UNITED STATES DISTRICT COURT

FOR THE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

)

)

) Case No.

)

)

)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

**APPLICATION OF THE UNITED STATES**

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

I, [NAME], 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 [DATA REQUESTED] that are stored at premises owned, maintained, controlled, or operated by [CLOUD PROVIDER] (the “Provider”), a web services company headquartered [CLOUD PROVIDER ADDRESS] (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 [STATUES] to require the Provider to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the web site.
2. [EXPLAIN POSITION AND QUALIFICATIONS OF APPLICANT]
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**

1. [DESCRIBE PROBABLE CAUSE]

**TECHNICAL BACKGROUND**

1. Based on my training and experience, I use the following technical terms in this Affidavit and Attachments A and B to this Affidavit:
   1. “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.
   2. “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.
      1. “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).
      2. “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.
      3. “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.
   3. “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

* 1. “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.
  2. “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.

1. The Provider is an IaaS Cloud Service Provider that 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. [INSERT ADDITIONAL DETAILS AS NECESSARY]
2. [DESCRIBE HOW CONSUMERS OF CLOUD SERVICES SIGN UP FOR AN ACCOUNT]
3. [DESCRIBE SPECIFIC SERVICES OFFERED BY THE PROVIDER]
4. [EXAMPLE: The Provider allows its users the ability to purchase computing resources on their cloud. This cloud 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. Users are billed based on the type of VM they choose, and the number of hours that the VM is running.]
5. [DESCRIBE HOW AND WHERE THE PROVIDER STORES DATA IN THE CLOUD]
6. Cloud Service Providers 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).
7. Therefore, the computers of the Provider are likely to contain all the material just described, including user-created content, stored electronic communications, and information concerning subscribers and their use of the cloud service(s), such as account access information, transaction information, and account application.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

1. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular [LIST STATUES VIOLATED], by using the warrant to require the Provider 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.
2. 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 the Provider, 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 the Provider, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:
   1. 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.
   2. 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 datacenters 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.
   3. [INSERT DETAILS RELATED TO THE CRIME]
3. In this case, the warrant application requests permission to search and seize [REQUESTED DATA], including those data that may be stored on a virtual machine. These things constitute both evidence of crime and contraband.
4. [EXAMPLE ADDITIONAL DATA: 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.]
5. 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.
6. 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:
   1. 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.
   2. 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.
7. The information requested should be readily accessible to the Provider by computer search, and its production should not prove to be burdensome.
8. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular [LIST STATUES VIOLATED], by using the warrant to require the Provider 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**

1. 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 the Provider there exists evidence of a crime, contraband, and fruits of a crime. Accordingly, a search warrant is requested.
2. 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).
3. 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,

[AGENT NAME]

[AGENT TITLE]

[AGENT EMPLOYER]

Subscribed and sworn to before me on \_\_\_\_\_\_\_\_\_\_\_:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to [DATA REQUESTED] that is hosted at premises owned, maintained, controlled, or operated by [CLOUD PROVIDER], a company headquartered at [CLOUD PROVIDER ADDRESS].

**ATTACHMENT B**

**Property to Be Searched**

1. **Information to be disclosed by [CLOUD PROVIDER]**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, the Provider is required to disclose the following information to the government for the IP address listed in Attachment A:

1. 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;
2. IP logs, including all records of the IP addresses that logged into the accounts associated with the IP address;
3. Firewall, router, and intrusion detection logs associated with the IP address;
4. 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).
5. **Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of [STATUES VIOLATED], including information pertaining to the following matters:

1. The virtual machine assigned to the IP address in question on [DATE OF CRIME];
2. A list of other IP addresses assigned to the virtual machine in question, and the dates and times they were assigned;
3. Packet captures of traffic to and from the virtual machine in question;
4. Data stored in any other cloud service controlled by the Provider, associated with the account running the virtual machine;
5. Records relating to who created, used, or communicated with the virtual machine assigned to the IP address in question on [DATE OF CRIME].