Chapter 7
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

DOI: 10.4018/978-1-4666-2662-1.ch007

of equipment that they would otherwise have purchased themselves. Cloud infrastructure offers an attractive prize for hackers, with exceptional 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.*

"Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. Telephone networks and the Internet are examples of Clouds. Cloud computing, however, is concerned with providing customers with raw remote computing resources such as computation or data storage, and the ability to provision those resources themselves.

There are many providers of cloud services, and even those that provide similar services have proprietary implementations. Amazon Web Services (AWS) is one example of a cloud service provider. AWS provides a variety of Infrastructure as a Service (IaaS) cloud services. The Elastic Compute Cloud (EC2) is a platform where customers can purchase computing power in the form of a computer connected to the Internet that the customer can control. The Simple Storage Service (S3) is a cloud storage offering, essentially acting like a large disk drive accessible from the Internet. Other examples of cloud service providers are Microsoft Azure, Salesforce, and Google App Engine.

For the purposes of our discussion about seizing evidence, we focus on gathering evidence from IaaS cloud providers. Online services, including social networking sites and Web-based email, inherently have different data of interest in e-discovery. Technical and legal experts have already analyzed many issues related to e-discovery of these services, including the publication of real subpoenas and search warrants. Concentrating on IaaS cloud services, we will take as broad a view as possible. However, remember that each provider may implement their cloud services in a proprietary manner that may influence the forensic data available, how those data are collected, and who has access to the data.

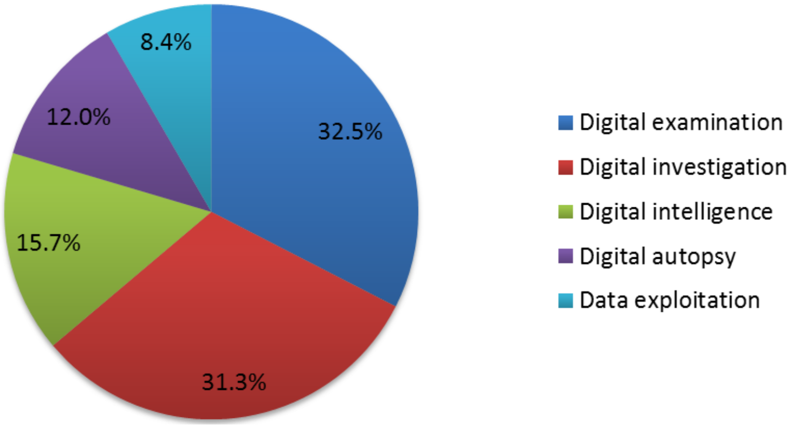
Digital Forensics and the Law

Digital forensics holds a unique place in the wider world of forensics distinguished by its meaning. In forensic odontology or forensic anthropology, for example, forensic investigators are concerned with applying their discipline to evidence of crimes and answering questions of interest to the legal system. In particular, these questions relate to how a crime was committed or how an individual died. "Digital forensics," on the other hand, has come to encompass a wide variety of activities. The term is so encompassing that it often refers to non-legal questions. Some people would say that any file recovery, such as an accidentally deleted term paper, is an example of digital forensics. Others would say that enforcing corporate policy is digital forensics, such as investigating an employee's computer to see if he or she were violating corporate policy against checking sports scores during work hours. This ambiguity in meaning threatens the credibility of the discipline.

In a recent online survey of forensic experts, primarily forensic investigators, 61% agreed or strongly agreed with the way the phrase "digital forensics" is used today (Dykstra, 2012). The respondents overwhelming felt that digital forensics did not need to involve a civil or criminal offense. However, of five published definitions of "digital forensics," they most agreed with those including the phrases "reconstruction of events found to be criminal" (43.8%) or "in a manner that is legally accepted" (39.3%).

The difficulty lies in the fact that there is no other accepted term to describe forensic-like digital investigations. Both legal and non-legal investigations may use the same software, procedures, and techniques. When the investigation must be legally sound, additional requirements are levied on the process, including chain-of-custody and authenticity. Our survey showed that given five alternative phrases, respondents preferred "digital investigation" and "digital examination" (see Figure 1).

Figure 1. Which of the following terms would best describe forensic-like activities that are not intended for legal process and are not bound by legal soundness?



For the purposes of these discussions, we assume that digital forensics is concerned with the acquisition and analysis of digital evidence to inform legal proceedings. Digital forensics is an umbrella term for any digital data that encompass sub-disciplines such as computer forensics, network forensics, database forensics, mobile device forensics, and video forensics. Even modest crimes involving digital devices require blending these disciplines, since nearly every computer is interconnected to another. Cloud computing, by its nature, draws upon computer forensics and network forensics since a networked computer is always involved. Other digital forensic disciplines may also be involved depending on the crime.

Related Work

We are unaware of any published template for writing a search warrant for cloud data. In 2006, a California attorney published an article titled "Search Warrant Language for Cellular Phones," describing how to obtain data from cell providers (Morgester, 2006). Several law enforcement manuals, which describe what data are available to law enforcement and how to request them, for Webmail and social networking Websites have leaked online. These may hint at similar data available for cloud services. Several search warrants have appeared in the press for services like Facebook (Willamette Week, 2011) and Gmail (Van Horn, 2009). The Department of Justice Search and Seizure Manual (2009) includes sample subpoenas, orders, and warrants which we used for guidance, but none of these were for cloud data.

Stephen Wolthusen (2009) highlighted a number of research challenges for forensic discovery in distributed environments. While he enumerated some of the legal challenges, he did not analyze the applicability of existing laws. Another study (Taylor, Haggerty, Gresty, & Lamb, 2011) looked more closely at UK-specific issues.

Other authors have taken a careful look at privacy related to cloud computing, the most common topic of law review articles related to cloud computing. Stylianou (2010) studied changes in the privacy terms of cloud services, and found that more private information was being surrendered to third parties but that companies were treating that data with more respect. Barnhill (2010) explained that court decisions extend no reasonable expectation of privacy in emails stored with third. Couillard (2009) wrote, "users expect their information to be treated the same on this virtual cloud as it would be if it were stored on their computer, phone, or iPod."

OBTAINING FORENSIC EVIDENCE FROM THE CLOUD

In criminal cases, discovery is the pre-trial phase where the prosecutor obtains information or evidence that may be used against a defendant during the trial. Electronic discovery refers to the exchange of Electronically Stored Information (ESI). Therefore, search and seizure of cloud-based evidence falls in the discovery phase of criminal prosecution.

In the United States, numerous constitutional and statutory provisions govern search and seizure, including that of forensic evidence from cloud providers. Since we focus on criminal cases, we will explore the Federal Rules of Criminal Procedure (FRCrP) and the Fourth Amendment. In this section, we show how these statues might apply to acquisition of cloud-based ESI. We intend only to introduce the array of issues rather than to dive deeply into each one.

One statute plays an important part in cloud forensics: the Electronic Communications Privacy Act of 1986 (ECPA), codified at 18 U.S.C. §§2510-22. ECPA includes two definitions that are important when discussing cloud computing and the law. The first is an "Electronic Communication Service" (ECS) that is "any service which provides to users thereof the ability to send or receive wire or electronic communications" (18 U.S.C. §2510). Title II of ECPA is referred to as the Stored Communications Act (SCA), 18 U.S.C. §2701-12, which adds the second definition. A "Remote Computing Service" (RCS) that is "the provision to the public of computer storage or processing services by means of an electronic communications system" (18 U.S.C. §2711). Different rules apply to the two services, and a cloud provider might be an ECS or RCS or both, depending on the services it provides.

Federal Rules of Criminal Procedure

The Federal Rules of Criminal Procedure (FRCrP) are a collection of 61 rules that govern the process of how criminal prosecutions are conducted in United States district courts. They were last amended in December 2011. In this section, we will consider six topics that describe how the Rules relate to seizing cloud-based data.

Available Data

The first question in considering cloud-based data is what data are available. FRCrP (2010) Rule 16 permits the ability to request data "in the defendant's possession, custody, or control." The respondent for discovery of cloud evidence will either be the cloud provider or a customer of the cloud service. The repackaging and reselling of cloud services introduces potential for legal complexity, since end-users may interface with a provider, which in turn uses cloud computing. Dropbox is an online storage service that uses AWS for data storage (Dropbox, 2012). Dropbox states that "All files stored online by Dropbox are encrypted and kept securely on Amazon's S3 in multiple data centers located around the United States." Customers negotiate services directly with Dropbox, not Amazon. If a Dropbox customer were under investigation, data could be requested from either Dropbox or Amazon or both. As we will see below, the petitioner's choice depends on what data are sought.

Unfortunately, the complete set of forensic data available to a requestor is publically unknown. The public cloud providers have thus far withheld their capabilities, possibly because they are protecting the proprietary cloud implementation that gives them competitive advantage. We speculate about data that are likely available, but cannot speculate about the provider's practical ability to collect these data. To discuss what data are in the cloud provider's control, it is important to understand what data might be available. Infrastructure as a

Service can be thought of as many layers of a cake, each independently providing part of the cloud service. The top layer of the cake contains the consumer's data and applications, which may be exposed to the Internet in the form of a Webpage or database. These data are the first that may be available, and by definition of IaaS are owned and controlled by the consumer. The next layer is the guest virtual machine, which in IaaS is also owned and controlled by the consumer. The third layer of the cake is the hypervisor, special software that runs on a provider's computer (called the host) and allows many virtual machines to run independently on a single physical machine. Below the physical machine is the distributed array of storage disks. The base of the cake is the computer networking that interconnects the components, and provides high bandwidth to the Internet.

Law enforcement policy manuals have not been made public by any of the major cloud providers that describe the records and data available under a search warrant. The providers control data related to subscriber information and billing records. As customers are billed based on their usage, records relating to service usage should also be available. Beyond these obvious requests, consider other data that the providers likely keep for some period of time. Connection information, sometimes called NetFlow records, that record the two endpoints of Internet communications are non-content data that can be useful as a historical record. Cloud services are provisioned by an out-of-band channel, usually on a special management website or through an Application Programming Interface (API). The provider may be able to produce logs showing successful and unsuccessful logins, from where those logins came, and when they occurred. If services can be provisioned programmatically, similar logs may be available. While it is not important to the functioning of the system for humans to know where data are located (*e.g.,* server or data center), the underlying infrastructure must know where they are. The provider may be recording system logs that describe where the data are, who created them, and when they were created, modified or deleted. In sum, law enforcement today has no template search warrants for cloud data and does not know what they can or should ask for.

Access to Data

Having considered what data are available, the next issue is the access to that data. With IaaS, data inside a consumer's virtual machine, such as a Webpage, are hidden even from the provider unless the consumer makes it available on the Internet. The cloud provider, whose ownership and responsibility extend to the hypervisor and below, could access the computer files that make up the virtual machine, and could provide a copy of the virtual machine during discovery. The provider also has other ample opportunities to collect content and non-content forensic evidence, all of which are in the provider's custody, possession, and control: they could collect network packet captures of all ingress and egress network traffic from their cloud; they have billing data about the provisioning and usage of cloud resources; they could collect logs showing the physical storage locations of data. The language of the contract between the provider and the customer will determine how much access the customer has to these data. In *Flagg v. City of Detroit* (2008), for example, the court ruled that text messages held by a provider were subject to the city's control, given that the city had some contractual right of access to the data. To complicate matters, there are data in the provider's possession over which the customer may not have legal custody (*e.g.,* infrastructure logs), and there are data in the provider's possession over which they may not have legal custody (*e.g.,* customer's data).

With most cloud providers, IaaS customers can usually collect network captures from inside their virtual machine, but they see only their own traffic. The Communications Assistance for Law Enforcement Act (CALEA, 1994) requires telecommunications carriers to assist law enforcement in performing electronic surveillance pursuant to court orders. However, the term "telecommunications carrier" does not include "persons or entities insofar as they are engaged in providing information services" (47 U.S.C. §1001(8)(C)(i), 1994). The law does not require cloud providers to provide real-time interception capabilities. In a statement before the House Judiciary Committee's hearing on *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies* (2011), the FBI and others identified this as a shortcoming (p. 23).

Preserving Evidence

Once law enforcement knows what data are available, and who has access to the data, the data must be preserved until it can be lawfully acquired. Preservation is an essential tool in electronic discovery, particularly with highly volatile and elastic data. The bar is very low to compel a provider to preserve a snapshot of potential evidence. In Section 2703 of the Stored Communications Act (2000), ECS and RCS providers "upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" for 90 days, which can be renewed for an additional 90 days. Section 2704 describes how a governmental entity, in a subpoena or court order, may order the provider to create a backup copy of the contents of the communications. Cloud providers need some mechanism for preservation, if they do not have one already. On one hand, the providers have an advantage in preserving even large volumes of data since they advertise broad storage resources. This alleviates traditional concerns about cost, such as in *Viacom Int'l Inc. v. YouTube Inc.* (2008), where the court ruled that the need for 12 terabytes of data overweighed the expensive and burdensome of production. Additionally, IaaS resources such as virtual machines inherently enable snapshots to be taken of the running machine at any time. On the other hand, the providers may have no way to prevent the de-provisioning of resources or deletion of data.

Consider the following example where cloud practices inhibit preservation. Cloud resources, such as virtual machines, are launched using a user's private key. A hacker steals the key from the legitimate owner, and uses it to launch hundreds of machines that flood a popular website and take it offline. The prosecution, wishing to subpoena data from the legitimate user, might ask for logs of activity showing who launched the machines, and copies of the machines themselves. However, the legitimate user may have no logs to produce, and the attacker may have deleted the hundreds of malicious machines. In traditional digital forensics, investigators create a bit-for-bit image of a hard drive that the examiner can search for deleted files. Tragically, while providers know when files are deleted in their storage array, and may have logs to prove it, they probably lack the ability to recover deleted files or to produce complete hard disk images. The Service Level Agreement for Microsoft Azure reads "You're responsible for backing up the data that you store on the service…Data that is deleted may be irretrievable" (Microsoft Corporation, 2010).

With the elasticity of cloud computing, ephemeral data will be problematic. In *Columbia Pictures v. Bunnell* (2007), the court concluded that Random Access Memory (RAM) data was discoverable. *Bunnell* also concluded that IP addresses were discoverable. In the Cloud, both data and infrastructure are potentially fleeting. Cloud providers ultimately must at least know when resources are provisioned and de-provisioned, since those activities directly determine billing of the customer. Elasticity also demands a method to preserve evidence either due to standard business practices or negligent destruction, known as spoliation. The courts have mandated preservation when litigation is reasonably anticipated (Zubulake v. UBS Warburg, 2003; AAB Joint Ventures v. United States, 2007). In civil cases, the Federal Rules of Civil Procedures in section 37(E) also protect the provider if data are “lost as a result of the routine, good-faith operation of an electronic information system.” There is no exact analog in the FRCrP, where willful, intentional destruction falls under obstruction of justice. Even so, “only persons conscious of wrongdoing” can be held liable, as Chief Justice William Rehnquist wrote when the Supreme Court overturned Arthur Anderson’s conviction of willfully destroying documents related to Enron (Arthur Andersen LLP v. United States, 2005).

Legal Right to Data

Ownership issues should be detailed in the contract between the cloud provider and consumer. Amazon Web Services has such a customer agreement (2012). In this contract, “content” is defined as “software (including machine images), data, text, audio, video, images or other content” (Amazon Web Services, 2012). In Section 8.1, Amazon clams “no rights under this Agreement from you or your licensors to Your Content, including any related intellectual property rights” (Amazon Web Services, 2012). The document defines “Service Offerings” as “the Services (including associated APIs), the AWS Content, the AWS Marks, the AWS Site, and any other product or service provided by us under this Agreement” (Amazon Web Services, 2012). In Section 8.4, Amazon clams that “we or our affiliates or licensors and reserve all right, title, and interest in and to the Service Offerings” (Amazon Web Services, 2012). In other words, the consumer explicitly owns their virtual machines, and does not own the IP address, hardware, or cloud-hosted infrastructure. Microsoft contracts contain similar language. “Except for material that we license to you, we don’t claim ownership of the content you provide on the service. Your content remains your content” (Microsoft Corporation, 2010). “Content” is not defined in this service agreement.

In cases where content is not defined, we must look to case law. In *Flagg* (2008), the court found that the city had a contractual right to text messages held by a third party provider. *Flagg* did not address the ownership of other data, such as the provider’s logs. In the issuance of a subpoena or search warrant, it will be vital to differentiate what data are in the custody, possession, or control of the provider verses the client.

Jurisdiction and Venue

Jurisdiction for cloud computing is somewhat different from other jurisdiction jurisprudence to date. Even in cases regarding online data, the cases almost exclusively revolve around websites. Online services such as Facebook and Gmail, though they comply with legal process for information, have neither been challenged about the backend geographic location nor locations of the resultant data. In the Cloud, the issue compounds since data will certainly be stored in several jurisdictions, and may be stored across international boundaries whose laws may be in conflict. In *United States v. Drew* (2009), the defendant was tried in California because she was accused of violating a social networking site’s terms of service, and the site’s owner was located in California. Courts have recently been applying the “effects test” for personal jurisdiction, based on “(1) intentional actions, (2) expressly aimed at the forum state, (3) causing harm, the brunt of which is suffered—and which the defendant knows is likely to be suffered—in the forum state” (Core-Vent Corp. v. Nobel Industries AB, 1993). Under that framework, one would expect most cloud-based litigation to occur in the cloud customer’s forum state. Many people assume that the laws protecting data are those where the data physically exists. However, there is no precedent or case law supporting this assumption. The effects test would lead us to believe that in most cases, crimes are committed against the data owners in their forum state, and not with the intent to cause harm in the forum state of the data.

FRCrP Rule 18 (2010), which says, "…the government must prosecute an offense in the district where the offense was committed," is no longer a straightforward issue. When a suit is brought where the cloud is the object of the crime, four options exist for venue of the trial: the perpetrator's forum, the cloud provider's forum, the cloud customer's forum, or the online data location forum. Cloud service providers may dictate the venue in their contract. Barring contractual establishment of venue, allows for offenses committed in one district to "be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." The Supreme Court held in *United States v. Beddow* (1992) that determining the proper venue "is best described as a substantial contacts rule that takes into account a number of factors—the site of the defendant's acts, the elements and nature of the crime, the locus of the effect of the criminal conduct, and the suitability of each district for accurate fact finding…" None of these factors are obvious in determining venue for cloud-based crimes. Any of the four venues we identified could make a compelling case to host the trial.

Cloud computing and most other Web services exist without deference to geographical location. We contend, however, that consumers have a "reasonable expectation of location" for their data. In general, users sensibly believe that if they are using a service provided by a US company that their data reside in the United States. They may also look at top-level domain names and assume that data stored by www.state.md.us, for example, is in the United States while that for *mail.ru* is in Russia. Most Service Level Agreements (SLA) for online services do not specify the location where data will be stored. Unless they have reason to believe otherwise (*e.g.*, Amazon Web Services allows customers to specify the geographic region where data is stored), consumers and end-users will make assumptions about the location of their data, and subsequently the laws governing it.

How to get Data

Finally, we consider the vehicles available to compel data from a provider. Traditional search warrants are authorized under FRCrP Rule 41. This type of warrant can be used to seize physical evidence, but only (with few exceptions) for objects in the court's jurisdiction. ECPA offers five mechanisms for the government to obtain electronic information from a provider, including its own kind of warrant. These five mechanisms are:

1. Subpoena;
2. Subpoena with prior notice to the subscriber or customer;
3. § 2703(d) court order;
4. § 2703(d) court order with prior notice to the subscriber or customer; and
5. Search warrant.

According to the DOJ Search and Seizure Manual (2009), "Department of Justice policy favors the use of a subpoena or other less intrusive means to obtain evidence from disinterested third parties, unless use of those less intrusive means would substantially jeopardize the availability or usefulness of the materials sought" (p. 111). Loss of availability is of paramount concern given the elasticity of the cloud. Regardless of the vehicle used, we have already seen a difference in what data are in the provider's possession, custody, or control, and what data are in the cloud customer's possession, custody, or control. To complicate the matter, 18 U.S.C. §2701 et. seq. prohibits a provider from disclosing user content in response to a civil subpoena. This was affirmed in *Flagg* (2008), saying "[The Stored Communications Act] lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to subpoena or court order." This decision on communication and the SCA provide drastically different protection for data storage in an ECS versus a provider of RCS, where 18 U.S.C. §2703(b) allows a cloud provider acting as a provider of RCS to disclose the contents of an account used for remote storage without a warrant, and without notifying the customer or subscriber. Kerr (2010) suggested that this is unconstitutional.

The final issue to consider is time. Typically, the issuing party will allow between 10 and 30 days to comply, except where the issuing court's local rules dictate a minimum time period for compliance. Given the ease with which cloud data could be destroyed by a criminal, and the lack of mechanisms likely available for providers to preserve evidence, the threat of spoliation is dramatically increased. One solution is to require faster compliance with court orders. The primary detractor to this approach is that it requires human intervention at the cloud provider and doesn't scale well. Another solution is to empower data owners and investigators to gather forensic evidence themselves. We are actively exploring this area.

Costs of Data Production

Upon execution of a warrant, the cost of cloud-based ESI production could be extensive. The situation is not entirely analogous to Zubulake v. UBS Warburg (2003). In Zubulake, the majority of the $273,649 production costs arose from the restoration of five offline magnetic tapes and attorney fees. Data stored in the Cloud are online and available for access. The physical act of locating and copying the data may still take considerable time. For example, Amazon (2012) offers an export service that enables customers to have their data copied to a storage device and mailed to them. This service costs $80.00 per storage device handled plus $2.49 per data-loading hour. These costs are unlikely to approach the costs of magnetic tape restoration; however, the analysis costs of large data volumes will dwarf the data production costs. If a cloud customer arbitrarily had two terabytes of data in the Cloud, it would take nearly 10 hours to copy to a USB hard drive, totaling $104.90. Degnan (2011) estimates forensic analysis at $1000 per gigabyte, bringing two terabytes to $2 million. Importantly, an IaaS cloud provider may be unable to search the corpus of data and produce specific evidence (*e.g.,* a particular file), but rather would have to hand over the whole data set.

Fourth Amendment

Search and seizure for evidence of crimes committed in or against the Cloud must be valid under the Fourth Amendment. This amendment reads:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const., amend IV).*

In this section, we will examine how the Fourth Amendment applies to cloud computing in three areas: expectation of privacy, requirements for a warrant, the execution of search warrants, and exceptions to the warrant requirement.

Expectation of Privacy

For simplicity, and given the previous work in this area, we assume that cloud computing customers have a reasonable expectation of privacy for their data, even though they have entrusted it to a third party. We also proceed under the current doctrine that applies the Fourth Amendment to online data. Therefore, under Katz v. United States (1967) and its progeny, we grant that a search is performed in obtaining cloud data, and that the Fourth Amendment is implicated by the violation of the reasonable expectation of privacy. Instead, we explore the issues surrounding the execution of a warrant for cloud data.

Requirements for a Warrant

Before a lawful warrant can be issued, a number of basic requirements must be met. First, the warrant must be approved by a court of law. Second, the Fourth Amendment requires probable cause, in a sworn statement, that the law enforcement officer requesting the warrant believes that the search will reveal criminal activity. Third, the Amendment requires that a warrant "particularly" describe the person, place, or thing to be searched. This third requirement presents an issue for cloud-based crimes.

In previous sections we examined the location-independent nature of cloud computing. This is clearly counter to the requirements of the Fourth Amendment. In addition to physical location, pinpointing the data to be searched is also problematic. In recent years, warrants for Web-based email could specify a particular sender, receiver, and timeframe, preventing the unnecessary production of the entire corpus of email. In IaaS, the warrant may equally narrow the search for data by filename, creation time, or author. Lawyers like to use an analogy between hard drives and filing cabinets. Given the nature of digital evidence, electronic searches do not overcome the need to scan the container for the evidence. Just as one would leaf through a filing cabinet looking for a particular document, so too must the investigator interrogate the computer looking for the particular file (Kerr, 2005). Unfortunately, distributed cloud data may require the leafing through many filing cabinets in many warehouses in many locations, where data is co-mingled with other user's data. Despite the potential for an unprecedented and overwhelming volume of ESI from cloud crimes, search warrants in these cases have a unique opportunity to address the particularity issue often associated with digital searches. Unfortunately, since cloud providers are opaque about their infrastructure, it would be impossible for the warrant to specify the search strategy or approach of execution ahead of time. With a basic understanding of cloud computing technology, magistrates should decline to impose conditions of issuing cloud-targeted warrants.

Execution of Search Warrants

The Fourth Amendment makes no explicit statement about who should execute the warrant, in other words, who should carry out the intentions of the warrant. Today, most search warrants for online data are served to the provider, and subsequently executed by the provider. The legal authority for the provider to execute a warrant comes from statute and case law. In particular, 18 U.S.C. § 2703(g) says "Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service." In United States v. Bach (2002), the court held that "The Fourth Amendment does not explicitly require official presence during a warrant's execution; therefore, it is not an automatic violation if no officer is present during a search." The practical reason is also germane: law enforcement does not have the resources or expertise to execute the warrant themselves. When the provider executes the warrant at the bequest of law enforcement, they may become agents of the government, a potentially undesirable state. In US v. Richardson (2010), the court held that America Online was not acting as an agent for the government when it uncovered and report child pornography in a user's email. However, this activity was not done at the government's request. Steven Morrison (2011) recently suggested that ISPs be treated as state actors for any search of user's email. Cloud providers may also look for ways to empower customers and law enforcement to acquire forensic data. This capability is admirable and would free the provider from the burden of doing all the work, and be an attractive feature to potential security-minded clients. Whether the provider or law enforcement does the search, it leads to two new questions: where can the search be done, and whose law applies?

Consider an example that illustrates this problem. Imagine a cloud provider incorporated in California has a data center in Virginia. A judge in Washington, DC, issues a warrant for data that resides in the Virginia data center. A resident of New York is the owner of the data. If executed by the provider, the search is done from a computer terminal in California. The provider also makes it possible for the FBI to execute the search remotely from their offices in DC. We propose that it does not matter where the search is done (inside of the United States), and that the search must comply with California law. The interconnected, networked nature of a national or global company makes it irrelevant where the search is done. Even if the provider executes the search in California, they will remotely access the data, across many interstate networks, in the Virginia data center. It follows, however, that the provider, being incorporated and governed by California law, ought to have jurisdiction over the search no matter where it happens.

Exceptions to the Warrant Requirement

The Fourth Amendment does not apply, and warrants are not required, in a number of circumstances. Two of these situations—consent and plain view—are considered here. In cloud crimes where a crime has been committed against an innocent data owner, that party can give consent to a search, and a warrant is not required. Someone whose website, hosted in the Cloud, has been hacked or whose data has been stolen, for example, is likely to cooperate with law enforcement in the criminal investigation. Another type of cloud-based crime is that where the party controlling the cloud resources is committing the crime. For example, if some party is distributing child pornography on a cloud-hosted website, it would be immediately apparent to an officer that incriminating evidence is hosted on the site. This situation is known as plain view, and no warrant is required to seize that contraband. Bear in mind, however, that after an officer identifies the contraband in plain view, a warrant based on the plain view evidence discovered is required for subsequent searches.

SEARCH WARRANTS FOR CLOUD DATA

Having considered some of the applications and implications of the law for seizing cloud-based ESI, we now turn to the act of acquiring the evidence. In preparation for a full search warrant example, let us walk through some of the cloud-specific parts of the warrant.

The first part of a search warrant must describe what is to be seized. The law requires “reasonable particularity” in the description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

In cloud computing environments, the “property to be seized” should contain a description of information (such as computer files) rather than physical hardware, regardless of the role of the computer in the offense. By definition, the physical hardware of a cloud provider is not owned by the suspect (unless the provider is the subject). Seizure of physical hardware yields no benefit that data alone cannot provide, and in fact may be disruptive to other cloud clients sharing that hardware. The “property to be seized” described in the warrant should fall into one or more of the categories listed in FRCrP Rule 41(b):

1. “Property that constitutes evidence of the commission of a criminal offense.”

This is a very broad authorization, covering any item that an investigator reasonably believes would reveal information that would aid in the investigation. "Property" has come to include tangible and intangible property. Case law has established that electronic data are also "property" that may be searched and seized.

2. "Contraband, the fruits of crime, or things otherwise criminally possessed."

In cloud environments, contraband could take one of the following forms. Contraband, including child pornography, pirated software, and other copyrighted materials, may be kept in cloud storage or inside of cloud virtual machines. When a hacker breaks into a machine hosted in the Cloud, that machine could be the fruits of the crime—that property acquired as the result of the crime of unauthorized access.

3. "Property designed or intended for use or which is or had been used as a means of committing a criminal offense."

Cloud environments could be used as the instrument of a crime in several ways. Cloud storage could be used to transmit child pornography, and cloud-based virtual machines could be used to produce it. A virtual machine could be used for hacking, or used to host websites with illegal content. In each case, the cloud contains property used to commit an offense.

The second step in drafting a warrant is to describe the property's location. The law, rooted in the physical world, is interested in where the property is. The location, which must be noted with reasonable particularity, has historically been a safeguard to citizens that limit the scope of the warrant. Search warrants for online Webmail have traditionally specified only the email address as the "place to be searched." "Location" requires special consideration when dealing with online data, especially with cloud computing. Only rarely will data be stored on a single server at the address of the data custodian. In many cases, the servers will be dispersed across state or international boundaries. Further, cloud data are often replicated to multiple datacenters. This seemingly presents a problem when describing the "location to be searched," since the agent or prosecutor may not know where the data containers are.

The search warrant for cloud-based data should not specify a physical address to be searched, lest the search exclude data stored at other physical locations. Instead, the warrant should specify the desired data and the warrant served to the data custodian.

Here is an example of how to describe the location of cloud-based data in some datacenter owned and controlled by Amazon:

Data, metadata, and account information created, stored, or controlled by Amazon Web Services LLC, 410 Terry Avenue North, Seattle, WA 98109-5210, related to IP address 1.2.3.4 for the time period beginning 12:01 a.m. CST (January 1, 2012) through 12:01 a.m. CST (July 1, 2012).

The terms "data" and "metadata" include all of the foregoing items of evidence in whatever form (such as virtual machines, user-created content, log data, packet captures, intrusion detection alerts, billing records) and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as volatile and non-volatile information on an electronic or magnetic storage device, including hard disks, backup storage, live memory, as well as printouts and readouts from any storage device), in any physical location controlled by the provider where the data may reside.

The third step in drafting a warrant is to set the parameters for executing the warrant. Federal warrants allow the specification for the time of day during which to execute the warrant, and the date by which to execute the warrant. These are further safeguards to ensure a limited lifetime of the warrant and minimal disruption (*e.g.* "in the daytime between 6:00 a.m. to 10 p.m.") to the subject of the warrant.

The elasticity and near instant provisioning and de-provision of data poses a legal challenge in cloud computing. Unless physical machines are seized or virtual machines are turned off, execution of the warrant is unlikely to impact or disrupt the data owner, but in fact risks spoliation if announced. The search warrant can be executed at any time in the day or night, but should be executed as soon as possible to preserve evidence. The traditional response time of 10 days should be shortened as much as possible, within reason of the logistical constraints of the cloud provider.

An affidavit to justify the search and seizure of cloud-based computer data should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy.

While agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases, cloud computing is a new discipline and currently requires special attention to defining new terms. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Figure 2 shows a sample definition for "cloud computing" which could be used in the affidavit. This, and several others, is included in the sample search warrant later in the chapter.

These concepts are embodied in the sample search warrant that follows. The key thing to remember is that the seizure should focus on data rather than hardware, and that the data may be distributed across physical locations.

Case Study

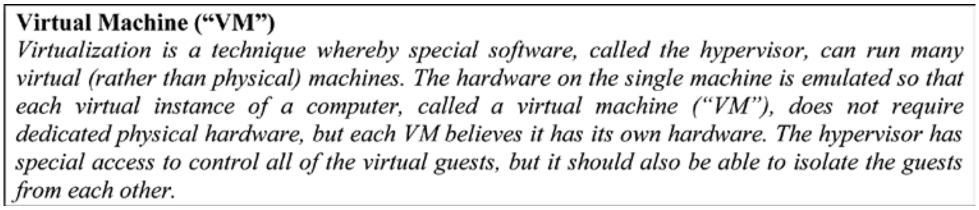
To illustrate the application of the concepts presented so far, we will now look at a hypothetical case study of a cloud-based crime. This case study was previously used to explain technical issues in cloud forensics (Dykstra & Sherman, 2011). After analyzing the scenario, we can then construct a sample search warrant that could be used in this case.

Here is the hypothetical crime:

Polly is a criminal who traffics in child pornography. He has set up a service in the Cloud to store a large collection of contraband images and video. The website allows users to upload and download this content anonymously. He pays for his cloud services with a pre-paid credit card purchased with cash. Polly encrypts his data in cloud storage, and he reverts his virtual Web server to a clean state daily. Law enforcement is tipped off to the website and wishes both to terminate the service and prosecute the criminal.

This is a case where the computer is incidental to the offense. Let us assume that this scenario took place in Amazon EC2. Let us assume that law enforcement first contacts the cloud provider with a preservation order to retain evidence pend-

Figure 2. Definition of "virtual machine" for use in a search warrant



Virtual Machine ("VM")
Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a virtual machine ("VM"), does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

ing a warrant. Preservation is authorized under 18 U.S.C. §2703(f)(1) which says "A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." Tracking down the user is the more difficult task.

The examiner has no technical ability to image the virtual machine remotely since the cloud provider does not expose that functionality, and in doing so would alter the state of the machine. Deploying a remote forensic agent, such as EnCase Enterprise, would require the suspect's credentials, and functionality of this remote technique within the Cloud is unknown. Simply viewing the target website is enough to confirm that the content is illegal, but it tells us nothing about who put it there. Additionally, no guarantee can yet be made that the target Web server has not been compromised by an attacker, or that the examiner's request to the Web server was not the victim of DNS poisoning, man-in-the-middle, or some other alteration in transit.

Consider other possible sources of digital evidence in this case: credit card payment information, cloud subscriber information, cloud provider access logs, cloud provider NetFlow logs, the Web server virtual machine, and cloud storage data. Assistance from the cloud provider is paramount here. Law enforcement can issue a search warrant to the cloud provider, which is adequate to compel the provider to provide any of this information that they possess. Law enforcement need not execute or witness the search. The warrant specifies that the data returned be an "exact duplicate," the forensic term that has historically meant a bit-for-bit duplication of a drive. Since child pornography is a federal offense, the provider must comply with the order. A technician at the provider executes the search order from his or her workstation, copying data from the provider's infrastructure and verifying data integrity with hashes of the files. Files may have been distributed across many physical machines, but they are reassembled automatically as the technician accesses them. Though the prosecution may call the technician to testify, we have no implicit guarantees of trust in the technician to collect the complete data, in the cloud infrastructure to produce the true data, nor in the technician's computer or tools used to collect the information correctly. Nonetheless, the provider completes the request, and delivers the data to law enforcement.

To reconstruct the crime, the forensic investigators need evidence to help them piece together the following:

- A copy of the virtual machine in order to understand how the Web service works, especially how it encrypts/decrypts data from storage;
- Keys to decrypt storage data, and use them to decrypt the data;
- Copies of all files in order to confirm the presence of child pornography; and
- Cloud access logs or NetFlow to identify possible IP addresses of the criminal.

By viewing the website it is clear that it contains illegal content, but not who the data owner is. Timestamps and other file metadata may prove useful, provided they are available and accurate. For this reason, complete bit-for-bit copies of the original evidence are important.

Case Study Search Warrant

The appendix presents one example of an application for a search warrant in the hypothetical case study. Note how the request focuses on data rather than on hardware. For this reason, it is written as an ECPA §2703(d) warrant. An FRCrP Rule 41 warrant would have been used to seize hardware or imaging disk drives on-site. A template warrant can be found at http://cisa.umbc.edu/warrant/. The document is an academic example and is not legal advice. The warrant should not be used in practice without seeking legal counsel.

Paragraph 1 establishes the request for cloud data in investigation of the crime. Paragraph 4 details the cloud crime and presents probable cause that the provider has relevant evidence. The technical background in paragraphs 5-12 is specific to cloud computing, using Amazon as the example. They describe how the service works and what data may be available. Paragraphs 13-23 are similar to language found in any request for electronic evidence.

CHALLENGING CLOUD EVIDENCE

Earlier in the chapter, we discussed the details of seizing cloud data. This section describes defenses that may be asserted to discredit that evidence. Some issues parallel the scrutiny of any evidence, while others arise explicitly from the use of cloud technology. We consider four topics here: issues with jury comprehension, problems with the execution of the search, the *Daubert* test for scientific validity and relevance, and whether now is the right time for judicial decisions.

Jury Comprehension

By nature, the cloud-computing environment is more complex than a single computer or a server. The environment has many layers of implementation that must be trusted to produce authentic data (Dykstra & Sherman, 2012). In 2009, for example, Kostya Kortchinsky (2009) at Immunity demonstrated a working exploit to break out of a virtual machine and attack the host. In a real world situation this may have eroded confidence in the forensic evidence. The courts have repeatedly said that the *possibility* of an action is insufficient to say it is so (Noblesville Casting Div. of TRW v. Prince, 1982). That opinion also said that "Of course, an expert's opinion that something is "possible" or "could have been" may be sufficient to sustain a verdict or award when it has been rendered in conjunction with other evidence concerning the material factual question to be proved." There are numerous "what if" scenarios for data tampering in the Cloud. A non-comprehensive list includes: data could be tampered with in transit over the network inside the cloud network; redundant copies of the data could have gotten out of sync; the credentials of the data owner could have been compromised resulting in false data creation or data tampering; there could have been opportunities for insider threats at the provider; the hypervisor may be insecure allowing a malicious user to manipulate other virtual machines; the host operating system could be compromised; there could be weak or no encryption on the provider's internal infrastructure for data in transit or data at rest allowing malicious actors to change the data. Nevertheless, computer malfunction and malfeasance must be investigated and can raise doubt in the confidence of the evidence. The hypervisor is especially vulnerable to scrutiny given its powerful position to see and manipulate all of the virtual machines that it controls, including the data therein. Many cloud service providers use custom, proprietary hypervisors that have not been seen or audited independently by the global security community.

Complexity of evidence also stands to challenge judges and juries who lack knowledge about cloud computing. This kind of complex litigation might leave the lay juror "spinning with information too strange to digest and often too intimidating to ponder" (Broyles, 1996). Much has been written, particularly over the last 20 years, about jury comprehension of complex evidence, including highly scientific evidence such as DNA. In *Citizen Comprehension of Difficult Issues: Lessons from Civil Jury Trials* (Cecil, Hans, & Wiggins, 1991), the authors recommended comprehensive examination of how courts handle scientific and technological complexity in litigation. While 78% of American adults—and potential jurors—use the Internet as of August 2011, according to The Pew

Internet and American Life Project (2011), this says nothing about their comprehension about how it or their computer works. Cloud computing is one of the most complex computing environments today, likely to challenge even the most technically inclined juror. Evidence and expert witness testimony must be artfully presented.

Execution of the Search

In the status quo, cloud providers execute search warrants and subpoenas on behalf of law enforcement. In this regard, cloud providers act no differently than any other Internet-based entity. Doing so raises a conflict of interest. The cloud providers have an interest in protecting their reputations, and may not be disinterested parties in an investigation. Furthermore, the provider may not have authority or discernment about what other evidence is in plain view. The courts, in fact, have been split about the issue of plain view for digital evidence (United States v. Williams, 2010; United States v. Mann, 2010). Rigorous guidelines, such as how to challenge the scope and procedure of the search, are lacking today. Barring these changes, it would be preferable for an independent third party to execute the warrant or subpoena at a cloud provider. Until the process of how a search is executed by the provider is well understood, the prosecution should call the technicians to testify about how records are created and the methodology used to retrieve them. As has been noted before, "the Government need not call each of the technicians who did the search so long as it" presents a witness who can "`explain and be cross-examined concerning the manner in which the records are made and kept'" (United States v. Cameron, 2009).

In Covad Communications Co. v. Revonet, Inc. (2009), Judge Facciola wrote, "it is the rare case that a litigant does not allege some deficiency in the production of electronically stored information…" Production of cloud-based evidence will be no different, particularly since that kind of evidence is entirely new to the courts. Some of the issues that could be raised about the deficiency of production of cloud-based ESI include: Who at the provider executed the search warrant, what were their credentials, and how was the search done? Can the technician who executed the search attest to the reliability and authenticity of the data, including, but not limited to, the security of the workstation used to execute the search, the security of the network to prevent data tampering over the network, and a record of who had access to the data? Does the provider maintain aggressively enforced records management policies that can provide authenticity and authentication of the data, perhaps in the form of data provenance? Can the provider attest to the reputation and integrity of the cloud infrastructure, including the hypervisor and host operating system? Were the data located on drive, or distributed over many? If multiple, are the timestamps of those systems internally consistent? Is it possible that important evidentiary data once existed and has been deleted, and if so, is there any record of it? As these questions illustrate, the most vulnerable aspects of cloud discovery are expert witness testimony and the forensic methodology used.

The Daubert Test

The Daubert standard, from the landmark Supreme Court case Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993), can be used to measure the scientific validity and relevance of forensic evidence. Daubert includes factors such as whether a theory or technique has been tested, whether it has been subject to peer review and publication, where there is a known error rate, and whether the theory or technique is generally accepted within the relevant scientific community. Because cloud forensics is a new discipline, the answer to each of these factors is "no." Popular forensic tools such as EnCase have passed the Daubert test, given in part to their commercial availability, testing by the government, long-term use by the community, and extensive acceptance in court. On the contrary, techniques for remote forensics, let alone cloud forensics, do not enjoy any consensus in the forensic community.

Tools designed specifically for cloud investigations have not yet appeared, and forcing existing tools into this role may be ill advised. Forensic practitioners, unfamiliar with cloud environments, will be tempted to use their existing tools like EnCase when first investigating cloud crimes. According to Guidance Software (2011), "There are more than 40,000 licenses of EnCase technology worldwide, the EnCase Enterprise platform is used by more than sixty percent of the Fortune 100, and thousands attend renowned Guidance Software training programs annually." Even so, the advertised features of commercial tools, including EnCase, which can be used for remote forensics, have not been tested for correctness or error rate, and have not yet been presented in court. In the United States, the National Institute of Standards and Technology's (NIST) Computer Forensic Tool Testing (CFTT) group is charged with testing digital forensic tools, measuring their effectiveness, and certifying them. NIST (2012) evaluated EnCase 6.5 in September 2009, but has never evaluated EnCase Enterprise which includes the remote forensic features. This software is not without fault. In 2007, a vulnerability was found in the authentication between the remote EnCase client and the server which could allow an attacker to corrupt or falsify data (Giobbi & McCormick, 2007).

When to Rule

Finally, cases emerging today involving cloud-based evidence are unlikely to produce judicial guidance, particularly from the Supreme Court, on ripeness grounds. Ripeness refers to the fact that because the technology is new, legal decisions are contingent upon future changes that cannot be anticipated. Cloud computing technology has evolved over time and continues to change on a regular basis. Amazon Web Services announced new features or service changes at least one time per month during 2011. Other providers have a similar pace of change. Adjudicating too narrowly on cloud-specific issues would be premature, even though broad application of established principles (*e.g.,* Fourth Amendment search and seizure) are apropos. In fact, recent comments by US Supreme Court Justice Sotomayor reveal potentially changing attitudes about the expectation of privacy in data given to third parties, a decision whose consequences would affect cloud computing. In United States v. Jones (2012), she wrote "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."

FUTURE RESEARCH DIRECTIONS

Because cloud crimes are not yet widespread and public, it is difficult to predict how the legal system will handle them. Public cases could reasonably be predicted in the next one or two years. These proceedings will test the viability of search and seizure of ESI in cloud environments. Successful legal prosecution will rely on continued education of the players involved, legal interpretation by the courts, and technical capabilities of forensic investigators.

The global, distributed nature of cloud computing will require scholars in other countries to consider how laws in their countries may apply to cloud crimes. Further, ample work remains for establishing how law enforcement will cooperate in cross-boundary cloud investigations.

CONCLUSION

Cloud computing is an advancement in the history of computation due in large part to the convergence of technologies. The economics of the paradigm will drive growth and adoption rates from companies and individuals. Where the people, the data, and the money go, so does crime. While investigators struggle with the new problems of acquiring and analyzing cloud data, the law must prepare for the legal challenges associated with acquiring and presenting cloud data in court. 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 a new legal precedent.

When these cases emerge, each player's actions will be shaped by an interpretation of how traditional discovery rules govern the cloud crime. As we saw, applying these rules can be murky and unclear. Preservation, ownership, jurisdiction, and search warrant execution are just some areas where we saw non-trivial challenges.

Examining a concrete case study helped highlight the practical implication of the complex considerations for acquiring evidence. However, the case study introduced a context against which to build a search warrant. As a first public example, this language arms law enforcement agents with topics to consider when they draft their first warrant for cloud data. Arming the prosecution also led us to outline some of the areas that defense teams could incorporate into their own strategies.

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-based crimes. Our exploration of seizing electronic evidence from cloud computing provides a foundation to forensic investigators and legal professionals as they investigate and prosecute of cloud-based crimes.

REFERENCES

AAB Joint Ventures v. United States, 75 Fed. Cl. 432 (2007).

Amazon Web Services. (2012a). *AWS customer agreement*. Retrieved from http://aws.amazon.com/agreement/

Amazon Web Services. (2012b). *AWS import/export*. Retrieved from http://aws.amazon.com/importexport/

Arthur Andersen LLP v. United States, 544 U.S. 696 (2005).

Barnhill, D. S. (2010). Cloud computing and stored communications: Another look at Quon v. Arch Wireless. *25*. *Berkeley Technology Law Journal*, *27*, 621–671.

Broyles, K. E. (1996). Taking the courtroom into the classroom: A proposal for educating the lay juror in complex litigation cases. *64*. *The George Washington Law Review*, *714*, 721–722.

Cecil, J. S., Hans, V., & Wiggins, E. (1991). Citizen comprehension of difficult issues: Lessons from civil jury trials. *40*. *The American University Law Review*, 727–774. Retrieved from http://www.wcl.american.edu/journal/lawrev/40/cecil.pdf

Columbia Pictures Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal 2007) (2007).

Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001-1010 (1994).

Core-Vent Corp. v. Nobel Industries *AB*, 11 F.3d 1482, 1486 (9th Cir. 1993) (1993).

Couillard, D. A. (2009). Defogging the cloud: Applying fourth amendment principles to evolving privacy expectations in cloud computing. *Minnesota Law Review*, *93*, 2205–2239.

Covad Communs. Co. v. Revonet, Inc., 2009 U.S. Dist. LEXIS 47841 (D.D.C. May 27, 2009) (2009).

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Degnan, D. (2011). Accounting for the costs of electronic discovery. *Minnesota Journal of Law. Science& Technology*, *12*, 151–190.

Dropbox. (2012). *Where does Dropbox store everyone's data?* Retrieved from https://www.dropbox.com/help/7

Dykstra, J. (2012). *Survey of digital forensics and the law*. Unpublished Raw Data.

Dykstra, J., & Sherman, A. T. (2011). Understanding issues in cloud forensics: Two hypothetical case studies. In *Proceedings of the 2011 ADSFL Conference on Digital Forensics, Security, and Law*, (pp. 191-206). ADSFL.

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure as a service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*. Retrieved from http://www.csee.umbc.edu/~dykstra/DFRWS_Dykstra.pdf

Flagg v. City of Detroit, 252 F.R.D. 346, 353 (E.D. Mich. 2008) (2008).

Galante, J., Kharif, O., & Alpeyev, P. (2011). Sony network breach shows Amazon cloud's appeal for hackers. *Bloomberg*. Retrieved November 2, 2011, from http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html

Giobbi, R., & McCormick, J. (2007). *US-CERT vulnerability note VU912593 - Guidance EnCase enterprise uses weak authentication to identify target machines*. Retrieved from http://www.kb.cert.org/vuls/id/912593

Guidance Software. (2011). *Leading eDiscovery, forensics, and cybersecurity solutions – Encase*. Retrieved from http://www.guidancesoftware.com

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review*, *119*, 531–585.

Kerr, O. S. (2010). Applying the fourth amendment to the internet: A general approach. *Stanford Law Review*, *62*, 1005–1029.

Kortchinsky, K. (2009). *CLOUDBURST: A VMware guest to host escape story*. Retrieved from http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Microsoft Corporation. (2010). *Microsoft services agreement*. Retrieved from http://explore.live.com/microsoft-service-agreement

Morgester, R. (2006). Search warrant language for cellular phones. *Cyber Crime Newsletter*. Retrieved from http://www.olemiss.edu/depts/ncjrl/pdf/May-June%202006%20Final%20Copy.pdf

Morrison, S. R. (2011). What the cops can't do, internet service providers can: Preserving privacy in email contents. *Virginia Journal of Law & Technology*, *16*, 253–300.

National Institute of Standards and Technology. (2012). *Disk imaging*. Retrieved from http://www.cftt.nist.gov/disk_imaging.htm

Pew Internet and American Life Project. (2011). *Internet adoption*. Retrieved from http://www.pewinternet.org/Trend-Data/Internet-Adoption.aspx

Stored Communications Act of 1986, 18 U.S.C. §§ 2701-2712 (2000).

Stylianou, K. K. (2010). An evolutionary study of cloud computing services privacy terms. *The John Marshall Journal of Computer & Information Law*, *27*, 593–612.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigations of cloud computing systems. *Network Security*, *3*, 4–10. doi:10.1016/S1353-4858(11)70024-1

United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (2002).

United States v. Beddow, 957 F.2d 1330, 1335 (6th Cir.1992) (1992).

United States v. Cameron, 573 F.3d 179, 183 (4th Cir. 2009) (2009).

United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (2009).

United States v. Jones, 132 S. Ct. 945 (2012).

United States v. Mann, 592. F.3d 779, 782 (7th Cir. 2010) (2010).

United States v. Williams, 2010 U.S. App. LEXIS 1327 (4th Cir. Jan. 21, 2010) (2010).

US Department of Justice. (2009). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. Retrieved from http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

US Government. (2010a). *Federal rules of civil procedure*. Retrieved from http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Civil%20Procedure.pdf

US Government. (2010b). *Federal rules of criminal procedure*. Retrieved from http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Criminal%20Procedure.pdf

US House of Representatives Committee on the Judiciary. (2011). *Going dark: Lawful electronic surveillance in the face of new technologies*. H.R. REP. NO. 112-159. Washington, DC: US House of Representatives Committee on the Judiciary.

Van Horn, C. (2009). *Chris Coleman documents and search warrants*. Retrieved from http://www.examiner.com/article/chris-coleman-documents-and-search-warrants

Viacom Int'l Inc. v. YouTube Inc., 2008 WL 2627388 (S.D.N.Y. 2008) (2008).

Willamette Week. (2011, April 8). You look like Obama: FBI seeks Facebook records for person of interest in mosque arson. *Willamette Week*. Retrieved from http://www.wweek.com/portland/blog-26890-you_look_like_obama_fbi_seeks_facebook_records_for.html

Wolthusen, S. (2009). Overcast: Forensic discovery in cloud environments. In *Proceedings of the Fifth International Conference on IT Security, Incident Management, and IT Forensics*, (pp. 3-9). IEEE.

Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003) (2003).

Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 291 (S.D.N.Y. 2003) (2003).

KEY TERMS AND DEFINITIONS

Daubert Test: The *Daubert* Test is based upon the US Supreme Court decision in *Daubert v. Merrell Dow Pharmaceuticals*, which establishes a set of standards for dealing with the reliability of scientific techniques used in forensics. The four factors are: testability, peer review, error rates, and acceptability.

Electronic Communication Service: Electronic Communication Service is defined in 18 U.S.C §2510 as "any service which provides to users thereof the ability to send or receive wire or electronic communications."

Electronic Discovery: Electronic discovery, or e-discovery, is the process of seeking, locating, collecting, and producing electronic data as evidence in a civil or criminal legal matter.

Evidence Preservation: Preservation broadly refers to the process involved in ensuring continued access to evidence, including protection against destruction or deterioration of evidence.

Remote Computing Service: Remote Computing Service is defined in 18 U.S.C §2711 as "the provision to the public of computer storage or processing services by means of an electronic communications system."

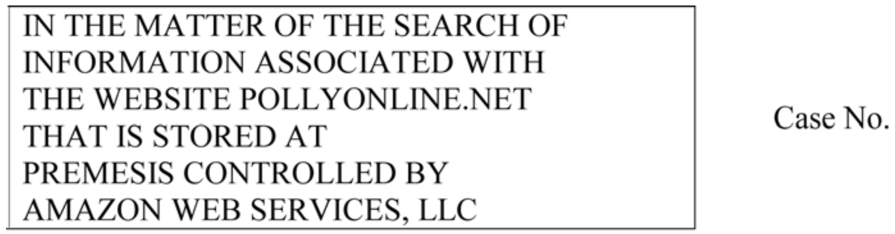
Search Warrant: A search warrant is a legal document which authorizes law enforcement to search and seize a person or location for items named in the warrant as evidence of a crime. In the United States, searches must be reasonable and specific under the Fourth Amendment of the US Constitution.

Seizure: Legal seizure is the confiscation of property, against the will of the possessor or owner, by legal process.

APPENDIX: Sample Warrant

UNITED STATES DISTRICT COURT

FOR THE ____WESTERN DISTRICT OF WASHINGTON**____**



IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE WEBSITE POLLYONLINE.NET
THAT IS STORED AT
PREMESIS CONTROLLED BY
AMAZON WEB SERVICES, LLC

Case No.

APPLICATION OF THE UNITED STATES

FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(D)

I, JOHN DOE, being first duly sworn, hearby depose and state as follows:

INTRODUCTION AND AGENT BACKROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Amazon Web Services (AWS) accounts and Internet Protocol (“IP”) address that are stored at premises owned, maintained, controlled, or operated by Amazon Web Services (the “Company”), LLC, a Web services company headquartered at 410 Terry Avenue North, Seattle, Washington, 98109 (the “Premises”), which functions as an electronic communications service provider and remote computing service. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require AWS to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the Web site.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since January 2003. I am currently assigned to the Baltimore Field Office, Cyber Squad. Since joining the FBI, I have been involved in investigations of computer intrusions, intellectual property right violations and Internet fraud. I have also been assigned to investigate Sexual Exploitation of Children (SEOC) violations of federal law. I have gained experience conducting such investigations through training and everyday work related to these investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter

PROBABLE CAUSE

4. On April 1, 2012, an anonymous tip was submitted to the FBI's Baltimore Field Office that the website www.pollyonline.net contained and was distributing child pornography, in violation of 18 U.S.C. §§ 2252 and 2252(a). I determined that the IP addresses for the website hosting the material resolved to one assigned to Amazon Web Services. On April 3, 2012, a preservation request was sent to AWS related to this website and its IP address. Accordingly, this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

TECHNICAL BACKGROUND

5. Based on my training and experience, I use the following technical terms in this Affidavit and Attachments A and B to this Affidavit:
   a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.
   b. "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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.
      i. "Infrastructure as a Service" (IaaS) allows a consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

ii. “Platform as a Service” (PaaS) allows a consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

iii. “Software as a Service” (SaaS) allows a consumer to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSPs offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage.

CSPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSPs reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.”

CSPs may be able to provide some of the following, depending on the type of services they provide:

NetFlow
Full Packet Captures
Firewall and Router Logs
Intrusion Detection Logs
Virtual Machines
Customer Account Registration
Customer Billing Information

d. “Virtual Machine” (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

6. Amazon Web Services (AWS) is an IaaS Cloud Service Provider, a subsidiary of Amazon.com, Inc., that does business online at http://aws.amazon.com. AWS allows its users to establish accounts with the company, and users can use their accounts to purchase the use of a variety of cloud computing resources offered by AWS.
7. AWS requires users to provide basic contact information during the registration process. This information includes the user's full name, contact e-mail address, physical address (including city, state, and zip code), telephone number, credit card information, and billing address. Users must read and agree to the AWS Customer Agreement. The final step in the registration process is identity verification where an automated system at AWS calls the phone number provided with a verification code that must be entered online.
8. AWS users have the ability to store and retrieve data in the Amazon Simple Storage Service (S3). S3 can store an unlimited number of data objects, which may be documents, photos, videos, or other data. Each object is retrieved using a unique, user-specific key. AWS users are billed based on the amount of data stored, and the transfer into and out of the cloud.
9. AWS provides its users the ability to purchase computing resources on the Amazon Elastic Compute Cloud (EC2). EC2 is a virtual computing environment that allows users to create, use, and manage an unlimited number of virtual machines. Each virtual machine is associated with the user that created it. The user has complete freedom to configure and use the VM as they wish, including installing software and services such as a Webserver. AWS users are billed based on the type of VM they choose, and the number of hours that the VM is running.
10. AWS stores user-generated data in more than one physical location. They state "Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region." (http://d36c-z9buwru1tt.cloudfront.net/AWSRiskandComplianceWhitepaperJanuary2012.pdf). User-generated data are unlikely to be stored at the Premises. However, system administrators, using the software that controls the cloud infrastructure, have the ability to identify the physical and geographic storage location of the disk drives containing the data.
11. Cloud Service Providers like AWS typically retain information about their users' accounts, such as the types of service utilized, the date and time of when the services were started and stopped, and connection information (such as the Internet Protocol ("IP") address from where the request initiated).
12. Therefore, the computers of AWS are likely to contain all the material just described, including user-created content, stored electronic communications, and information concerning subscribers and their use of AWS, such as account access information, transaction information, and account application.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Amazon Web Services to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
14. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the Premises or data centers controlled by AWS, in whatever form they are found. I submit that for some computers or electronic medium found on the Premises or in data centers controlled by AWS, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:
    - f. Based on my knowledge and experience, I know that Cloud Service Providers bill customers based on the usage of services, and that current and historical billing records are likely to be kept for resources currently being used.
    - g. I know that Cloud Service Providers have a tremendous amount of storage capacity, and that this storage is distributed across physical storage media (i.e., hard drives) in multiple data-centers in multiple geographic locations. I also know that software keeps track of how data is stored in this environment, and that it has the ability to identify the physical location of any piece of data and reconstruct the pieces into their original format.
    - h. I know from training and experience that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. Even a small portable disk or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials.
15. In this case, the warrant application requests permission to search and seize images of child pornography, including those that may be stored on a virtual machine. These things constitute both evidence of crime and contraband.
16. I know that when an individual uses a website to distribute child pornography over the Internet, the Web server will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

17. Because several people share the Premises as customers of the cloud service, it is possible that the Premises will contain data that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found with those intermingled data, this application seeks permission to seize that data as well.
18. Based upon my knowledge, training and experience, I know that searching for information stored in cloud providers may result in a large amount of electronic storage to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
    i. The volume of evidence. Computer storage devices (like hard disks) can store the equivalent of millions of pages of information. Cloud computing offers a vast amount of storage for very little cost. Additionally, a suspect may try to conceal criminal evidence; he or she might encrypt the data or store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored.
    j. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software, and non-traditional data formats used to support a cloud environment requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources, destructive code imbedded in the system, or malicious insiders, a controlled environment may be necessary to complete an accurate analysis.
19. The information requested should be readily accessible to Amazon Web Services by computer search, and its production should not prove to be burdensome.
20. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require AWS to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

21. Based on my training and experience, and the facts as set forth in this affidavit there is probable cause to believe that on the computer systems in the control of Amazon Web Services there exists evidence of a crime, contraband, and fruits of a crime. Accordingly, a search warrant is requested.

22. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A). Specifically, the Court is "a district court of the United States… that – has jurisdiction over the offense being investigated." 18 U.S.C. §2711(3)(A)(i).
23. Pursuant to l8 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations, as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,
JOHN DOE
Special Agent
Federal Bureau of Investigation
Subscribed and sworn to before me on ___________:
____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the website www.pollyonline.net resolving to IP address 23.20.70.250 that is hosted at premises owned, maintained, controlled, or operated by Amazon Web Services, a company headquartered at 410 Terry Avenue North, Seattle, Washington, 98109.

ATTACHMENT B

Property to Be Searched

I. Information to be disclosed by Amazon Web Services
To the extent that the information described in Attachment A is within the possession, custody, or control of AWS, AWS is required to disclose the following information to the government for the IP address listed in Attachment A:

(a) All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers of the user or users of services associated with the IP address;
(b) IP logs, including all records of the IP addresses that logged into the accounts associated with the IP address;
(c) Firewall, router, and intrusion detection logs associated with the IP address;
(d) The length of service (including start date), the types of service utilized by the user or users associated with the IP address, and the means and source of any payments associated with the service (including any credit card or bank account number).

II. Information to be seized by the government
All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252(a) involving www.pollyonline.net from April 1, 2012 to April 30, 2012, including information pertaining to the following matters:

(a) The virtual machine assigned to the IP address in question on April 1, 2012;
(b) A list of other IP addresses assigned to the virtual machine in question, and the dates and times they were assigned;
(c) Packet captures of traffic to and from the virtual machine in question;
(d) Data stored in any other cloud service, including S3 and DynamoDB, associated with the account running the virtual machine;
(e) Records relating to who created, used, or communicated with the website.