B26 Legal Processes for Cloud Forensic Investigations

Aaron Alva, William H. Gates Hall, Box 353020, Seattle, WA 98195; and Ivan Orton, JD**

After attending this presentation, attendees will gain an understanding of the legal challenges involved in cloud computing investigations and the potential legal processes that may be used to demonstrate the admissibility of cloud-based forensic evidence.

This presentation will impact the forensic science community by providing a legal perspective on the emerging area of cloud forensics. Attendees will learn what steps may be necessary to authenticate potential forensic evidence from public cloud computing providers for criminal or civil investigations.

Organizations have continued to adopt cloud computing as a cost-effective processing and storage platform. As the cloud's prevalence increases, it will have an increasing impact in legal proceedings. Once cloud-based data is obtained, it is minimally useful unless it is accepted as evidence in a case. The Federal Rules of Evidence (or similar applicable rules) were originally designed for paper documents, and updates to address digital evidence have yet to consider the cloud's different paradigm. Unlike traditional hard drive forensics, forensics involving cloud computing does not include the ability retain a physical, original hard drive. The lack of original, physical-based forensic evidence presents admissibility and authenticity concerns.

Authenticity concerns are the main barrier for the use of cloud-based data in legal proceedings.[1] Cloud-based data that is obtained from a public cloud is, by definition, physically comingled. When challenged in legal proceedings, a party must be able to demonstrate that the data produced is associated with a particular user. While this may be established through methods including testimony of a witness with knowledge, additional concerns arise when the admissibility challenge is targeted toward the actual processes and functions of the cloud computing environment. When the actual process for obtaining cloud-based evidence from a particular cloud user is challenged, a party may be required to prove the reliability of the underlying cloud computing process or system. This may require expert witness testimony from the cloud provider.

A walkthrough will be provided of the applicable rules of evidence that may apply to cloud-based forensic data. The potential processes for admitting and authenticating cloud-based evidence into a case will be explained. These potential processes have been modeled to address the particular unique issues of cloud-based evidence. Other hurdles that may arise when authenticating cloud-based evidence including the Daubert test for digital evidence will be discussed.

In conclusion, the nature of cloud-based forensic evidence requires new applications of legal processes. This presentation will provide the legal and digital forensic communities with a fundamental understanding of such processes, and potential challenges for the use of cloud based data.

Reference:

1. See I. Orton, A. Alva, and B. Endicott-Popovsky, "Legal Process and Requirements for Cloud Forensic Investigations," Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, 2013, pp.186-235; http://ssrn.com/abstract=2197978

Cloud Computing, Digital Forensics, Legal Processes

** Presenting Author*