Understanding Basic Elements of Cloud Operation

Catherine Sanders Reach

Follow this and additional works at: https://via.library.depaul.edu/bclj

Recommended Citation
Available at: https://via.library.depaul.edu/bclj/vol12/iss4/2
DEAN MARK: Thank you very much, and thank you very much for coming to DePaul University and especially the college of law today. It is a great pleasure for me to welcome you here, especially because what we see here today is the interaction of two different journals, the Business & Commercial Law Journal and the Journal of Art, Technology & Intellectual Property. What I think is especially terrific about both of these Journals is that they are student run, and so this represents the best, the most entrepreneurial aspect of the law school. Our students come together in the event of a cutting edge conference because very few things can be considered more cutting edge than the use of the Cloud and the legal ramifications thereof.

I can only say, by way of example, that just two minutes ago I was talking with my colleague, Josh Sarnoff—who you will hear from later today—about the terms “bull” and “bear,” and he asked if I knew the terms’ origins. Given my history experience and my interest in corporate law, I turned to him and I said, “No, I think it might have something to do with pitting a bull against a bear in a medieval marketplace.” But why are we asking each other this hypothetical question when we can just go to the Cloud and get the answer. And the answer is, Josh?

JOSH SARNOFF: There are multiple possible sources, including that “bull” in French, meaning “above, inflate, or swell,” and bear, meaning “swipe down”; bull, swipe up. And I can go on.

DEAN MARK: Right. That tells you how immediately accessible information can be even if it turns out you do not get at the definitive answer. But the Cloud presents, not just the possibilities of obtaining information, but all kinds of issues about its use from obvious questions of jurisdiction to other questions about how you—even if you had jurisdiction, how do you chose to access it.

I am delighted that this conference is here today to talk about some of the most cutting edge issues. As I said, it represents the best of the college of law. It represents the best that our students have to offer.

On that note I should leave the rest to the real speakers here today and simply say thank you for coming and please share my joy in the efforts of the students.

AARON COOPER: Good afternoon. My name is Aaron Cooper and I am the editor-in-chief of the Journal of Art, Technology & Intellectual Property Law. I also want to echo Dean Mark's welcome to you.

Our first speaker will be Catherine Sanders Reach. She is the director of law practice management and technology for the Chicago Bar Association. She was the director at the American Bar Association's Legal Technology Resource Center for over ten years, providing practice technology assistance to lawyers. Prior to her work at the CBA and ABA, she worked in library and information science environments for a number of years, working at Ross and Hardies as a librarian. She received her master's degree in library and information studies from the University of Alabama at Tuscaloosa and her bachelor's in English, also at the University of Alabama at Tuscaloosa. Please join me in welcoming Ms. Sanders Reach.

CATHERINE SANDERS REACH: How many of you know what Cloud computing is? How many of you do not know what Cloud computing is? What we are going to do is try to describe Cloud computing and some of the issues to consider. Then the other speakers are going to elaborate on those issues. I am going to set the stage for what you should think about as you are thinking about the practice of law and how it is affected by the Cloud.

The first thing is I want to describe is the architecture of Cloud computing. It can be complex and varied. Actually, there are a lot of formal ethics opinions that have come out about Cloud computing because of all the issues that are going to be discussed today and how lawyers are using the Cloud. One formal opinion borrowed a maximum PC article definition, saying it is a fancy way of saying "stuff is not on your computer."

Cloud computing is using data or resources stored on remote servers. The Internet is twenty-five years old. So this is not new technology. This stuff has been around a long time. I remember in 1999 when the concept of software as a service came into the mainstream. At the time it was called application service providers, or ASP, which is a terrible acronym considering the alternative meaning. Everyone was using it. There was a time and billing application that lived in the Cloud, and many lawyers jumped on it. Then it disappeared, and then for ten more years the paranoia was rampant. As the Cloud slowly was encroaching in every aspect of computing, lawyers started using it.
again. Now, we have Microsoft Office in the Cloud. You can use Microsoft Office in a browser version or it can integrate with your installed desktop version.

The Cloud is a friendly way of applying web-based computing services that are hosted outside of your organization. In essence your IT infrastructure resides off premise. You will hear on premise, off premise. “On premise” simply means that the data or service is local, meaning it is in a room somewhere in the building. “Off premise” means that the data is maintained over the Internet by a third party instead of residing on a server at your home or office. With Office 365, for example, data and software is located and managed remotely on a server owned by Microsoft. So the IT infrastructure may no longer be serviced by DePaul or whatever law firm you may be working for. The data is owned by someone else, and this is intrinsic to one of the problems we see in terms of who owns the data and how it is manipulated and who has access to it. Data located online or in the Cloud is virtually accessible from anywhere, which is one of the benefits, but also a concern.

Cloud computing has evolved over the years. We started with mainframes. Over the years, we have seen a migration from mainframe, which was a thin client model. All the computers were patched into the mainframe where everything resided, and a dumb terminal was used to access it. We are coming back to that model again. Consider the tablet device. A tablet device has a light operating system, but the tablet’s power comes from what you can access through the Internet. The ease of access to data is one of the big reasons that moving to the Cloud has become popular so quickly because people can access their data anywhere. Before, data was stored on a disk, CD, DVD, or thumb drive. These devices do not have enough room to store very much data, and they are easy to lose—you forget where you put them. Now, data can be replicated all over the place. Data can be accessed from a phone, an iPad, a laptop, at home, at work. If data is put in the Cloud, it can be accessed anywhere. It is convenient. We can now access and manipulate data on portable devices. Cellular carriers have 4G and 3G network, in addition to cable and DSL. Internet is wherever you go. This is what has enabled the Cloud to become such a popular platform. Moreover, the delivery model in terms of pricing has allowed smaller businesses to become more flexible and more powerful in their use of technology.

Traditional IT models include having to buy servers and hire IT staff to maintain a network and then install software that carries a per license fee plus maintenance and support. With a Cloud provider, you
pay per user, per month. If you pay for six months or a year, the cost may come at a discount. All of the support, maintenance, and infrastructure is built into that cost. So although it may appear to be more expensive, the cost of a Cloud provider may end up being about the same as traditional IT models. It is difficult to do an apples-to-apples comparison of a Cloud provider versus installed software. You have to compare the cost over a five-year period to see which one costs more.

Another cost of traditional software is human resources—humans cost money. You also have to pay for insurance and employment tax. There is a lot of cost associated with operating an on premise network and software as opposed to having access to it through the Cloud model. However, another thing to consider when you do start your own business are capital expenses and whether it is going to be advantageous in terms of taxes to purchase software. You generally do not have to install anything to use the Cloud. You may have to install an application on your iPad or download a plugin for a browser. However, for the most part, there is no software to install. For a lot of the attorneys I work with, installing software in and of itself is scary. With the Cloud, there is rarely anything to install and get it to work. It is like magic, which is why attorneys like it so much.

There are a myriad of terms flying around regarding the Cloud. If you are using a computer at this point, you are probably using the Cloud in some form or flavor. Consider your day-to-day life and what constitutes as Cloud services. Take Netflix, for example. You stream a video through a Cloud service to your machine. No one buys movies anymore. We stream them. Dropbox is another example. People are storing their documents in the Cloud. Things like LexisNexis.com are Cloud services. Now, we see applications like Clio and Rocket Matter for law practice management.

There are a lot of acronyms that get thrown around to define the Cloud, and I am going to try to explain them from a broad perspective. You have SaaS, or software as a service; this is the broadest use of the Cloud and is fairly comprehensive. SaaS is browser interface software. Examples include Google applications and Microsoft Office 365. You get the software through the browser, and it takes care of storage, network back-up, and everything else that is needed to run the software from the server level. All aspects are taken care of by the vendor. There are also combination models of Cloud services. Large companies, for example, may actually own and operate a lot of their own technology. So it is advantageous to move some computing to the Cloud model, but not completely.
For instance, IaaS (Infrastructure as a Service) is a Cloud computing model in which the company manages the local applications and data, but the Cloud service provides the servers, storage, and networking. Examples include Amazon and RackSpace. Interestingly, those companies are also providing the servicing or networking for SaaS vendors. Thus, in addition to being able to use IaaS services for your own company, companies like Rocket Matter are actually storing data with Amazon.

Other Cloud models include Platform as a Service (PaaS), in which you can own and manage the platform and data. The vendor provides the operating system, databases, and web servers, and you supply the applications. And then there are mixed models, such as hosted platforms in which the server is hosted. Consider Microsoft Exchange. Microsoft offers Exchange for four dollars per user per month in order to be in a hosted Exchange environment. Originally, it was an on-premise server software, in which you would first have a server and then install the software, manage it, and maintain it. Now, you can get Microsoft to do all of this for you, as well as a whole lot of other providers.

For instance, a company called Legal WorkSpace maintains the entire desktop on their server that you access through any Internet enabled device. This is conceptually similar to using GoToMPC or LogMeIn where you are logging in from another computer. The hosting provider maintains all the licensing for your software. They do the maintenance, installation, and support. You log in and have the full Microsoft Office Suite, including whatever applications you might want to have. You pay them a per-user, per-month fee to do all that. This model makes sense for some law firms and somewhat reduces risk. However, you are still using the public Cloud.

So what is the difference between a public Cloud and a private Cloud? A private Cloud is similar to a virtual private network where you tunnel through the Internet but nobody can see you. Then, they come up with https, using the public Internet, to create a private tunnel. This allows products like the File Transporter to come into being. File Transporter is physical box that lets you store files and remotely access them online. Instead of setting up a complex VPN network, it is ready to turn on and go: You have your own private Cloud. Those are some of the models that are out there.

When we talk about the legal ramifications of Cloud computing, the issues are often about chasing down the data, who owns the data, and where the data lives. Because security is paramount, there are a lot of questions around using Cloud computing. All of a sudden we have
gone from all data stored on premise to an off-site vendor, and even with the best security they are big targets. The reality is that the small law firm’s office network is probably less secure, and some of these big providers have a lot to lose if they get breached. When we hear about breaches we want to know what assurances for security you get when you contract with a Cloud provider. The reality is, though, they can tell you what they do, but they are not going to tell you too much because that puts them at a security risk. I was working with a company called Box. Fantastic product. They said “we’ll be happy to tell you about the security, but you need to sign a nondisclosure agreement first.” They did not want me to be able to talk about it outside.

There are numerous security and Cloud standards in development now. Soon, in theory, you can go to a Cloud provider, like Box, and look on their security page online and see where they show a seal of approval from somebody that gives you some kind of assurance that the provider is doing all the right things. Unfortunately, that standard does not exist right now. There are a lot of different standards in play, and they all mean slightly different things. If you ever go on a website for a Cloud provider and it says SAS 70 certified, walk away. That certification means nothing, it has been superseded—it was never a certification. Rather, it is an audit report from the American Institute of Certified Public Accountants. The current auditing report standard is SSAE16. But you still did not get to see the report, and it is really about physical security; for instance, the height of the bushes in front of the windows and building access security.

The standard that is farthest along is the ISO 27000 series for information security management. Additionally, NIST (National Institute on Standards and Technology) computer security division is developing standards. You probably heard of Truste and Thawte. Those certifications are more about the transfer of information or if you are sending over a credit card through a website or data transfer. And then you also got entities like the Cloud Security Alliance, which is probably the farthest along, but the companies looking for a STAR certification self-assess based on the standards checklist. In terms of standards, I hope that some day the ABA or some large group has the ability to help lawyers out by developing a seal of approval for Cloud providers that pass all the qualifications to be used by attorneys. Otherwise, attorneys should be asking a lot of questions and then crossing their fingers and hoping everything works out.

So rent versus owning. How many of you remember books? You still have a library, right? It’s full of books. I was a librarian. Back in the day, we bought books and we had stand-alone terminal access to
Lexis and West Law. That was cutting edge. We started subscribing to databases that could be accessed over the Internet instead of using loose-leaf periodicals. We accessed them on line, but you still had the books. Not so much anymore. We no longer need books. We are just going to subscribe to it online. But what happens when you quit subscribing? If you do not subscribe to Lexis, you lose access. You no longer own the content—it is gone. You no longer have access to it anymore. So they got you over a barrel to a certain extent.

When you look at these things like free services, DropBox is a premium product, where they give you something for free, and if you want more you have to pay for it. There is no such thing as a free lunch. And in the Cloud world, there is no free lunch because you are not paying for a product—you ARE the product. If you are not paying for the product, they are collecting data about you. They are aggregating it and selling it other companies. That is their business model. That is how they make money. They do not exist to be charities. They are making money, and then they eventually want to get you to pay for something. They do not care because either way they are making money by selling information about you and your behavior. If you learn that, it gets scarier and scarier as far as what they know about you.

So the other thing is that you should be looking at the terms of services for Cloud providers, especially for the free stuff. They may make claims that the data is theirs or they have rights to the data, like some of the photo sharing sites. Who owns the content? For example, who owned the copyright of the picture that Ellen DeGeneres took at the academy awards? Was it Bradley Cooper because he actually took the picture, or does Ellen hold the copyright because it was her phone? Or does Samsung own the copyright because it was their phone and they were letting her use it? I suggest you read the terms of service and think about the applications.

With Dropbox, they do not say they own your data, but they do not let you access your data after your account has been dormant for 90 days; however, they don’t necessarily delete it either. And if you read their terms, they say if you quit accessing the data or request to discontinue the service and you use the fee-based service then they will delete the data. The reason we care about that is because of considerations like subpoenas and the NSA and warrants served against the Cloud providers. Are they going to turn over your data, despite the fact that you deleted the account because you knew a subpoena was coming?
If you are working with a third party there is a lot of trust involved and this is not necessarily a new thing. People use companies like Iron Mountain to store their paper files. You look to brand names, but then some of the biggest brand names in Cloud computing have been hacked. The question is can we trust them. Do you trust Google? We are supposed to trust them. These companies are in the business of making money. So you have to think about what is their motivation. We are giving all of our data to these vendors, and you have to know enough about the vendor and how they are going to react to certain situations if they get served with a subpoena or if the NSA comes and says we want a back door or decryption code to your data.

Who has access to the files that are being stored? In some cases you find out the data is being encrypted in transit and storage, but certain people have access to the files in order to do normal maintenance. I usually tell lawyers to use a third-party encryption tool. That way you are the only one who has the encryption key and it no longer matters whether Dropbox has access to the files. There are many issues you need to think about when using third parties. Another one is what if the Cloud goes down? I just read an article about Twitter going down for 30 minutes. Is this a tragedy? According to Venture Beat it is because this is the way people are providing information that urgent. For example, there’s a twister coming in Kansas. The National Weather Service is tweeting this kind of stuff. But the Cloud does go down, and you have to think about how you are going to deal with it if it goes down or if the company goes away altogether and your data just disappears.

Other Cloud issues to consider include software as a service and organizations outsourcing to another company for data storage. You need to actually find out where the data is stored. Amazon and Rack Space will give you levels of storage. If you pay a little bit more you can have your data stored at the server farm in Maryland and a rollover to Indiana, and you can get three levels of failsafe so if one of their server farms goes down your service does not stop. It depends on the vendor you are working with, how much they pay the third-party provider, and whether they can continue to provide service. And then where is the data stored? It is much cheaper to store data in Malaysia than it is to store it in the United States. So many companies are offshoring the data in some situations.

Another issue is which laws apply. If the data is in Russia or China, what privacy laws do you have there and does that apply to your data? These are the kind of questions you need to ask—where is my stuff
and what laws apply to it? You have to follow the trail and make sure you know. The ABA Ethics 20/20 Commission was a group put together to look at how technology is affecting the rules of professional conduct, and they did a very good job and helped promote modifications to the Model Rules in 2012. One change was to the comments on Rule 1.6, the confidentiality rule regarding the reasonable care standard. In the past, reasonable care was never defined. Now, we have a definition of reasonable care. There is a five-point checklist, which includes sensitivity of information, the likelihood of disclosure without safeguards, the cost of additional safeguards, difficulty of implementing the safeguards, and the extent to which the safeguards affect lawyers in their ability to represent clients. So it does not have to be one-hundred percent secure. That has never been a requirement. You have files in a file cabinet. You cannot guarantee someone is not going to break in and get access.

The thing with using Cloud computing is the level of sensitivity of the information. If you have client files that have social security numbers and credit card information, that's considered personal identification (PI) under the data breach notification laws. And this is a scenario I do not know the answer to. Maybe the panelists can come up with a response. You as a law firm or a corporation that you are working with has a lot of PI and they are storing all their files in the Cloud. That Cloud vendor is breached. You get notification of it. Under Illinois data breach notification law, it only talks about on-premises storage. The law does not consider Cloud storage. And so if it is your data stored on a third-party server and you know that there has been a breach, do you have to notify your clients that there's been a breach? I think it is something that we have to consider. There are a lot of small firms that do have PI in their files; and of course businesses do, and it becomes even more important.