SECTION ONE

Cloud Computing: Basics of Technologies and Applications

CHAPTER 1

Cloud Computing Definitions and Technical Considerations

Christopher Thieda

The introduction of cloud computing has taken technology users by the hand and brought them into a new realm of possibilities. Whether the purpose is for personal, corporate use, or anything in between, today's everyday tech users have been exposed to a multitude of cloud practicalities. Cloud computing applications allow computer users to conveniently rent access to fully featured applications, to software development and deployment environments, and to computing infrastructure assets such as network-accessible data storage and processing. Those that have exposure to common applications such as Google Apps or Microsoft Office 365 likely already have experience with cloud computing, even though they may not have realized it.

The term *cloud computing* has a variety of definitions, mostly because it has become a powerful marketing term. The National Institute of Standards and Technology, the federal technology agency that works with industry to develop and apply technology, offers this definition:

> Cloud computing is a model for enabling 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]

Today, technical questions remain that occasional users might not dare to ask regarding how virtualized models actually operate, where data

actually resides, or who actually controls access to the data and applications, but for some users that are financially dependent on or have sensitive data involved with their cloud solution, those questions should be addressed. Parties to litigation will also naturally be concerned with the answers to those questions as well. Of course, there are numerous advantages to cloud computing from the perspective of the customer. Scalability, cost efficiency, ease of implementation, and optimal resource allocation are some of the main benefits that stem from virtualization. Conversely, concerns have risen concerning cloud practices regarding security, storage location, and intrusion protection. For parties and their counsel involved in litigation, cloud computing has increased the complexity of electronic discovery. In this chapter, we will address the different cloud computing models, the issues of cloud computing applications, and the legal regulations involving virtual data capture. Cloud computing is a developing area, and the strengths, weaknesses, delivery models, and legal implications of its use are constantly in flux.

Virtualization is the key technology involved in cloud computing. In a virtual computing model, an organization can obtain the exact hardware and/or software solutions required, at the exact time it is required, without the need for a large capital commitment. Virtualization allows hardware and software owners to partition their resources and provide the exact quantity of resources needed to satisfy their customers. This model has existed for a while, but has been advancing in recent years due to the common availability of low-cost, high-speed data communications infrastructure.

There are three main service models seen in today's cloud computing environments. We will focus on: cloud Infrastructure as a Service (IaaS), which allows organizations to outsource hardware, cloud Platform as a Service (PaaS), which allows organizations to outsource operating systems and web infrastructure, and cloud Software as a Service (SaaS), which allows companies to outsource applications. These layers create the core of cloud computing. Since they share the commonality as components of the cloud, each of the three layers accomplish specific tasks and have the capabilities to complement one another in an entirely virtual environment. IaaS is the substitution of virtual solutions for hardware that is commonly used within a company's network. PaaS is created for users to be able to build and implement their own virtual, web-based solutions. SaaS is centered around supporting users entirely through web-based resources, and it is the most commonly seen model in today's cloud market. Every cloud layer provides a differentiation factor versus standard enterprise networking while providing a broad range of possibilities for users looking to delve into the world of virtualization. Most consumers will typically contract with an SaaS vendor to provide a web solution, and may not be aware that the

infrastructure and platform levels have also, in turn, been outsourced to other cloud vendors.

IaaS

Cloud computing has provided organizations with the advantage of configuring their network based on using resources in the most efficient manner. IaaS is the foundation of the three cloud layers. It is a virtualized availability of hardware that can substitute for pertinent networking items such as servers, firewalls, and load balancers. Instead of purchasing a physical server and firewall with a set amount of data capacity, virtual network solutions are available where storage and computing power is scalable depending on the organization's requirements. Virtual machines have also created a way for users to obtain similar functionality to preexisting hardware while eliminating data center space and recurring physical support costs including maintenance, power consumption, and expertise to operate the hardware. The elimination of overhead costs and flexibility are the main reasons why companies choose to source their infrastructure through the cloud.

Although there are many benefits of virtualizing an environment, network administrators must have a thorough knowledge of networking and how infrastructures should be constructed in order to properly configure their cloud requirements. Administrators must be well-versed in dealing with different virtualized operating systems and interfaces. An example of an important resource to be familiar with when dealing with a cloud-based infrastructure is a hypervisor. A hypervisor is software that enables users to monitor and control servers that are built on hosted environments. Hypervisors are an extremely useful technology piece to remotely allocate shared resources that can have a large impact concerning how efficiently data is transferred.

There are two types of hypervisors, depending on how they are implemented. The first is a type-1 hypervisor, which is built directly on the server platform and communicates with resources designated by the service provider. The second is a type-2 hypervisor, which is built on a preexisting host operating system and can interact with associated virtual systems thereafter. A type-1 hypervisor is more commonly used in business practices, as it minimizes any latency potential and maximizes networking efficiency from its direct source of interaction with the server. Type-2 hypervisors are still a useful way to virtually manage servers and can be effective when the operating system is communicating with input-output style computing processes, similar to how personal web surfing is conducted. VMware, a popular cloud service provider, offers both type-1 and type-2 hypervisors with their operating

systems. VMware's ESXi is an example of a type-1 hypervisor, whereas their VMware Server software is a type-2.

It is important to understand hypervisors and how they work, as it could aid in reducing potential security threats. If an organization is looking to minimize risk against their virtualized infrastructure, they could implement an efficient hypervisor strategy to stop any malicious attacks from taking down their entire network. Hypervisors can be set up by separating virtual servers with the intention of preventing compromised network channels from negatively impacting other servers. Instead of an attack on a host causing a severe security breach for all virtual machines associated with it, hypervisors can be set up by segregating how information is transferred. Hypervisors also provide the advantage of transferring data using encrypted communication methods such as Internet Protocol Security, commonly referred to as IPsec.

The most significant element concerning cloud computing infrastructure is that there are differences regarding how cloud networks can be implemented. This breakdown is categorized into three cloud computing groups: public, private, or hybrid. Each is distinctively separated in terms of how the software, firmware, or infrastructure is hosted.

Public Cloud

Public cloud computing provides users with the availability of hosted online resources through service providers. This is the most common cloud application seen in today's market due to the integration ease for new users and its convenient bundles that can be purchased according to requirements and usage. Instead of having hardware on site and needing to constantly create data center space, public cloud computing is an alternative hosting solution.

Because it is externally hosted, the added benefit of network flexibility also comes along with vagueness regarding how data is stored and where it resides. As previously mentioned, public cloud is a service provided and sourced entirely through a service provider's infrastructure; the service provider is providing services to hundreds if not thousands of organizations. Thus, public cloud solutions are hosted through an infrastructure with a mixture of data from other entities. In a traditional computing model, organizations operate with enterprise hardware they actually own and control, and have the benefit of physically knowing where data is being stored at all times. Cloud users operate with the hindrance of not having direct physical control over the hosted network (i.e., the actual hardware) within which their data lies. During discovery, this limits the ability of investigators to directly access the data of interest. This transparency limitation can also cause the potential for unfavorable variances with data security.

Not only is there a lack of direct control over hardware resources with public cloud computing, but there is also the limitation of knowledge regarding how data is being secured. Most cloud service providers have security precautions in place, but for the wellness of your network and your data there should be an audit of the service provider's security measures prior to any solutions being implemented. Users should address vendors with questions asking about the set of security standards by which they abide. An example of an information privacy standard is the ISO/IEC 27000, which is a series of security regulations recommending best practices regarding maintaining information security management procedures. Guidelines like these provide insight into minimizing vulnerabilities and constantly being aware of new security threats. It is important to implement information security business practices that help protect against threats compromising information relating to their company, their employees, or their customers.

With this data being stored through a public cloud service, organizations must have a way to obtain data when needed. Accessing externally hosted data is made possible through cloud application program interfaces, or APIs. APIs allow users to communicate with a multitude of software components to be able to properly transfer data from one source to the next. These APIs are created to conform to interfaces such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP). REST and SOAP are web-based protocols created to oversee the sending and receiving of HTTP data between operating systems.

Continuing further, APIs are entitled to communicate with cloud storages to specify what data users are looking to obtain. An API that conforms to REST can use HTML requests to obtain data quickly and easily. Things become more complicated when archived data stores must be accessed from a cloud service provider. These actions can take much longer periods of time to retrieve, as cloud archival data stores are created to be accessed only on an occasional basis, and typically only for a file or two at a time. A wholesale restore from archival data can require a surprising amount of time.

Hosted archives can provide an additional discovery point during litigation, and the existence, location (i.e., host name), and chronology of those archives should be cataloged as part of the discovery process.

Private Cloud

The private cloud is a way of implementing a cloud infrastructure for the use and management of a single organization. The purpose of private cloud computing is to have the benefits of virtualization, such as the elimination of multiple servers, while having an infrastructure dedicated to one entity. It can either be hosted internally or externally, meaning that their infrastructure

could be served through their internal resources or through a private cloud service provider. Private cloud solutions are typically utilized by larger organizations who wish to control potential risks that come from operating with a public cloud.

From a discovery standpoint, private clouds are more akin to traditional computing models. Hardware is typically directly controlled by the organization, and, because the private cloud does not involve a service provider offering service to the public, the disclosure restrictions of the Stored Communication Act do not apply. Technical issues may still be present as servers and archives are virtualized, however, the legal restrictions placed upon a third party responsible for the data should not be present.

Self-hosted private cloud solutions serve as a tool for organizations to obtain a singularly dedicated environment that is internally managed. It creates a highly secure network structure while giving administrators more control over the configurations of the network in comparison to public cloud computing. If hosted internally, it would require on-premise hardware for the cloud architecture to function, thus creating initial and recurring operating costs for the organization.

With external hosting, there is still only one entity being managed through the cloud. The main difference between self-hosting and external private cloud hosting is the lack of control and insight with regard to data management and storage. Despite this, utilizing these computing resources can be a potential option for organizations that prefer to operate with the flexibility that comes with the public cloud while addressing the security risks that come along with sharing service provider resources.

Hybrid Cloud

Those who see cloud computing as a pertinent piece to introduce into their network but wouldn't particularly benefit from a completely externally or internally hosted infrastructure can pursue hybrid cloud computing. Hybrid cloud computing is a flexible way of combining on- and offsite applications without running the risk of exposing potential vulnerabilities or accruing unnecessary physical maintenance costs. Therefore, this style of configuration can help organizations choose what network resources they feel should be privately managed and those that should be publicly hosted for less security-sensitive applications.

For example, a company is looking to deploy an architecture that would efficiently and securely correspond to their sector and customer needs. They could utilize hybrid cloud computing through using multiple deployment models, obtaining the most ideal resources from each model. The company could use a more traditional private cloud environment for their internal

portals and network servers. Additionally, their website could be externally hosted, considering the information is already made for public viewing and is less of a security concern if those information stores were to be breached. Minimizing exposure to security risks is one of the fundamental elements that differentiates hybrid computing from a standalone public or private cloud architecture. For discovery purposes, it will be important to understand the relationship between the organization and the service provider. If the service provider is providing services to the public, restrictions of the Stored Communication Act may be in play with regard to the data.

PaaS

PaaS is one of the most powerful ways that cloud computing has changed how applications and resources are created and maintained. This cloud layer provides developers with the architecture to which they can construct their own applications; PaaS vendors provide a ready-to-go hosting area for applications. This ability is generated through virtually hosted services supplied by a cloud service provider. PaaS has made it easy for web developers, software developers, and others to create their own solutions without owning any hardware or installing any tools on their computer. Regardless of the complexity of the applications that are being developed, users can then deploy these applications without the need for enterprise networking or technical skills. Many popular cloud applications are hosted on PaaS platforms owned by another provider.

PaaS providers offer a multitude of offerings to help aid in the development. There are platforms available where users are guided through a simple, step-by-step process that eliminates the need for a technical understanding of the framework. Users can also choose to build their platform based on a preexisting architecture, which can remove any initial layout confusion. Through its flexible development procedure, if users need to make alterations to their platform after it has already been deployed, they can easily retain or exclude necessary features without accruing high-level costs. PaaS services are frequently utilized through subscriptions where users are only expected to pay for what they need. PaaS is an efficient way to allocate resources by using what is necessary to develop and manage the application.

PaaS is highly suitable for developers interested in creating a web-based application. It can be a very useful tool involving scenarios where the automation of testing and deployment proves to be a primary advantage. Additionally, PaaS can become a fundamental resource when collaboration is an important factor in the applications building process. However, the service can be counterproductive if large data must be incorporated within the application.

SaaS

The term *Software as a Service* originated in the 1990s and therefore predates the current term *cloud computing*. While many variations of SaaS are possible, a simple explanation is that it is software deployed as a hosted service and accessed via the Internet.

The rapid rise in consumer needs and expectations has caused the ongoing development of efficient ways to deliver data through on-demand and rapidly responsive applications. Thus, information service providers and organizations have introduced services through the SaaS cloud model. SaaS applications are frequently developed as a broad solution for users of all demands and technical backgrounds. Added with the scalability of these services, consumers can easily upgrade their level of service, such as storage and data capacity, while still using the same functionality and maintaining fluency within the tool. Thus, clients only pay for what they need, creating an elastic financial solution. This "pay-as-you-need" model is a staple for SaaS and has been a major reason why it is so commonplace in the consumer technology sector.

Despite its applicability, SaaS is very interchangeable from one solution to the next. It is difficult for information service providers to present a unique benefit that would help draw consumers toward their solution versus comparable services. For most successful SaaS platforms, intuitiveness and ease for users within the tool has seemed to be fundamental for its success. Customer resource management providers such as Salesforce and e-mail providers such as Google were some of the early implementers of SaaS. Thus, they have garnered the benefits as first-movers by being two of the top resources in their respective categories.

Despite its advantages, the SaaS cloud layer is still not yet a universally reliable tool. Thus, disagreement has arisen regarding when SaaS should be applied in business practice. SaaS is commonly utilized when remote data storage and virtualization outweigh the costs associated with having onsite hardware. The advantage of having service providers supply the application software through the cloud eliminates necessary maintenance. However, SaaS might not be appropriate when speed is of the essence. Due to the hosting of the layer, data is only transferred as fast as Internet speeds allow. This latency could be substantial for organizations of larger sizes or those that deal with urgent applications.

Considerations for Discovery

Data in a cloud computing solution may be contained within assets owned by up to three different companies: an IaaS vendor who owns and operates the actual physical server hosting the data, a PaaS vendor who controls the

operating system and distribution of the data, and the SaaS vendor who controls the application. In a public cloud model, the end customer will typically only have a relationship with the SaaS vendor, however, in some circumstances, and certainly in a private cloud model, the end customer would have relationships with the other layers as well. Parties to litigation should consider the relationships with cloud vendors across the platforms when crafting their discovery strategy.

To the extent that the cloud vendor is providing service to the public, discovery may be restricted by the provisions of the Electronic Communications Privacy Act, as discussed later in this chapter.

Service level agreements will likely be in place between the end customer, and directly or indirectly between vendors in the different layers of the cloud computing platforms. Parties to litigation should understand the terms of the service agreements as they define the relationship and responsibilities between the parties, including the duties of the cloud customer and those of the cloud provider. They will also potentially describe the procedures to access data in the event of litigation. The following are excerpts from the Gmail (Google-hosted e-mail) cloud e-mail application:

> Information we share
>
> We do not share personal information with companies, organizations, and individuals outside of Google unless one of the following circumstances applies:
>
> - With your consent
>
> We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.
>
> - For legal reasons
>
> We will share personal information with companies, organizations, or individuals outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:
>
> - Meet any applicable law, regulation, legal process, or enforceable governmental request.
> - Enforce applicable Terms of Service, including investigation of potential violations.

- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property, or safety of Google, our users, or the public as required or permitted by law.[2]

The terms of service agreement should also define the vendor's data preservation requirements. Many agreements specify that if a subscriber's access to cloud services is terminated "for cause," (i.e., because the subscriber has violated the cloud's acceptable use policies or for nonpayment) the provider may state that they have no obligation to preserve any consumer data remaining in cloud storage. The terms of service agreement should also indicate the disposition of data in the event the subscriber stops using the service, for example, if they did not log into their hosted e-mail account for a period of time; providers generally state that they will suspend the service after an interval, but will not intentionally erase the consumer's data for a period of 30 days beyond that interval. Some providers indicate they will preserve only a snapshot of consumer data, or recommend that consumers: (1) back up their data outside that provider's cloud inside another provider's cloud, or (2) back it up locally.

Most cloud services require acceptance of the terms of service during the subscription process. This can help identify the subscribing party who might be deemed in control of the contents for purposes of compelled disclosure.

Providers generally reserve the right to change the terms of the service agreement at any time, and to change pricing with limited advanced notice; notice would typically be given to the subscriber of the service. For standard service agreement changes, notice is generally given by a provider by posting the change to a website, and it is the consumer's responsibility to periodically check the website for changes. Changes may take effect immediately or after a delay of several weeks. Litigation involving customer account information should consider that changes could be made to the terms of service over time, and that it might be essential to determine the terms of service applicable during the time frame of the litigation period.

Data Transfer Regulations

The movement of data around the world through cloud computing solutions is technically quite easy. However, it can be heavily limited through global restrictions. There are policies in place to prevent the misuse and unnecessary disclosure of data pertaining to individuals, but these regulations are created on a sectorial basis or, in other words, promulgated by particular countries. However, just because they are created by one country doesn't mean that they

aren't applicable internationally. Cloud computing is highly correlated in this sense, as it relates to the global ease of data transfer and storage. With cloud computing solutions, data could reside within multiple different entities or countries equating to the potential need of complying with multiple different data regulation policies.

The Electronic Communications Privacy Act (ECPA) is the primary law regulating disclosure of information in the United States. Courts have determined that law applies to user information of foreign nationals, even if they themselves have never been to the United States. In *Beluga Shipping v. Suzlon Energy Ltd*,[3] Suzlon claimed that three former employees had formed an independent company and profited from shipping Suzlon's cargo. The former employees used Gmail accounts to communicate with each other and with potential customers. Suzlon petitioned for leave to conduct discovery in aid of foreign judicial proceedings pursuant to 28 U.S.C. §1782; Google moved to intervene and opposed the petition. The U.S. District Court, Northern District of California, San Jose Division held:

> Suzlon seeks, inter alia, the contents of the individual cross-defendants' email accounts. Pursuant to Electronic Communications Privacy Act (18 U.S.C §§2701-2712), non-party Google states that consent from the individual cross-defendants is required, and that until, and unless, their consents are obtained, it is unable to comply with the subpoenas. *See* 18 U.S.C. §2702 (the ECPA's description of the voluntary disclosure of customer communications or records); *see also Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004) (the ECPA protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility); *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1447 (2006) (the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted). A subpoena can be permissible if it seeks the identity of specific emails or of accounts. *See O'Grady*, 139 Cal. App. 4th at 1447. The ECPA, however, prohibits a subpoena if it seeks the content of any email account absent a consent. *See* 28 U.S.C. §1782 (2010). Because Google knows that it cannot comply with the subpoenas, it seeks to intervene at this stage of the proceedings and to oppose the petition, even though the subpoenas or deposition requests have not yet been issued.
>
> Suzlon contends that the ECPA does not apply to foreign citizens, and, therefore, Google may comply with the subpoenas. Specifically, Suzlon relies on Zheng v. Yahoo! Inc., which held that the ECPA does not apply to electronic communications of foreign citizens. *See Zheng v. Yahoo, Inc*, 2009 U.S. Dist. LEXIS 111886 (N.D. Cal. Dec. 2, 2009)

> (M. Chesney). However, the court in Zheng found that because the email interceptions and disclosures occurred outside of the United States by a company whose servers were located outside the United States, the ECPA would not apply or extend to the foreign nationals. In the present case, however, Google and its servers are located within the United States and, therefore, the ECPA applies. As such, the ECPA prohibits Google from disclosing the contents of those email accounts until it receives consents from the email account holders. Therefore, it is futile for the subpoenas to issue until notice has been served and consent has been obtained from the cross-defendants. Accordingly, it is appropriate for non-party Google to intervene at this juncture to oppose the petition and to deny the petition insofar as it seeks the content of the specific email accounts set forth above.[4]

Another example of this type of data regulation is the European Union's Data Protective Directive 95/46/EC. This policy heavily restricts the data transfer of global organizations due to its rigid guidelines. The directive was created to limit and protect the personal data of European Union residents. This legislation not only applies to entities that lie within the European Union but also to non-European organizations. Additionally, those that use equipment located within those said EU boundaries must comply with this policy. Thus, cloud service providers must abide by these regulations when providing solutions to organizations located in the European Union, or while using hardware resources and data centers located within the European Union.

There are a number of requirements within the EU Directive that are highly applicable to cloud computing processes and services. If data is shared, organizations must obtain consent from the subjects whose data is being shared. Organizations must also have procedures in place to keep data safe and secure from potential threats, including security breaches and unauthorized intrusions. Involved subjects also must be made aware that their information is being collected and stored by the parties involved in the storage of said data. These are just a few of the necessary protocols that must be institutionally implemented to conform to the EU Directive.

The distributed nature of cloud computing makes understanding the applicable regulations and abiding by those regulations challenging. A primary example is the sourcing of public cloud computing resources. Since public cloud computing solutions can be globally sourced, there are numerous difficulties involved with security of information, along with users not knowing where their data lies. For example, an application developer may contract space with a PaaS vendor, and in turn the PaaS vendor may host their platform with an IaaS vendor who owns and operates data centers in a foreign country. The application developer may not even know that the data centers are hosted there, but could

be responsible for conformity with legal standards in that country. If a cloud service provider has international data centers, there could be a possibility that it may be hosted through a country that has its own set of compliance rules and regulations.

The European Union is currently looking to fully adopt a new data protection policy by 2016, called the General Data Protection Regulation, which is a revision of the original Data Protective Directive 95/46/EC. With the increase in cloud computing practices, non-European organizations are troubled that this new legislation will make data transfer within member countries of the European Union even more difficult and come with even greater penalties for nonconformance. These revisions call for the potential erasing of data if it is misused, the prevention of personal data being sent outside of the borders of the European Union and larger fines for noncompliant businesses. Fines could cap out at 5 percent of an organization's total revenue if they do not abide by these new regulations, replacing the previous policy's max fine of 2 percent. These data protection policies could cause a massive hit to internationally operating tech companies that supply cloud services. Increasing global regulation is just one of the many ways that the use of cloud computing is changing not only how technology environments are created but also how compliant business must be with regard to data handling.

Notes

1. NIST Cloud Computing Definition, NIST SP 800-145.
2. Gmail, Privacy Policy, retrieved January 29, 2014, www.google.com/intl/en/policies/privacy.
3. *Beluga Shipping GMBH & Co. KS "Beluga Fantastic" v. Suzlon Energy Ltd*, Federal Court Proceedings, NSD 1670 OF 2008 Before the Federal Court, New South Wales, Australia.
4. *Beluga v. Suzlon* 09-23-10, Order.