## E27 Search Warrant Language for Cloud Computing

*Josiah Dykstra, MS*, Univ of MD - Baltimore County, Baltimore, MD 21144*

After attending this presentation, attendees will be able to understand and create search warrants for data in cloud-computing environments. Attendees also will be able to enumerate potential challenges facing the production of cloud-based evidence.

This presentation will impact the forensic science community by arming the legal and digital forensic communities with language for cloud-specific search warrants, an example warrant based on a case study, and a list of potentially relevant cloud-based forensic artifacts.

Cases involving evidence from cloud computing environments will soon dominate criminal and civil litigation and the legal community must be armed with the knowledge about how to execute e-discovery of cloud evidence. Companies are embracing cloud technology to offload some of the cost, upkeep, and growth of equipment that they would otherwise have purchased themselves. The general public is increasingly storing their data in clouds, sometimes unknowingly. Cloud infrastructure – with exceptional bandwidth, storage, and computing power – offers an attractive prize for hackers. Where the people, the data, and the money go, so too does crime. While many people have lamented how the users of the cloud and their data are protected, few of these discussions have considered the difficulty of responding to security breaches, including forensics and criminal prosecution.

This presentation gives the first public discussion of search warrant language that could be used to compel cloud-based data from a cloud provider. Law enforcement and legal professionals may be unfamiliar with this new technology, and therefore unsure what electronic evidence may exist and what to seize in a warrant. Many audience members will be familiar with e-discovery of online webmail and social media, but cloud computing differs in important ways that make acquisition of data different. This presentation will rely on technical expertise of cloud computing to suggest possible language for use in a search warrant. In particular, friendly definitions of technical cloud terms, and a list of potentially relevant data to ask for in a warrant will be presented. This work builds on discussions with cloud providers about the forensic data they collect, and incorporates prior work from legal scholars about the legal challenges associated with cloud-based data.

A hypothetical case study of child pornography being hosted in the cloud will be used to illustrate suggested wording and phrases to use in a search warrant. While fictional, it describes a common computer crime where the cloud is an accessory to a crime. This sample language is useful for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of data from cloud computing environments. In particular, this example is tailored to Amazon Web Services, the largest and most popular public cloud service provider.

Following the discussion of warrant language, several potential shortcomings of cloud-based e-discovery in general will be enumerated. The defense could use the deficiencies identified to challenge and discredit the process and product of cloud-based evidence. Such issues include the untrustworthiness of cloud data, extreme complexity of the cloud environment, and likely failure of the *Daubert* test.

Now is an exciting time for cloud computing as innovative new product offerings emerge. The legal community is also at the threshold of a wave of cloud-related litigation. The first public cases involving cloud-based ESI are likely to appear soon, and the people involved in those cases have a unique opportunity to set new legal precedent. This exploration of seizing electronic evidence from cloud computing provides a foundation to forensic investigators and legal professionals as they investigate and prosecute cloud-based crimes.

**Cloud Computing, Digital Forensics, E-Discovery**

 ** Presenting Author*