Chapter 97
Compliance in the Cloud and the Implications on Electronic Discovery

Dean Gonsowski
Symantec Corporation, USA

ABSTRACT

Cloud Computing will be a disruptive technology that will ultimately change the face of computing with a market approaching $300 billion over the next five years, according to recent study from the Market Intel Group (Mathews, 2010). The unstoppable migration of data to the Cloud is undoubtedly due to numerous financial benefits, particularly for small and medium-sized companies, which historically do not have the same capital budgets as larger enterprises. However, this boundless upside is not without risks from a legal and compliance perspective, making it all that more important for entities to look before they leap. Today, nearly every corporation is required to preserve and produce Electronically Stored Information (ESI), such as emails and other electronic documents, as part of their response to litigation, regulatory inquiries, and subpoenas. When the subject ESI happens to be stored in the Cloud, there are a handful of potential obstacles that serve to complicate the eDiscovery process. For some, this leads to sanctions and increased compliance risks. In order to navigate these potentially treacherous waters, organizations need to be proactive and follow a "measure twice, cut once" approach. This chapter will discuss the basics of eDiscovery and explore ways to minimize potential compliance hurdles when migrating significant data stores to/from the Cloud.

BACKGROUND

Navigating the complex issues surrounding eDiscovery in a cloud environment requires, at a minimum, incorporating both legal and technical viewpoints, while also considering related corporate functions such as information security, records management, risk, and compliance. Once these constituents are brought into the fold the groups must inherently consult applicable regulations, emerging case law and industry best practices. To this end, standards bodies like the EDRM and Sedona Conference Working Group on Electronic Document Retention and Production

DOI: 10.4018/978-1-4666-6539-2.ch097

will be referenced to augment relevant case law and statutes such as the Federal Rules of Civil Procedure (FRCP).

The goal of this chapter is not to delve into basic cloud characteristics (e.g., on-demand, self-service, broad network access, resource pooling, or rapid elasticity) or delivery models (e.g., Software-as-a-Service, Platform-as-a-Service, or Infrastructure-as-a-Service). The various deployment models (private, public, hybrid, etc.) will be discussed with a particular focus on public clouds since private cloud environments tend to look very similar to on-premise IT environments. Finally, specific tools, techniques, and methodologies will not be discussed in this chapter since most applicable case law and regulations do not articulate set standards or deployment methods. Instead, the focus will be on the strategic considerations, as well as any risks attendant with conducting alternative approaches.1

eDISCOVERY IN THE CLOUD

It's All the Same, Just Different

Computer forensic experts, judges, lawyers, and eDiscovery practitioners alike are all facing the next big challenge when dealing with ESI. On one level, the new cloud infrastructure seems to hold a dizzying array of both promise and risks. On the other hand, some will argue that the cloud paradigm really does not change anything at all. In the end, both opinions are somewhat correct: eDiscovery and regulatory compliance issues are all fundamentally the same, but the cloud medium does threaten to pose a range of tactical and strategic challenges.

There is an issue that's looming that hasn't really been discussed or addressed yet. That is the role of governance for companies that are consuming the services versus the role of governance for companies that are providing the services. – Joe McKendrick, Independent Analyst and ZDNet Blogger (Gardner, 2009)

Before diving right into the details surrounding cloud computing and the associated electronic challenges, it is worthwhile to examine where this relatively new discipline fits into the larger information governance infrastructure, as a discipline. While many of these definitions are still evolving, Gartner proffers the following definition regarding information governance:

Information governance is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals (Gartner, 2009).

Similarly, the EDRM organization has attempted to abstract upwards to include notions of governance into their newly promulgated Information Governance Reference Model (IGRM) as shown in Figure 1, which purports to tie various legal duties to the underlying data assets (EDRM, 2011). The purpose is not to conduct a deep dive surrounding the IGRM but to show electronic discovery's place in the larger landscape.

Regardless of which larger information governance umbrella is selected, there are a wide range of applicable Records and Information Management (RIM) regimes that may apply to a given organization, depending on size, location, vertical orientation, and regulatory posture. These RIM imperatives include SEC Rule 17a-4, FINRA, Sarbanes-Oxley, HIPAA/HITECH, EU Data Protection Act, Stored Communications Act, State Privacy Protection Laws, Gramm-Leach-Bliley Act, Safe Harbor Rules, Dodd-Frank, etc. Beyond the above list there may ultimately be thousands of discrete mandates (at the local, state, and federal level) that govern how ESI must be retained and