# Fred Cohen & Associates - Analyst Report and Newsletter

***Welcome to our Analyst Report and Newsletter***

## Culture clash: Cloud computing and digital forensics

Cloud computing is getting a great deal of attention these days, and there are a lot of good reasons to move into the clouds for a lot of people. Whether it's; .mac users who use Apple for their email, Web services, file sharing, and so forth; Google for gmail, advertisements, searches, and storage; or any of the other companies that provide services for free or fee, there is a lot to be said for the economy of scale when you don't really need integrity, availability, confidentiality, use control, or accountability. But what happens when you do?

### Legal requirements for digital forensic evidence

At the opposite end of the spectrum is the legal system. In the legal system, there are some mandatory standards that must be met in order for digital forensic evidence, or any other evidence, to be presented in court. These include, without limit, requirements on evidence, people who present evidence in a legal setting, the tools used with respect to the evidence, and how the evidence is handled throughout its life cycle. Requirements also extend to records retention and disposition processes, confidentiality issues associated with trade secrets, witness protection, and other sorts of protective orders, orders for destruction or return of evidence and work product, attorney client privilege and other sorts of privileges, and chain of custody. Without going into details of each of these, at a minimum, it must be recognized that controls and people who can testify as to those controls over specific items of evidence, processes undertaken, methodologies, and tools used are mandatory for the legal system.

### Properties of cloud computing today

Various people have investigated cloud computing for its security properties, and while the specifics vary greatly, one thing all of their reports have in common is this:

- When the report is from a cloud computing company, everything is safe and secure;
- When the report is from independent security experts, nothing is safe or secure.

From where we see it today, cloud computing has some tremendous advantages, and these advantages should be leveraged wherever possible. But what is lacking today, is a cloud computing company that can authoritatively meet the serious protection requirements of the legal system, the financial system, or any other system that is important to the well being of society.

### Some details of the culture clash

For those who are stuck on things like facts, they are few and far between when it comes to open source information on security problems with cloud computing. So here are some of the facts as we have come to believe them, without any attribution or basis other than our word on it. Nothing here would be admissible in court, since it's all hearsay.

Attacks and exploitation within the clouds:

 

- Within existing cloud computing systems, malicious actors use the same sorts of methods they use in the Internet in general, and infiltrate computers, gaining control over them.
- With these capabilities, they carry out further attacks, within the clouds, between clouds, and between the cloud and the rest of the Internet to extend their reach and improve their relative anonymity.
- With these capabilities, they directly access content and programs both within the virtual computing environment, including those used on the computers that they reside on within the clouds, and in the hardware environment that they reside on.
- With these capabilities, they leak information, corrupt information, destroy information, perpetrate frauds, sell stolen information, extort monies from victims, sell illegal goods and services, illegally sell legal goods and services, operate illegal and legal businesses, and resell services to others.

In addition to the malicious actors in the cloud computing environment, the providers of cloud computing capabilities are using the large distributed networks they create and support to reduce costs through economies of scale. Depending on the needs of their clients, they may trade a great deal to keep costs low. For example, Google literally throws out computers when they fail rather than trying to fix them. They don't try to recover the data, the simply lose it and live without it. It is their normal business model for much of the data they hold.

Where is the computing done and where is the data stored? It's in the cloud, and for the most part, the cloud computing crowd does not know or care where the data is or where the computing is done. This is completely reasonable for most cloud computing cases, and it keeps costs lower if you don't have to track everything that happens. If you want to investigate an incident in the cloud, you can count on few if any records to support your activities, and the cloud computing companies are unlikely to be more supportive than to answer legal subpoenas with the minimal information they need to provide. Why would any rational company do anything else? They wouldn't and they don't!

But what makes for a great business model for many purposes, makes a completely unworkable business model for the legal system. The inability to meet the mandates of the legal system is an enormous problem for those who want to leverage the low costs of the cloud computing model. But today, there is no cloud computing capability that combines the economies of scale of the clouds with the surety requirements of the legal system. And think about it. Would you really want your life or fortune to depend on the outcome of a Google search? And who could testify about how the trade secret document that was originally provided to the cloud went from computer to computer, disk to disk, and country to country, who had access, how they handled it, where it went, how it was properly destroyed at each site as it was moved to the next one, and how it's integrity was maintained in the process? When you run a forensic analysis, how are you going to prove that it was correct and repeatable, when you can't even tell me what operating system and software was doing the analysis?

**Forensics and the cloud computing model**

There is hope for cloud computing in the forensics arena, but it won't likely look like the cloud

 

computing of today, and it won't gain from the economy of scale in the same way as other sorts of cloud computing. It won't likely be an advertising model, at least not one where the forensics is free, but you have to watch advertisements when you do your examination. And "low cost" is a relative term. Digital forensic evidence examiners start in the $250/hour range and go to twice that much if you want real expertise. What then can you expect from digital forensics in the cloud?

- You can expect that rather than storing the data associated with legal holds inside the company, it will be imaged to a trusted and properly controlled cloud computing facility that has as good or better; physical controls, chain of custody controls and records, document control mechanisms, record retention and disposition policies and processes, personnel with proper credentials, and backup and recovery capabilities
- You can expect that the cloud digital forensics provider will also provide testifying experts who have been qualified to courts of competent jurisdiction for their knowledge in controls over forensic data, and who can testify as experts about all aspects of how the relevant materials were identified, collected, preserved, transported, stored, processed, and destroyed in all of the relevant jurisdictions.
- You can expect that they will provide interfaces to allow authorized individuals, on a read-only basis, and with suitable controls, to work with forensically sound copies of the digital forensic evidence from locations convenient to them and at times convenient to them, in keeping with the mandates of the legal system, including all of the requirements surrounding court orders and other related requirements.
- You can expect that they will provide fully licensed copies of the tools you use and the tools that others use, provide the means to do specialized tests and analysis, provide redundant tests and analysis with independent mechanisms, provide the means to create customized programmed analytical methods, and support all of these methods with experts who do development, testing, and certification processes associated with all of these tools and techniques.
- You can expect that this will be a nationally recognized, fully accredited digital forensic laboratory, with certified background checked workers who are qualified and current in all of the areas of expertise where they do work.

The value they will bring will not be in the low cost of their service, but rather, in the high quality of their work, and the certainty that they provide to support the legal issues in the case. While saving costs in legal matters is certainly desirable, consider that in law suits where hundreds of millions of dollars have been at stake, process errors have resulted in tens of millions of dollars in sanctions and fines, and adverse instructions to juries.

If cloud computing and digital forensics will one day meet, it will be because the digital forensics cloud has better and more reliable integrity, availability, confidentiality, use control, accountability, and quality. The economy of scale will be from the expertise of the cloud provider, and the high cost of having that expertise in each party to each case.

 