LAYERED CLOUDS: LOOMING ISSUES FOR LAWYERS FROM SUB-CLOUDING BY CLOUD COMPUTING PROVIDERS

Date: 06 July 2011

Author: Shannon Brown, Esq.

As cloud computing continues to pose new challenges for the legal community, an non-obvious complexity may arise when Cloud Provider A sources (or to coin a term, "sub-clouds") services from another cloud provider (Cloud Provider B). Issues with Cloud Provider B may cascade upwards and affect Cloud Provider A and Cloud Provider A's subscribers. This emerging phenomena results in "layered clouds" and may involve a number of layers.

As the recent Pennsylvania Informal Ethics Opinion (Inquiry 2010-60, January 10, 2011) addressing cloud computing suggests, while the Pennsylvania Rules of Professional Conduct (Rules) do not preclude cloud use by lawyers, use of the cloud is nevertheless conditional—predicated on the lawyer "making reasonable efforts" to, among other things, protect client confidentiality. The looming cascading issues arising from sub-clouding and layered clouds add yet another dimension to evaluating the reasonableness of cloud computing use by law firms.

Understanding Cloud Computing Types: IaaS, PaaS, STaaS, and SaaS

To understand the issue, one must understand the basic types of cloud services. While definitions of cloud types continue to evolve, four primary categories now exist. Briefly, Storage-as-a-Service (STaaS) and Software-as-a-Service (SaaS) are high-level cloud types. Think of these services as complete computer applications, already assembled, and requiring minimal (if any) configuration. These high-level services often mimic desktop software applications.

In contrast, Infrastructure-as-a-Service (IaaS) is a low-level cloud type and is usually confined to physical hardware (servers, routers, storage), server software, and internet connectivity. Think of IaaS as a bare bones virtual server—you get basic hardware, basic functionality, perhaps some systems management, but not much else.

Finally, Platform-as-a-Service (PaaS) exists in between STaaS/SaaS and IaaS. PaaS usually involves a set of application development tools (APIs, modules, or software components) that the end-user configures (or more likely has a software development team configure) for the end-user's specific needs. Think of PaaS as a kit approach or a TinkerToy model. You must assemble the kit to meet your needs or otherwise you just have unusable software pieces.

Thus, the cloud services in order of functional complexity are:

1. SaaS/STaaS

2. PaaS, and
3. IaaS.

Understanding Cloud Layers and Sub-clouding

In the simplest cases, an entity subscribes to a cloud service of some type where the cloud provider controls and delivers all the basic services to the cloud subscriber. A one-to-one relationship exists between the subscriber and the provider. Most people assume that all cloud models operate in this manner.

In more complex cases, however, the cloud provider may sub-cloud (sub-lease or sub-contract) services from another cloud provider lower on the ladder. For example, Lawyer Linda contracts with SaaS cloud provider SaassySoftwareStuff.com for basic word processing cloud services. Simply, Linda contracts with Saassy. But, unknown or not evident to Linda, the SasssySoftwareStuff application is actually built with tools provided by a PaaS provider named PaassablePlatformPieces. But, Saassy has a contract with with PaassablePlatformPieces to use Paassable's software components to build the Saassy application. SaassySoftwareStuff is thus a layered cloud. The top layer is the software that Linda receives. The second layer arises from Saassy assembling Paassable's software components. Unless Linda carefully inquires, Linda may be unaware of the Saassy-Paassable relationship.

The issue can get even more complex. Paassable may sub-cloud its servers and infrastructure from an IaaS cloud provider named InertIaaS. This creates yet another layer. Again, Linda may be unaware of the Paassable-InertIaaS relationship and unaware of this additional risk.

In summary, from Linda's perspective, there may be two or three cloud layers involved in the delivery of her cloud-based word processing application:

SaassySoftwareStuff,
PaassablePlatformPieces, and
InertIaaS.

Problems with any one of the layers may cascade up or down to affect the other layers. The permutations of cascading are complex, but an illustration demonstrates the implications of cascading in layered clouds.

Cascading Issues in Layered Cloud Computing

For Linda as a lawyer, Linda must assure that the use of the cloud service, at minimum, reasonably protects client confidential information. Assume in this scenario that Linda composes and stores client documents (including confidential information) in her SaassySoftwareStuff account. Hackers breach security at InertIaaS and are able to access all information in Linda's SaassySoftwareStuff account.

Did Linda check the security and privacy policies of all three layers—SaassySoftwareStuff,

PaassablePlatformPieces, and InertIaaS? Perhaps more important, does Linda even know about PaassablePlatformPieces and InertIaaS? What happens when a data breach occurs at InertIaaS—will Linda, as a lawyer, receive notice about such a breach so she can comply with her obligations? Where is InertIaaS located, and what data breach reporting requirements, if any, apply in that jurisdiction? Were the security measures employed by all cloud providers involved adequate? If not, is the inadequacy fairly imputed to Linda?

In this scenario, not only might there be Rule 1.1 (Competence) and Rule 1.6 (Confidentiality) ethics issues related to the reasonableness condition (see Informal Ethics Opinion 2010-60), but there might also be an ethics issue related to Rule 1.15 (Client Property) if Pennsylvania Formal Ethics Opinion 2007-100 (2007) holds—implying that electronic client documents may be client property and thus potentially subject to Rule 1.15 duties.

Pennsylvania also has a data breach reporting act (73 P.S. §§ 2301, *et seq.*) that may impose additional statutory obligations on the lawyer arising from a breach. Thus, failure to report the breach might trigger both statutory penalties and additional ethical problems arising from the failure to report as potentially required by law.

As the simple illustration shows, the permutations are complex, responsibilities evolving, and consequences potentially severe. The questions posed above, thus, should be asked before the breach occurs, not after. Unfortunately, this is but one example of the complex issues that may arise (privity, contract, remedies, pan-jurisdictional issues, negligence, malpractice, and conflict of laws immediately come to mind).

Conclusion: Peeling Back the Layers

Layered clouds and the cascading issues directly stemming from layered cloud computing loom on the near horizon. As the incidence of lawyer adoption of cloud computing increases, presumably so will the incidence and implications of layered cloud issues. Lawyers, thus, should carefully assess not only their direct, cloud provider's services but should also carefully inquire into any sub-clouding issues. As suggested above, sub-clouding might not be readily apparent. The lesson: really know your cloud provider (or providers) before launching into the cloud.

END OF ARTICLE