Global Knowledge®

Expert Reference Series of White Papers

Legal Issues of Cloud Forensics

Legal Issues of Cloud Forensics

David Willson, Attorney at Law, CISSP, Security+

Introduction

The use of cloud services has skyrocketed primarily because it is cheaper and more convenient than the alternative. Unfortunately, many companies have entered the cloud without first checking the weather forecast or performing a risk analysis. What happens if the cloud gets stormy, you suffer a breach, and you find yourself in the position of having to conduct digital forensics? What now? Can you collect data yourself? Where is your data? Who else has had access to your data? Is the provider the actual data holder or have they subcontracted? Many of these issues are better addressed before you enter the cloud. Failing that, what can you do?

Challenges of Cloud Forensics

Unlike traditional digital forensics, cloud forensics presents a unique challenge due to the omnipresent nature of "the cloud." Many of these challenges are legal and can be overcome by planning. National Institute of Standards and Technology (NIST) defines the cloud as, "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."[1] Okay, in English, the cloud is a service, like online backup, online software, and other computing services, owned by someone else and not physically resident on your computer, similar to renting a car. It can be accessed from anywhere you have an Internet connection.

Many people mistakenly assume that services such as Gmail, Yahoo, LinkedIn, etc., are cloud services. The primary difference is that those services are free, whereas cloud services require payment by subscribers. This distinction is important, because it provides a clearer description of the cloud. Privacy and legal issues will likely differ for paid and free services, as will the ability to negotiate the terms of service. The absolute necessity to negotiate the terms will be discussed later in this paper.

The four defining characteristics of the cloud are: on-demand self-service[2], rapid elasticity[3], location independence[4], and data replication[5].

Why You Would Need to Collect Data from a Cloud Provider?

This white paper explores issues a company or forensic examiner may face when collecting information from the cloud with a primary focus on civil litigation or other action as opposed to collecting evidence for criminal pros-

ecution. Much overlap exists between the situations, and some comparisons will be made. Although this paper discusses many legal issues, this is not a legal "how-to" article, as it does not discuss any and every potential issue, tool, technique, etc. The purpose is to provide some insight into cloud forensics. My research on the topic has not yielded a source that provides clear and concise guidance, so I hope this starts the ball rolling.

The issues I'll cover include:

- Can you collect the data yourself?
- Which jurisdiction applies?
- Can you compel the disclosure of data?
- What tools or techniques are available for compelling information?
- Can you prepare for cloud forensics?

Can You Collect the Data Yourself?

Once you suspect an incident has occurred and decide to collect data, you must decide **why** the data are being collected (e.g., for remediation, court, or some other reason) and, thus, **what** data need to be collected. If you can easily collect the necessary data in the normal course of business via the company's access to the cloud, you should revert to standard digital forensic techniques following well-established procedures and ensuring a clean chain of custody.

On the other hand, if you have to ask for assistance from the cloud providers, you must identify the provider. Doing so may not initially be obvious, since your company may have changed providers over time, the person who initiated the cloud usage may no longer be with the company, or many other reasons.[6] Once the provider is identified, determine where its headquarters and state of incorporation are located. This is necessary so you can determine the applicable jurisdiction and law, as you may have to send legal documents, preservation letters, or litigation holds and subpoenas in order to preserve the data and compel collection.

At this point, a quick note on data ownership is necessary. When you put your data in the cloud, you assume you still own that data. In most cases that is true, but just in case, check the contract, service-level agreement (SLA), and terms of service (ToS). Remember, there are two types of data: content, which in most cases you still do own, and meta data or data about data, which in many cases the provider owns and controls. You may be able to easily collect content, but it is the meta data you may need, and it is the meta data that is likely the toughest to obtain for many reasons.

Which Jurisdiction Applies?

In most instances the corporate structure of the cloud provider can be complicated. The headquarters may be located in one state and the servers may be located in one or more separate jurisdictions. One or more of its servers may even be located overseas. Therefore, the question, "Where's my data?" may not be an easy one to answer. If your data is truly scattered across numerous servers, how do you determine which jurisdiction applies (e.g., which state court do you rely on to issue subpoenas, file a civil suit, etc.)?[7] Your initial thought may be to determine where your data is stored and utilize that jurisdiction. However, this may be a daunting task since your data could be scattered across multiple servers across multiple jurisdictions at any given time.[8]

The simplest answer to the jurisdiction question is to look to the state of incorporation or headquarters for the cloud provider. Currently, there is no right answer, but this is probably the best, and the alternative(s) may be too cumbersome. For many providers—at least the big ones—an address and sometimes procedures for serving a subpoena are on its web site, although this may still leave the question of jurisdiction unanswered.

Can You Compel the Disclosure of Data?

If necessary, how do you compel your provider to gather and turn over data to you? If you believe the provider is going to give you access to its servers to dig around and figure out what you need to collect, you will be sadly mistaken. If your SLA or contract allowed for access, it would be relatively easy, and making this happen will be discussed later. In most cases, you will not have access to the provider's server(s), and it's a pretty good bet your provider will not simply say, "Tell us what you need, and we will provide it immediately."

This leaves you with at least two options: **negotiating** for what you want in the event of an incident prior to signing a contract with a provider, and, if that's not an option, attempting to **compel** the provider, via legal wrangling, subpoenas, and other tools, to give you what you need. Negotiating contracts and SLAs, which will be covered at the end of this paper, is still possible at this stage, although remotely. Once the provider is notified about the incident and provided a preservation letter or litigation hold, attempt to negotiate for the data needed. Depending on how big the provider is and how big your company is, you may have some leverage if you threaten to move all your business elsewhere.

What Tools and Techniques Are Available for Compelling Information?

Preservation Letters and Litigation Holds

Once you determine your cloud provider and the location of its headquarters or state of incorporation, immediately issue a preservation letter or litigation hold. A litigation hold "is a temporary suspension of the company's document retention destruction policies for the documents that may be relevant to a lawsuit or that are reasonably anticipated to be relevant." This can also be used to induce the provider to begin collecting data normally destroyed on a monthly, weekly, or even daily basis. A company must preserve data or evidence when it has notice or reason to believe that the data or evidence is relevant to litigation or should have known that the data or evidence may be relevant to potential litigation.[10] The litigation hold or preservation letter provides that necessary notice.

When issuing the letter or hold, it is very important to attempt to define, in as much specificity as possible, the data or information you are seeking and in what form or format, that is "its original format." A provider, to make its own life easier, may just copy the data to a drive or other storage unit and provide it to you. The format you receive it in may not be the original format, and you will not likely receive a chain of custody or documents describing the particular collection techniques used unless you dictate what you are looking for and how.

Federal Rules of Civil Procedures and Subpoenas

Assuming you were able to request or compel the provider to preserve data, but you have not been successful in compelling cooperation in collecting data, the following Federal Rules of Civil Procedure (FRCP) and subpoenas may be applicable and some of the few tools available in our scenario. Remember, in this scenario your focus is not criminal prosecution.

FRCP Rule 34 allows you to submit a request to preserve data and may even allow you to collect and inspect data. FRCP Rule 45 allows you to specify in a subpoena the form or forms for collection of electronically stored information (ESI). However, FRCP Rules 26 and 37 could play against your efforts by limiting what the provider must produce and what is considered reasonable at the time. These rules are briefly summarized below.

Each state uses its own rules of civil procedure, and many were crafted after the FRCP. So in many jurisdictions, rules may be similar. As practitioners from many different jurisdictions are likely to read this paper, we will focus on the FRCP. Also, in the interest of brevity, this paper will not delve into whether you should use state or federal rules. Suffice it to say, if you can cleanly claim all interested parties and information are within your state jurisdiction, then lean toward state civil procedure rules, although many other factors should be reviewed as well.

Per FRCP Rule 34, one party may request from another who is in possession or control of cloud data that the holder "produce and/[or] permit the requesting party or its representative to inspect, copy, test, or sample the… items in the responding party's possession, custody, or control."[11]

Assuming your litigation hold or preservation letter was followed and effective, this rule could enable you to see and/or collect exactly what you need or, at the very least, request the information from the provider.

FRCP Rule 34(b)(2)(E), titled "Producing the Documents or Electronically Stored Information (ESI)," specifically states:

> Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
>
> (i) A party must produce documents as they are kept in **the usual course of business** or must organize and label them to correspond to the categories in the request;
>
> (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms….

FRCP Rule 45 (a)(1)(C), titled "Combining or Separating a Command to Produce or to Permit Inspection; Specifying the Form for Electronically Stored Information," states:

> A command to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises may be included in a subpoena…or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced.
>
> (a)(3) Issued by Whom. The clerk must issue a subpoena, signed but otherwise in blank, to a party who requests it. That party must complete it before service. An attorney also may issue and sign a subpoena as an officer of:
>
> (A) A court in which the attorney is authorized to practice….

Now, before you get too excited, let's take a look at FRCP Rules 26 and 37.

FRCP Rule 26(b)(2)(B), titled "Specific Limitations on Electronically Stored Information (ESI)," states:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Finally, FRCP 37(e) states that a party may be relieved of its duty to preserve if the data is "lost as a result of the routine, good faith operation of an electronic information system."

All is not lost though. Forensics requires a lot of out-of-the-box thinking, just as much of cybersecurity does. For instance, cloud providers keep much data for billing purposes, and this data can be very valuable. "Cloud providers likely retain information regarding when resources are provisioned and de-provisioned for billing purposes."[12]

Can You Prepare for Cloud Forensics?

The key to avoiding much of this pain is being prepared before an incident occurs. So, how do you accomplish this? Negotiate the SLA or contract and its terms before you sign on the dotted line. Once you become a customer, you have lost much of your leverage. Some of the things you should consider negotiating:

- The provider will notify you immediately or within 24 hours if there is any type of breach or compromise or if one is even suspected on the provider's system since it may impact your data.
- The provider will allow you to access to the servers or system so you can self-collect.
- Determine what type of data the provider collects, how long the provider holds it, and if the provider will store this data for you for a longer period of time.
- Determine if the provider actually owns and controls the servers.
- Write a business continuity/disaster recovery plan. In it, include the necessary procedures and contact information for those to call if an incident occurs. Also, try to determine in advance either the data or type of data you will need for a forensic investigation. This may require talking to companies that have been through a breach or contacting a forensic investigator to help you determine what you will need to collect. Once you have identified the data, negotiate into the contract the ability to access this data or to have the provider preserve it, collect it for you, and provide a chain of custody as well as detailed procedures regarding how they did it.
- Determine where—in what state, states, or country—your data will be stored so you can determine which laws may apply.

These tips and issues are obviously not exhaustive, but they should provide a good start.

Conclusion

Preparation is the key to success. Negotiating the SLA or contract ahead of time enables you to react quickly and easily when and if things go bad—similar to establishing a disaster recovery and business continuity plan. If you were not prepared, which I am sure was a result of circumstances completely out of your control, the above tips should be helpful.

Footnotes

[1] Mell, P., & Grance, T., Definition of Cloud Computing: NIST Special Publication 800-1, (2011) at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Hereinafter NIST.

[2] On-demand self-service in the cloud context refers to the customer being able to add and delete services as he/she sees fit, quickly and easily. Techopedia at https://www.techopedia.com/definition/27915/on-demand-self-service.

[3] Rapid elasticity is the ability to scale or add and remove resources both up and down as needed. Cloud Computing Glossary at http://cloudglossary.com/home/id.Rapid-Elasticity/i.html.

[4] Location independence, just as the name conveys, allows the customer to be anywhere in the world where he/she has access to an Internet connection and access his or her cloud services, e.g., office, storage, etc. ReliScore.com at http://reliscore.com/blog/cloud-computing-the-very-basics/.

[5] Data replication involves sharing information to ensure consistency between redundant resources, such as software or hardware components, to improve reliability, fault-tolerance, or accessibility. Wikipedia at https://en.wikipedia.org/wiki/Data_replication. See NIST at Note 2.

[6] You might wonder why a company may not know who is holding its data. If your company is very large, there may have been personnel turnovers in the IT department, you may have been using the cloud for a while and don't remember who the provider is, or at some point changed providers over the years. Additionally, the cloud provider company could have changed hands. There are numerous scenarios that could all contribute to a lack of knowledge of your company's current computing architecture.

[7] The Privacy Commissioner of Canada has noted, "By its very nature, cloud computing has the possibility of sending, storing, and processing data in multiple jurisdictions…." Office of the Privacy Commissioner of Canada, Reaching for the Cloud(s): Privacy Issues related to Cloud Computing (March 2010), http://priv.gc.ca/information/pub/cc_201003_e.cfm.

[8] For some of the smaller companies, location may be easy, e.g., a handful of servers in one location. For the larger companies, there are likely servers located in multiple jurisdictions and your data may not be on just one of those servers but scattered over many in order to create redundancy, protection, backup, and economy of scale. See, Dexter Duncan, Xingchen Chu, Christian Vecchiola, and Rajkumar Buyya, "The Structure of the New IT Frontier: Cloud Computing – Part I," Cloud Computing and Distributed Systems (CLOUDS) Laboratory Department of Computer Science and Software Engineering, The University of Melbourne, Australia, accessed Feb. 15, 2013, at http://www.buyya.com/papers/AnekaMagazineArticle1.pdf.

[9] USLegal.com Definitions, http://definitions.uslegal.com/l/litigation-hold/.

[10] Zubulake v. UBS Warburg, 220 F.R.D. 212, at 216 (S.D.N.Y. 2003).

[11] Forsheit, Tanya, "Legal Implications of Cloud Computing — Part Four (E-Discovery and Digital Evidence)," Information Law Group, (November 27, 2009), http://www.infolawgroup.com/2009/11/articles/cloud-computing-1/legal-implications-of-cloud-computing-part-four-ediscovery-and-digital-evidence/.

[12] Josiah Dykstra and Damien Riehl, "Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing," XIX Rich. J. L. & Tech. 1, available at:

http://jolt.richmond.edu/wordpress/index.php/2012/11/forensic-collection-of-electronic-evidence-from-infrastructure-as-a-service-cloud-computing/.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, Global Knowledge suggests the following courses:

- Cybersecurity Investigations and Network Forensics Analysis: Practical Techniques for Analyzing Suspicious Network Traffic
- Cloud Essentials
- Virtualized Data Center and Cloud Infrastructure Planning and Design
- Foundstone Forensics & Incident Response
- RSA NetWitness Forensics Fundamentals
- CSFI: Defensive Cyber Operations Engineer (DCOE)
- CompTIA Advanced Security Practitioner (CASP) Prep Course

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

David Willson is a licensed attorney in NY, CT, and CO, and a leading authority in cybersecurity and the law. He is the owner of Titan Info Security Group, LLC, a risk management and cybersecurity law firm focused on technology and the law, helping companies lower the risk of a cyber incident, and reducing or eliminating the liability associated with loss or theft of information. He also assists companies with difficult legal/cybersecurity issues. David is a retired Army JAG officer. During his 20 years in the Army, he provided legal advice in computer network operations, information security, and international law to the DoD and NSA, and he was the legal advisor for what is now CYBERCOM. He has published many articles, including "Hacking Back in Self-Defense: Is It Legal; Should It Be?" and the recent "Cyber War or Cyber Cold War?" He is an active speaker at engagements, including ICCS, RSA, CSI, HTCIA, ISSA, FBC, Conference on Cybercrime and International Criminal Cooperation in Australia, Cornerstones of Trust, FISSEA, and ASIS. He holds CISSP and Security+ certifications and has two LLMs—one in international law and one in intellectual property law. He is a VP of his local ISSA chapter and a member of InfraGard.