NYMITY

Toronto / Washington DC / Brussels
www.nymity.com

Privacy Interviews with Experts
July 2010

Tanya Forsheit
Partner
InformationLaw Group

David Navetta
Partner
InformationLaw Group

Lessons Being Learned about Cloud Computing

Nymity: What makes cloud computing different from computing in-house or normal IT outsourcing?

Forsheit / Navetta: This question gets asked a lot and can be a little misleading since at the end of the day cloud computing is simply the utilization of a particular technology infrastructure to outsource a business process. However, that technology infrastructure may magnify the challenges for organizations as compared to "traditional outsourcing." I will start with some of the increased challenges posed by cloud.

For example, as the name suggests, the location of data and processing activities may be harder to pin down when using cloud computing. Cloud providers often have data centers in countries all over the world. When talking about privacy and security laws, the location where particular data is stored, processed or transmitted can determine which countries' privacy laws apply. The country of residence of the data subjects also matters. For example, personal information put into a cloud data center in the U.S. or another country outside the EU or EEA could be problematic under the EU Data Protection Directive and require implementation of compliance mechanisms such as Safe Harbor certification, standard contractual clauses, and/or Binding Corporate Rules. Further, data from a Canadian or EU company that is stored or processed on a U.S. server may be accessible by the U.S. Government under the USA Patriot Act. The issue of geography, therefore, needs to be carefully considered before entering into the cloud.

Multi-cloud relationships and subcontractors are also an issue when using a cloud provider. The entity with whom a Customer is contracting may not be the entity that is ultimately storing, processing or transmitting the Customer's data. Many SaaS providers build their software in the clouds of other providers, who in turn may outsource processing to other providers, and so on. Some companies act as cloud service bundlers – pulling together multiple SaaS services together from different SaaS providers and providing a seamless package. An organization might have a contract with the bundler, but may actually be dealing with several other entities. This raises several thorny issues. As mentioned above, divergent privacy laws around the globe mean that a customer must determine which cloud subcontractor is doing the processing and where that processor's data centers are located. Further, a customer may have no or limited contractual rights against sub-providers several steps removed from the "up front provider." Contract rights obtained from the upfront cloud provider may be meaningless unless sub-providers are subject to similar contractual requirements. Managing and retrieving data may be difficult if the data is several steps removed from the original cloud provider. For example, if litigation is filed and e-discovery requests are made, a customer may not be able to adequately preserve and retrieve data stored by a sub-cloud provider. This problem is likely to get worse as we approach what some are calling the "InterCloud" – an interconnected group of clouds that allow data to flow between them like water with limited transparency.

Cloud is also different because computer servers may store and process data from multiple customers. One of the hallmarks of cloud computing is virtualization. Within a particular physical computer server, cloud providers can create multiple virtual computer servers (each with the same functionality as a traditional physical server). The end result is that the customer's data is on the same server as other customers of the cloud provider. This can be problematic. For example, if a cloud provider has suffered a security breach with respect to a particular physical server, the provider might not allow a Customer to conduct its own forensic investigation of the breach because that would allow the customer access to the data of the provider's other Customers. Another issue also relates to security. Security professionals have deduced that hackers may be able to hack into a customer's virtual server by having the cloud provider set up a virtual server for the hacker on the same physical server as the company.

Nymity: What are the key benefits?

Forsheit / Navetta: There are at least three key benefits to cloud. First and foremost is cost. The entire business model of cloud providers is to achieve huge economies of scale to provide processing power at a very low price. It is not difficult for companies and their IT departments to see significant cost savings by going into the cloud. Scale allows the unit price for processing to go down from the start. In addition companies can realize significant cost savings if they don't have to maintain a large IT staff, if they don't have to house, store and purchase the physical computing equipment, and if they don't have to constantly update their IT systems to keep up with the times.

Second, and somewhat related to the cost savings, under cloud you get the computing power you need, instantly when you need it, and you only pay for what you need (just like electricity). Under the old model, for companies that managed their IT internally it might be necessary to over-purchase computer resources to meet spikes in demand during the year. For example, many online retailers were forced to buy enough servers and computing power to address the shopping surge that happens during the holidays.

Another example that one company gave was their increased need for computing power when they were refreshing new content on their websites across the world (this only happened a few days a year yet they had to maintain a separate data center to address this temporary computing surge). In both cases, during the rest of the year they might only use 25% of their computing power and the rest would lay idle (but would still have to be maintained). All of that changes with the cloud. With the ability erect and take down virtual servers instantly, companies using the cloud can meet computing surges when they happen, and go back down to their normal computing needs during slower times. Thus, these companies no longer need to over-commit on IT to run their organizations. This results not only in increased efficiency for the company, but also significant cost savings because the company no longer needs to purchase or maintain unnecessary resources.

The third benefit is expertise and state-of-the art technology. Some cloud providers are experts at running data centers and doing data processing. In many cases they can do this job better and more efficiently than organizations can do on their own. In addition, some cloud providers provide state-of-the-art technology to their customers. Companies with legacy systems or software that is several versions behind can benefit by getting rid of their antiquated IT infrastructure and leveraging one that is current (and that is typically being updated on a regular and ongoing basis).

Nymity: What are the key risks?

Forsheit / Navetta: There are several key risks, some of them described above, including location of data, use of subcontractors to process data, and multi-tenancy. The overarching risk, however, is loss of control. Unlike processing in an internal environment, customers using the cloud have less ability to control their IT environment, and that means less control across-the-board, including in the event of a security breach. When managing IT internally, companies have more flexibility to make decisions as their needs change. When locking into a cloud environment, the Customer's ability to make changes may be limited. Moreover, when customers have their own IT they can put their interests first. That may not be the case in a cloud environment where a cloud provider will be looking out for its own interests, as well as those of the cloud provider's other customers. When running its own IT, a company is the number one priority. This may not be the case when working in the cloud. At the end of the day, the customer is the data owner. That means that, in the absence of contractual provisions to the contrary, the customer bears the risk of loss, damage, etc., even when it cedes control of all that personal data to the cloud provider. And most cloud providers resist imposition of liability for breaches and other incidents involve sensitive information of employees and customers. So the perceived cost benefits of the cloud described above could be illusory in the long-run.

Nymity: Should in-house lawyers and compliance, privacy and security officers be concerned?

Forsheit / Navetta: These in-house stakeholders should absolutely be aware of, and understand, the significant risks associated with cloud computing, particularly on the privacy and security front. They should work to put themselves in a position to weigh those risks against the benefits of cloud computing, and they should explore options that allow them to get into the cloud while minimizing their risk. This requires foresight and taking time to learn the issues and how they can be addressed. The concern these stakeholders should have is having a cloud transaction put in front of them for review without sufficient time or information to conduct due diligence and analyze the risks. Since the cost-savings associated with cloud are very significant, there is a risk that these stakeholders could be "steam-rolled" without a chance to adequately analyze and address the risks.

Nymity: Many of us think there is still time to plan for cloud computing and are not aware that our company is already doing some form of cloud computing. What do in-house lawyers and compliance, privacy and security officers look for to identify such activities? When did it happen and where did it happen?

Forsheit / Navetta: We have encountered clients that did not know they were in the cloud, and the problem likely stems from a lack of communication between key stakeholders. For example, IT professionals who put data into the cloud may not realize that allowing data to be stored in another country could trigger legal obligations. On the flipside, legal departments, privacy and compliance officers may not understand the nature of the cloud or be aware that a particular SaaS vendor actually stores and processes information on a third party cloud. Breaking down artificial divisions between the stakeholders is very important when it comes to cloud. Ultimately, to get started, key stakeholders need to meet and understand their company's cloud initiatives, and then design processes to allow them to address the relevant issues and concerns of each stakeholder. To make this happen there typically needs to be a "champion" who understands that overlapping issues and concerns exist, and who is able to pull together the right people to begin addressing the issues.

Nymity: How do we quickly understand the new risks and implement new controls to reduce these risks?

Forsheit / Navetta: There is no magic bullet when it comes to understanding cloud risks. We have outlined some broad categories here, but the risks will vary depending on the organization (and their risk tolerance) and the nature of the transaction. The most efficient way to analyze these risks is to create a process that involves the key stakeholders and provides time for each to analyze the issues that impact their world. Some of these issues can be "pre-identified" and hopefully the due diligence process can be streamlined and made repeatable. In terms of controlling the risks, much of that work will have to be done in the contracts that arise out of cloud relationships. As part of the overall process, organizations should develop clear strategies and template contract language for use in cloud transactions.

Nymity: What do we, as in-house lawyers and compliance, privacy and security officers, do to educate our executive management? Are there studies or papers that might help make it easier?

Forsheit / Navetta: While initially there was not a lot of talk about cloud coming from the legal side, that has changed. Firms like ours have begun focusing on these issue as they have the potential to dominate the IT outsourcing world for a very long time. There are webinars and blogs that are discussing these issues. There is a lot of activity on the privacy, security and legal side in social networking circles. Organizations like the American Bar Association's Information Security Committee and the Cloud Security

Alliance are putting together working groups to tackle these matters. In our own experience, clients and associations have frequently called on our firm to present a high-level overview or CLE on the privacy, security, e-discovery, and other legal compliance risks associated with cloud, and those overviews often lead to issue-spotting which, in turn, allows organizations to identify specific issues and plan next steps for vendor management, due diligence, and contract negotiation. You can find a lot of free information on our site, www.infolawgroup.com.

Nymity: What does it look like when a company does a great job selecting a cloud vendor? What do they do up front before beginning the due diligence process? What do they do during the due diligence and contract negotiation processes? What risks do they mitigate? What controls do they put into place?

Forsheit / Navetta: A company that takes the time to understand what different cloud providers have to offer and conducts its RFP process and due diligence in a deliberate fashion to address anticipated privacy and data security risks will be best situated to find a vendor that meets its needs – or determine that the risks outweigh the benefits for a particular application or purpose where highly sensitive information is involved. As we noted before, the first step is to bring all the stakeholders together-IT, Information Security, privacy, legal, compliance, and the relevant business leaders-and find out what they need, and what kind and level of risk they can tolerate. Then the company is well positioned to develop questionnaires (internal and vendor-facing) for the RFP process, and due diligence checklists to address privacy and security concerns. Some of this can also be done moving in the opposite direction, starting with internal discussions of template privacy and data security contractual provisions that can be designed to mitigate risk (e.g., indemnification), and coming up with positions that reflect the organization's risk appetite. That being said, it is almost always too late to make this process work – to carefully map the process and discussion based on an organization's internal security standards and privacy compliance requirements - once the vendor has been selected and the contract is into the negotiation process. In-house lawyers, privacy officers, and compliance personnel need to ask questions early and often.

Nymity: What are the important compliance, security and privacy elements that you recommend be placed into a contract today and why? What do you see changing in the future? If these items cannot be negotiated into a contract, what protections do you recommend instead?

Forsheit / Navetta: Wow, we could write chapters on that one, and have. We highly recommend that you check out our many articles on cloud computing, which can be found here http://www.infolawgroup.com/articles/cloud-computing-1/, and Tanya's recent article, "Contracting for Cloud Computing Services: Privacy and Data Security Considerations," available here: http://www.infolawgroup.com/uploads/file/PDF%20BNA%20Article.pdf. Some of the key contractual provisions include the following:

- Definitions, including the scope of information protected and the definition of "security";
- Preventative Contract Terms, including controls in place to prevent data breach, "reasonable security," and specific controls
- Audit and Enforcement Terms, including assessment/scanning rights, non-compliance reporting, and credits/damages
- Incident Response Contract Terms; and
- Risk of Loss Contract Terms

Unfortunately, if privacy and security risks cannot be addressed by contract, there may not be many alternatives. An organization will have to weigh the risks against the perceived benefits of going into the cloud. One figure that often comes up in these negotiations is the Ponemon Institute's most recent estimate that it costs an organization approximately $204 per compromised record in the event of a breach (not including the practically unquantifiable reputational cost associated with the a breach). It is not too difficult to multiply the number of customer and/or employee records that might be put in a cloud by $204 to come up with at least a partial (but not comprehensive) figure to evaluate the risk.

Nymity: This interview is named 'lessons being learned'. What more is yet to be discovered about computing in the cloud so that we can be confident that we will not only gain the benefit of lower costs and scalability, but also keep our information private and confidential?

Forsheit / Navetta: There is no such thing as perfect security on the Internet and there will never be perfect security in the cloud. We will probably never see the day when an organization can have 100% assurance that it can gain all the benefits of the cloud while keeping information private and confidential. It is, and always will be, a balancing act. But increased education, use of technology-based security solutions (e.g., strong encryption in appropriate circumstances, segregation of data, etc.), and thoughtful data mapping/inventories, RFPs, due diligence, and contract negotiation will all help ameliorate risk. An organization needs to determine what is compliant, "reasonable," legally defensible, and best for its employees and customers, working with all relevant stakeholders. Dave has written at length about this-see, for example, his piece on the Legal Defensibility Era, http://www.infolawgroup.com/2010/05/articles/legal-defensibility-1/the-legal-defensibility-era-is-upon-us/.

Nymity: In the meantime, once we have contracted for cloud computing services, what types of practical ongoing management and controls do you recommend we have in place? What is the company's responsibility?

Forsheit / Navetta: See discussion above, particularly with respect to contractual provisions addressing audit and enforcement terms.

Nymity: What other laws and legal activity become more complicated because our company information is in the cloud?

Forsheit / Navetta: There are innumerable laws that could be implicated by putting data in the cloud. One big area of concern outside of privacy and data security is e-discovery. There are numerous considerations to take into account in the contract negotiation process and once a company is in litigation (records retention policies, litigation holds, Rule 26 conference, discovery requests, etc.) For an extensive discussion, see my article on the cloud and e-discovery here:

http://www.infolawgroup.com/2009/11/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-four-ediscovery-and-digital-evidence/

Nymity: In closing, what additional suggestions do you have for in-house lawyers and compliance, security and privacy officers and the rest of the business and technical entities involved in the procurement processes that include cloud computing?

Forsheit / Navetta: Every cloud deal is unique, sui generis. In-house lawyers and compliance, security and privacy officers should treat them that way. Nonetheless, organizations can pre-develop processes and approaches that help them analyze the risks of each cloud transaction in a streamlined fashion. This process should allow the company to identify the information to be put in the cloud, identify and measure the risks against the organization's risk appetite, and explore the kinds of protection the company needs. This process should flow into the contract requisition phase (as early as possible to create bargaining power), and the development and negotiation of contract terms to protect the organization.

Within an organization, if you anticipate that cloud computing is going to impact you world, become the cloud expert in your organization. Read up on the technology and the pros and cons of particular services and vendors-there is tons of material out there and resources such as the ABA, the CSA, and contract procurement organizations. Create a cloud team-including IT, IS, privacy, legal, compliance, and business reps. Meet early and often, long before you start meeting potential vendors. Plan ahead, way ahead. Conduct careful RFPs, do your due diligence, and read the contracts carefully.