Chapter 95
Seizing Electronic Evidence from Cloud Computing Environments

Josiah Dykstra
University of Maryland, Baltimore County, USA

ABSTRACT

Despite a growing adoption of cloud computing, law enforcement and the judicial system are unprepared to prosecute cloud-based crimes. This chapter illuminates legal problems in the United States for electronic discovery and digital forensics arising from cloud computing and argues that cloud computing challenges the process and product of electronic discovery. The researchers investigate how to obtain forensic evidence from cloud computing using the legal process by surveying the existing statues and recent cases applicable to cloud forensics. A hypothetical case study of child pornography being hosted in the Cloud illustrates the difficulty in acquiring evidence for cloud-related crimes. For the first time, a sample search warrant is presented that could be used in this case study, and which provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of data from cloud computing environments. The chapter concludes by taking a contrasting view and discusses how defense attorneys might be able to challenge cloud-derived evidence in court.

INTRODUCTION

Crime committed using cloud computing resources and against cloud infrastructures is inevitable. In early 2011, Sony was the victim of an online data breach that took down the PlayStation Network. In a widely cited report, Bloomberg News reported that the intruder used Amazon's public cloud to commit the crime (Galante, Kharif, & Alpeyev, 2011). The report also stated that the FBI was investigating the crime, but that neither Amazon nor the FBI would comment on whether the former had been served a search warrant or subpoena. No further information about the case has been made public. This is the first public case of a cloud-related crime, though many more are bound to emerge soon.

Companies are embracing cloud technology to offload some of the cost, upkeep, and growth of equipment that they would otherwise have purchased themselves. Cloud infrastructure offers an attractive prize for hackers, with exceptional

DOI: 10.4018/978-1-4666-6539-2.ch095

bandwidth, storage, and computing power, and a consolidated repository of data. While many people have lamented how users of the cloud and their data are protected, few of these discussions have considered the difficulty of responding to and prosecuting security breaches, including forensics and criminal prosecution.

Cloud computing introduces new and significant challenges in prosecuting cloud-based crimes that differ from traditional electronic evidence and electronic crime. The very attributes that make cloud computing attractive can be at odds with forensic and legal goals. For example, the cloud offers location independence so that data are available from anywhere, even though location may determine jurisdiction. Another example is the rapid self-creation and destruction of cloud resources, a powerful feature for customers, but a severe challenge for evidence preservation.

This chapter discusses the legal seizure of data from cloud computing related to the prosecution of cloud-based crimes. We explore the legal problems in the United States for electronic discovery and digital forensics arising from cloud computing as an infrastructure service and explain how cloud computing challenges the process and product of electronic discovery. We investigate how one might obtain forensic evidence from cloud computing using legal process by surveying the existing statues and recent cases applicable to cloud forensics. While this is not legal advice, we approach the problem from a computer science perspective and with a background in digital forensics. This technical perspective is intended to inform forensic practitioners about legal problems, and aid legal practitioners with prosecuting cloud crimes.

We use a hypothetical case study of child pornography being hosted in the Cloud to illustrate the difficulty in acquiring evidence for cloud-related crimes. While fictional, it describes a common computer crime where the cloud is an accessory to a crime. For the first time we present a sample search warrant affidavit that could be used in this case study. This provides an example and sample language for agents and prosecutors who will soon need to obtain a warrant authorizing the search and seizure of data from cloud computing environments.

We conclude by discussing how defense attorneys might be able to challenge cloud-derived evidence in court. It is important for both prosecution and defense to understand how cloud evidence may be challenged in court today. Some of these issues include complexity of the environment and lack of jury comprehension, the failure of cloud forensic evidence against the *Daubert* test, and changing attitudes of the US Supreme Court regarding privacy.

BACKGROUND

Before looking at the laws affecting the process of seizing evidence of cloud evidence, we provide some context and background about cloud computing, digital forensics, and the law.

Cloud Computing

Let us being by defining the scope of our discussion. It would be easy to let a discussion on cloud computing grow to encompass all Internet-enabled services as "cloud computing." There are good reasons for discussing forensic investigations of Facebook and Twitter specifically because those services are involved in many cases, but we will take a more formal definition. One often-cited definition of cloud computing comes from the National Institute of Standards and Technology (NIST) (Mell & Grance, 2011), which reads in part:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.