirably burdensome long-term costs over the life of a cloud-service agreement. A lawyer should also alert a client to potential costs arising from one of the cloud's greatest attractions, automatic provisioning of additional computing resources. If misconfigured, a cloud service may automatically provision cloud computing resources in an unintended and unexpected way, resulting in sudden, crushing expenses to the customer. Customers should know well the technical features of the products they are using, develop robust internal monitoring procedures, and use the provider's usage monitoring tools to manage this risk.

Amendment of Terms of Service. Virtually all cloud providers large enough to require the use of click-through agreements reserve the right to amend unilaterally the TOS. (The one notable exception is Salesforce.com, an online Customer Relationship Manager and the first big SaaS provider, which states that no modification to the TOS will be effective unless written and signed by the party against whom the modification is to be asserted.) Most cloud providers actually put the onus on the customer to check the provider's Web site for changes, many give no notice when a change is made, and some do not point out what terms have changed. As a result, customers are exposed to the risk of changes that disrupt what may have become a core business process for the customer. Some providers allow amendment-based cancelations of service, but the costs associated with termination may be significant.

Security. Providers invest heavily in physically securing their datacenters, deploying the most up-to-date technical controls, and maintaining robust administrative policies and procedures to protect their systems. A lawyer should help ensure clients do their part by implementing appropriate security controls. The more obvious password, encryption, and malware controls are not sufficient. Customers must implement strict procedures for controlling their cloud environments. Many notorious data breaches did not result from bad actors breaching cyber-security barriers. Rather, customers had simply misconfigured their cloud services. In one famous example, a company hired by a major political party to analyze voter data exposed the company's analysis of 198 million American voters, including sensitive identifying details, by leaving open a public-facing cloud server, unprotected by any security barriers at all.

Providers' Limitations on Liability and Remedies. A lawyer negotiating a cloud-services agreement should know that providers typically impose strict limits on their liability—a sensible idea from the position of a provider of a cheap, standardized commodity. Most often, a provider's liability is limited to an amount represented with reference to the customer's use over a given period, such as 125 percent of the customer's preceding six-months' paid fees. Lawyers should also attend to a provider's remedies in the event of a customer's breach of an acceptable use policy or, more often, a failure to pay. A customer whose business depends on a cloud service would potentially be crippled if a provider suspended service on little or no notice.

Data Ownership and Licensing. Cloud agreements vary in their clarity over the ownership of data uploaded to cloud services. Lawyers should advise clients to consider whether the cloud provider's agreements regarding data ownership and any attendant rights—licensing of uploaded data, for example—are compatible with the nature and sensitivity of the customer's data.

Common Terms in Cloud-Service Agreements

Although expressed in many forms, cloud-service agreements usually contain the following elements: Service level agreement, data ownership policy, acceptable use policy, security policy, data protection policy, business continuity policy, upgrade policy, and termination policy. There are currently no standard naming conventions, structures, or forms for these agreements.

Service Level Agreement. A service level agreement ordinarily sets out service-level objectives, such as service availability, data-handling capacities, and service reliability.

Often expressed as percentages, these objectives should state terms for the time frames for these measurements and specify sources for reported performance data. A lawyer may want to ensure clients have the opportunity to conduct third-party performance audits.

Acceptable Use Policy. The provider's acceptable use policy ordinarily constrains only misbehavior, such as using the provider's resources to engage in criminal activity, support terrorism, or distribute malware or spam. (Several prohibit using their resources to develop weapons of mass destruction.) A lawyer should read these provisions with an eye on the provider's contractual ability to access the customer's data to monitor compliance with the acceptable use policy.

Data Protection Policy. A data protection policy describes how the provider handles (what it knows to be) sensitive data. These policies are often expressed as quality objectives referencing third-party certifications, such as a Service Organization Controls report or an ISO 27001 certification. Lawyers should review the provider's data protection policy.

Security Policy. A security policy allocates security responsibilities between provider and customer. A lawyer should advise a client of the client's security obligations pursuant to the cloud services agreement. If, for example, a provider expressly does not encrypt customer data at rest, the customer bears the attendant responsibilities or risks the customer's data remaining unencrypted. The provider may specify its adherence to data security standards or its possession of relevant certifications.

Business Continuity Policy. A business continuity policy describes the service's resiliency features, including system redundancies, data replication techniques, and event-response objectives. Such a policy might describe a number and general location of datacenters at which the customer's data are replicated, maximum acceptable time within which the provider agrees to restore the customer's data or service, and the maximum acceptable time during which data might be lost.

Termination. A lawyer should review terms involving termination, including triggering events, notifications, opportunities to cure, data off-boarding, data reversibility, and data deletion. For example, a cloud-service agreement should not allow a cloud-based medical records provider from suspending service without adequate notice, essentially holding hostage a health-care provider's electronic medical records, after unilaterally declaring a substantial price increase.

Conclusion

These offerings change constantly. A practice considering moving some or all of its computing work to a cloud provider should thoroughly research the marketplace and the suitability of a particular product for a practice, read other users' online reviews, solicit input from friends and colleagues, take advantage of free-trial demonstration offers, and assess the long-term viability of prospective providers. In every case, however, lawyers should first be mindful of their unique responsibilities.

Is the Cloud Right for Your Practice?

The most dangerous aspects of cloud computing for a legal practice may be its invisibility and convenience, qualities that suit most businesses but that lawyers should consider from the perspective of their unique professional responsibilities. Dropbox, Microsoft 365, Google Drive, and many others are easy to use and widely adopted. Their economy and convenience work for most businesses. But a confidential communication between a lawyer and client is among the most protected of all information in the world. Lawyers owe their clients a duty to handle this and all of their clients' sensitive information with care. Lawyers should be aware when they entrust sensitive information to third parties and take reasonable steps to protect the confidentiality of their clients' information.

Before the 1980s, law practices ran on typewriters and copiers. In the 1980s, desktop computers introduced word processing, and information moved from papers in a file folder to graphic representations of folders on a computer's hard drive. In the early 1990s, office desktop computers became networked with each other, and the information in those abstract folders moved to a server down an office hallway. Advances in telecommunications soon connected on-site networks to the World Wide Web, and information could instantly move from a law firm's servers down a real hallway to someone else's servers far away—into the "cloud."

Client information does not move itself, and a lawyer should exercise due care when choosing to move sensitive client information away from the lawyer's servers that are located within premises the lawyer controls.

Cloud Computing

Rules of professional conduct for lawyers generally require that "[A] lawyer shall provide competent representation to a client . . . [which] requires the legal knowledge, skill, thoughtfulness and preparation reasonably necessary for the representation."[5] In 2014, the Supreme Court of Arkansas amended the comment to the Arkansas rule to include the following: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . ." The drafters of the Model Rules of Professional Conduct crafted this amendment to address technological developments such as cloud computing.

Professional-responsibility authorities in at least 20 states have published more expansive guidance regarding lawyers' use of cloud-computing services. Generally speaking, this guidance is based on rules of professional responsibility and duties of diligence and care that all lawyers share; common features of their opinions (expressed here in broad strokes) include the following:

- Learn about the provider, its qualifications, and its ability to fulfill its obligations;
- Pay attention to the TOS, including breach-notice obligations, notice of third-party data-access requests, encryption and replication features, data-destruction-on-termination duties, licensing rights, service limitations, and remedies;
- Understand the technologies involved—ask experts, as needed, and stay current on developments;
- Consider the sensitivity of the information (some is too sensitive to entrust to others);
- Mind legal and regulatory obligations (HIPAA, Graham-Leach-Bliley, *etc.*);
- Consider clients' instructions;
- Exercise meaningful oversight;
- Maintain good cyber-hygiene habits throughout a practice;
- Periodically review the foregoing.

Considering lawyers' professional responsibilities, cloud-computing services that are appropriate for many businesses may not be appropriate for some aspects of some legal practices. For example, consider Google Drive, a cloud-based office suite with word processing, spreadsheet, and presentation tools. Under the TOS, a Google Drive user grants Google "a worldwide license to use . . . communicate, publish . . . and distribute" any content that the user uploads, stores, sends, or receives through the service.

Once the professional-risk landscape is understood and managed, lawyers can enjoy the range of benefits cloud services generally provide. Files can be accessed by any Internet-connected browser or, in many cases, on a smartphone or tablet app. Computing costs shift from a capital expense to an operating expense. Software licenses, patches, and upgrades, depending on the service, become the responsibility of the provider, reducing a lawyer's in-house information technology labor and license expenses. The cloud-provider's experts and robust infrastructures assume responsibility for the physical security and maintenance of servers.

The range of cloud services is vast. At one end of the spectrum, some practices use only cloud-based storage for periodic, off-site backups. Those who do should take appropriate steps to ensure their confidential data remain secure. If the service does not provide for encryption of the data both in transit and at rest, lawyers should encrypt it first—a sound practice, even if the provider offers encryption.

At the opposite end of the cloud-service spectrum are cloud-based services specifically designed for lawyers. Many of these services originated as stand-alone software products but have evolved into cloud-based services.

Some of these serve single needs, such as billing and accounting, including trust accounting, or electronic-signature management. Others are built around supporting specific practice areas, such as bankruptcy, patent,

and personal injury, by integrating client-intake, calendaring, accounting, and document management features within the framework of each practice area. In addition to these law-practice-specific tools, there is a growing market of specialists who provide entire cloud-based computing environments for lawyers. These specialists anticipate practices' reliance on some of the more-popular practice-specific software products and integrate these products into their services, thereby promising that the migration of a practice to a comprehensive cloud environment will be a seamless exercise.

Notes

1. This article only addresses the public cloud. In contrast, the private cloud refers to computer infrastructure provisioned for the exclusive use of a single organization. A private cloud may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. *National Institute of Standards and Technology (NIST)* Special Publication (SP) 800-145.
2. *See NIST* SP 800-145, 146, and ISO/IEC 17788:2014.
3. ISO/IEC 17788:2014.
4. Given the big four providers' highly integrated product offerings, this particular scenario of fragmented services is not realistic. It is only intended to illustrate the potential existence of an undisclosed, complex supply chain.
5. *See, e.g.,* Arkansas Rule of Professional Conduct 1.1.