Law & Forensics

E-Discovery, Forensics, Cyber Security, and Cyber Warfare ™

By Daniel Garrie

INTRODUCTION: CLOUD COMPUTING

Cloud computing is a general term for the delivery of hosting and other services over the Internet. Instead of storing data in-house, the data and data applications are stored remotely, with access to the data provided via the Internet (the "cloud" in "cloud computing"). Whatever the specific form, the singular characteristic of cloud computing is separation of the computer hardware from the service. The major advantage of a cloud computing solution is its elasticity – the consumer is charged by use, can make as little or as much use of the service as desired, and need not purchase, maintain, or upgrade any computer hardware. Once data is hosted in the cloud, all the consumer needs is a personal computer and access to the Internet.

Several aspects of cloud computing significantly impact electronic discovery. Accordingly, these issues must be known and understood by both client and counsel before e-discovery commences. Indeed, these issues ideally should be considered by the client in deciding whether "cloud computing" is an appropriate choice for the company.

FIVE WAYS CLOUD COMPUTING COMPLICATES EDISCOVERY

The Physical Location of Data

While "cloud' references provide a useful metaphorical tool, in reality the data still sits on a server somewhere. Care should be taken to ensure that this physical location, and the electronic security protecting the data residing on the server, is appropriate and sufficiently robust. One aspect of turning hosting duties over to a third-party is that you lose control over these security and data protection issues, as some or all of those security and protection duties devolve to the hosting company. Not all "clouds" are the same, and you should make sure you understand the security parameters and limitations of your particular cloud. Likewise, if you are storing data in a cloud as part of a complex and sensitive litigation, it is critical that counsel understands who else is storing data in the cloud, and learns how the system is designed to ensure that the risk of commingling or unauthorized access to the data is negligible. Often, there are economies of scale in having all electronic discovery from all parties in a lawsuit hosted on the same cloud, and accessed by a single service provider. But

these benefits will rarely outweigh a security breach that leads to the loss of, or the unintended sharing and commingling of, information. Here, counsel might consider retaining an independent technologist to review and assess the cloud's security protocols and systems to ensure that they are not unnecessarily placing the client's data at risk.

The Data May Be Stores in a Different Format

The information that sits in the cloud is not all necessary searchable. It is possible that data sits in the cloud, but that the cloud lacks the necessary search component required to search and retrieve that data. For example, the information may be stored in a unique format proprietary to the client that is not recognized by the cloud. This in turn means that a client may find it impossible to readily access that information. It also means that, when counsel seeks to effectuate a production and collect responsive information during litigation, the resulting data set will not include any information from those files, possibly without counsel being aware that certain data exists that has not been searched and collected. Therefore, it is imperative that, before counsel works with cloud based systems, they make the inquiries necessary to establish the format(s) of the data stored in the cloud and confirm that all the data in the cloud can be searched and produced.

The Host is a Company like Any Other, with the Same Pitfalls

While cloud computing presents a compelling business value proposition, it is recommend that prior to adopting such cloud based technology, a company consider cloud evaporation scenarios and how they might impact the company and any pending litigations. Here, for example, are three unanticipated cloud evaporation scenarios which frequently occur: (1) your cloud is acquired by a competitor and you need to migrate the data in the cloud out of the cloud to another cloud or internal system; (2) the cloud goes bankrupt causing the cloud to evaporate and with it your data, if you don't migrate it out or, if possible, purchase the machines in the cloud; (3) the cloud provider has a security breach and the data stored in the cloud is compromised requiring either migration to a new cloud or system and an information audit. In all three "evaporation" scenarios, companies are suddenly required to make quick and likely expensive decisions with potentially far-reaching consequences for the security of their data. In addition, all three scenarios invite potential challenges to chain of custody, particularly in the event of a security breach. Considering these

and other evaporation scenarios now, rather than in the heat of the moment, will help prevent such events from wreaking havoc on the company and any attendant litigations.

Exposure of Data

Cloud based systems present novel privilege issues. All privileges are founded on restricted access. Should privileged information be shared with a third-party, the privilege vanishes. Usually, privilege is readily maintained because a company's sensitive information remains in-house in the company, until it is shared with outside counsel to whom the privilege still applies as part of the litigation. Cloud computing, however, necessarily involves migrating data outside the company and to a third-party host. Quite apart from any catastrophic breach in the cloud, it is likely that the specific elements of privilege, and the importance of maintaining that privilege, will not be as understood or appreciated by those that manage the cloud infrastructure on your behalf. Extra care must be taken to ensure that that the data managed is not accidentally accessed by a third-party or by a system administrator accessing privileged data in the context of resolving a technology issue.

Hidden Costs

Cloud based computing represents an attractive value proposition, but look for hidden costs that might arise as a result of the size of the data set, the difficulty of retrieval, or the need to repeatedly access and manipulate the data hosted on the cloud. It may make sense to migrate only a portion of a company's data to a cloud based computing system, while retaining in-house control over other areas of information.

CONCLUSION

Before adopting or deploying cloud based solutions for your enterprise, or for a specific litigation matter, client and counsel should carefully evaluate these six issues, including comprehensive conversations with the IT, business and legal units. Otherwise, the company and the firm may be exposed to unanticipated and unnecessary risks and costs.

About Law and Forensics:

Law and Forensics solves the complex legal issues at the convergence of technology and the law. Our team includes some of the foremost thought leaders in eDiscovery and electronic forensics as well as the pioneers in the latest techniques in cyber security. It is this expertise which allows us to solve information governance problems efficiently and cost effectively.

We work with our clients, whether law firms, corporate organizations or government agencies, to resolve eDiscovery issues, perform electronic forensic examinations and investigations, and help bridge information and communication gaps between technologists and legal professionals.

Law and Forensics is based in Seattle with additional offices in Atlanta, Delaware, Los Angeles, and New York.

6506 3rd Ave. NW, Suite C
Seattle, WA 98117

T: 425.395.4092

F: 866.893.4785

E: info@lawandforensics.com

W: http://lawandforensics.com