CLOUD STORAGE & DIGITAL FORENSIC EVIDENCE

Understanding Misconceptions and Providing Answers

A look into cloud storage for digital forensic evidence management

Author: Christopher E. Collins,
Detective Sergeant
Lake Jackson Police Department

The Future of Digital Forensics

How Cloud Storage Is Revolutionizing the Digital Industry

Abstract:

How can we leverage cloud-based storage solutions for digital evidence in a laboratory setting and is it safe? Technology is forever evolving, and one fact remains, storage is a finite resource. There are plenty of factors that play into the decision of storage solutions from USB tethered devices, on-site data servers, and cloud-based solutions. Any storage solution that is implemented on-site will always have constant factors that must be accounted for, the end user will be responsible for implementation/installation, upkeep, maintenance, security, and transportation in the event of a natural disaster or emergency. In today's technology driven climate new milestones are being achieved every day with data storage on consumer grade electronics. Storing digital evidence in a forensic laboratory is on the cusp of approaching the point of criticality as storage mediums approach end of life cycles and new technology is developed. Considering cloud storage as a solution in a digital forensic laboratory carries several misconceptions and fears as this technology is not understood by some or its capabilities and security are unknown. This article will help to provide the reader with answers and solutions.

End user considerations for on-site storage systems:

- Initial set-up (wiring / equipment / configuration)
- Cost of maintenance
- Cost of upkeep
- Replacement parts/drives
- Cost of expansion drives
- Contingency / Action plans

How do cloud-based storage solutions compare to on-site solutions for the end user?

× Initial set-up (wiring / equipment / configuration)
× Cost of maintenance
× Cost of upkeep
× Replacement parts/drives
× Cost of expansion drives
✓ Contingency / Action plans
✓ Yearly license fees (depending on product)
✓ Expand storage in the matter of seconds
✓ Data security
✓ Technical support
✓ Redundant back-ups
✓ Rigorous Federal Standards and Compliance

Table of Contents:

Introduction:

In the year 2000, the world saw an innovative storage device that was revolutionary in the market, the USB flash drive. The first USB drives had just 8 Megabytes of storage [1] and changed the storage front of technology. Today, USB drives still hold a valuable place in digital forensics as they're used for a multitude of purposes from portable data storage to being a vessel to launch operating systems and forensic software from. Another long-standing facet of digital storage has been the implementation of on-site data servers. Data servers have evolved through multiple phases of storage technologies from tape drives, magnetic disks, all the way to current generation solid state drives. The constant evolution of storage technology has changed data server builds throughout the last decade with the introduction of the solid-state and NVMe drives. Each iteration of storage drive technology that has evolved comes with an increased cost associated with it on the open market [2]. When considering on-site data storage, agencies must think about several factors to include storage drive lifespan, failure rates, external dangers associated with the storage type, backup/redundancy, physical vulnerability to environmental threats (flooding, fire, etc.), and more.

With the improvements made to storage technology throughout the years, it directly affects the digital forensics field, meaning that we must strive to be on par with the technology curve. Device storage specifically affects the field of data extraction and analysis as a direct relation to storage needs. Today, when an examiner completes the extraction of an Apple iPhone that has 1 terabyte of internal storage [3], they must be able to house the raw data extracted from that device which could be upwards of 900 gigabytes for that single extraction. Taking into account the parsed and compressed report file of the raw extraction, the report file size is approximately 50% or half of the raw extraction data file. All-in-all for the extraction and forensic analysis of a 1 terabyte Apple iPhone, they must allot approximately 1.4 terabytes for that single extraction. While not all devices processed in a forensic laboratory will be 1 terabyte in size, this is a metric that must be accounted for.

Reviewing computer storage drives, the average size of internal storage listed as "top selling" or "most reviewed" from several online retailers (Newegg, Best Buy, Office Depot, Dell, Staples, and Amazon) revealed that the average internal drive size sold is approximately 3tb, which would need the allotment of approximately 4.5tb of storage to house the complete extraction and report. As of March 2018, there is one solid-state storage drive from Nimbus Data that is commercially available, albeit expensive ($40,000 USD), with 100 terabytes of storage [4] this cost will plummet over time making it an affordable option in the future. A forensic extraction and report file for this drive could be 150-175 terabytes total. The need to increase evidence storage in a digital forensic laboratory is constantly growing.

Through this study, 3 digital forensic laboratories were polled for their device processing in a year. The Lake Jackson Police Department in Texas (2022), the Harris County District Attorney's Office Digital Forensics Unit in Texas (2021), and the Gulf Coast Technology Center in Alabama (2022). Combined all three laboratories logged in 2,151 mobile devices and 84 computers / hard drives, using a total of 109.2 terabytes of storage within the year denoted. The average across Lake Jackson and Gulf Coast Technology Center found that mobile device extractions and the associated report files contained approximately 72 gigabytes of data and computers / hard drives extracted contained approximately 1 terabyte of data, Harris County DFU did not track device extraction average sizes. In criminal law there are a myriad of outcomes & dispositions in court cases that can affect the need to maintain back-ups of digital evidence. Digital evidence is generally maintained for an indefinite period of time until a destruction or expungement order is received from the court.

Current Solutions for Digital Evidence Storage

USB Drives & Network Attached Storage

- Easily Portable
- Varying ranges of storage
- Higher chance of equipment failures
- Can be cost effective
- Ease of use and implementation
- Lower maintenance requirements
- Smaller size
- Not as forensically sound or secure

On-Site Data Server

- Physically large size for rack mounted storage
- High cost for implementation
- Monitoring for faults and failures required
- Advanced knowledge needed for set-up and operation
- Can be more secure
- Can be a forensically sound environment
- Redundant backups can be implemented

Cloud Storage

- No major cost for set-up
- Off-site storage
- Data security maintained by provider
- Maintenance/Failures covered by provider
- Redundant back-ups by provider
- Highly portable as it’s web based
- No advanced knowledge needed
- Multiple Federal Compliance Regulations
- Forensically sound environment
- Infinite storage options

Survey Of Responses to Cloud Storage for Digital Evidence

In February 2023, a survey was conducted by reaching out to digital forensic professionals in both Law Enforcement and the private sector on their thoughts involving the inclusion of cloud-based storage solutions for storing digital evidence. 58 responses were received to a survey as of May 5, 2023, and the complete responses can be found here [5]:

https://www.surveymonkey.com/results/SM-1xotQQ_2By5L2MoKyENUyxWA_3D_3D/

This survey indicated that 81% of the respondents answered that their agency or company have not implemented any form of cloud-based storage solutions, while 19% responded to the affirmative. This question allowed the respondents to expound on the simple yes/no question based and found that several of the “No” answers have in fact implemented cloud solutions partially into their systems. In this open field the responses indicated that while cloud solutions were used for temporary storage or data collaboration, this was not the main focus of their cloud usage.

To gauge what on-site solutions were being used in general, the survey opened the answer to allow for multiple selections of the following:

- USB Devices (Thumb Drives/External Hard Drives)
- Network Attached Storage (NAS) / Local Storage
- Dedicated On-Site Server

Of the 58 respondents’ answers received indicated that 45% were using USB Devices, 50% were using a NAS or Local Array, and 48% were using Data Servers. A look further into the respondents with the multiple answers a majority indicated they were using USB Devices and NAS/Local Arrays for their storage, while a split minority used combinations of USB, or NAS/Local Array & Data Servers. Two respondents indicated that they were utilizing all 3 options in varying configurations. Two other outliers indicated that they were also utilizing CD/Optical discs and/or tape drives for storage.

In criminal cases we must account for retention periods, all evidence must be retained until the court reaches a final disposition, barring any appeals made later in Judge/Jury convictions, this evidence must be retained indefinitely. A question was posed to the respondents about their retention periods of the evidence and back-ups. Of these respondents there are a mixture of Law Enforcement and private sector specialists who answered that excluding any outside factors of court destruction orders or expungement orders, that the evidence is retained indefinitely. Beyond these factors the indicated responses showed that 14% retained evidence for 1-2 years, 22% answered 2-5 years, 29% answered 5+ years, and 34% indicated that data is housed indefinitely.

With common misconceptions and fear in the area of cloud storage, the survey aimed to ascertain what were some of the major apprehensions in this area with a multiple-choice answer. The biggest issue identified by respondents (74%) was data transfer speeds for upload and download of digital evidence to the cloud storage. The secondary major factors identified by respondents was the digital security of the cloud site (62%), followed by the cost differential for setting up local storage options (55%). Other issues identified was a question of evidence integrity when data is transferred, the physical security at the data storage site, and the legality of transferring evidence to the cloud storage such as Child Sex Abuse Materials (CSAM).

This survey sought to identify some of the qualities or assurances digital forensic specialists would like to see to solidify their trust in cloud storage. The majority of the respondents answered that redundant data back-ups on the cloud storage provider would be a good trust builder (69%). This can be achieved by communicating the storage and security architecture to potential customers by the provider. Other factors identified to build trust would be dedicated end-to-end encryption connection, and the presence and documentation of Federal regulation and compliance standards being met.

When taking a marketing approach to presenting cloud-based storage as an option, respondents stated that they would take the use of and endorsement by Federal Law Enforcement Agencies as an outlet they can trust with 71% placing trust in them. The respondents further indicated through this survey that other trustworthy sources they would consider is the use of or endorsement by Military Services (52%), State/Local Law Enforcement (48%), and Industry Experts (44%).

The respondents were asked if they took issue with any single cloud storage provider, none of the respondents identified a single provider as untrustworthy or a basis of cloud storage concerns. When given the example of Amazon Web Services' GovCloud as a platform to trust, as they have multiple Federal regulation and compliance standards they adhere to, 47% of the respondents indicated that they trust AWS GovCloud or any other cloud storage provider with the same set of Federal regulation and compliance standards as AWS GovCloud, 10% replied that they do not trust AWS GovCloud or others on the same field, and 43% identified this as a non-factor in their decision for cloud storage trust.

The respondents were given a 1-10 scale of how open they are to adopting cloud storage as a primary solution for digital evidence. The ratings were across the board and 44% of the respondents chose ratings 1-5, while 56% chose 6-10.

Of these respondents 55% identified as being associated with Local/Municipal Law Enforcement, 24% State Law Enforcement, 12% Federal Law Enforcement, 5% Private Sector, and 3% as “Other”.

Federal Regulations on Cloud Storage Solutions

In relation to standards set forth within the United States of America, many Law Enforcement agencies are faced with adhering to multiple standards on the federal level for data security and protection of the electronic data. Here are several standards that Law Enforcement and other entities must adhere to that are supplied by cloud storage solutions using AWS GovCloud as an example [6]:

Criminal Justice Information Security (CJIS) - Federal Bureau of Investigation / Department of Justice:

Multiple security controls are required to maintain CJIS compliance. One of the cornerstones of maintaining compliance is "need to know / right to know" standards of control. This principle of least privilege is enforced by services such as AWS GovCloud by the use of encryption keys and key management that is validated under FIPS compliance 140-2. AWS GovCloud meets CJIS compliance with "at-rest" digital data encryption that is validated under FIPS 197 using AES 256-bit encryption. CJIS standards for "data in transit" are covered by AWS GovCloud's use of FIPS 140-2 Application Programming Interface (API) when uploading and downloading data. There is no central repository for CJIS compliance and must be individually identified for the use of such storage. When using programs such as AWS GovCloud the Law Enforcement agency must show these aforementioned standards and document that access to the cloud stored data is deemed as "escorted access". The term escorted access means that an employee of AWS does not have access to the data housed, which they do not, and in the event of technical support, the technician will be escorted via remote access from the agency's own computer accompanied by an end user.

Federal Information Processing Standards (FIPS):

These standards are documented in publications and validations made by the National Institute of Standards and Technology (NIST). FIPS compliance in the AWS GovCloud realm as previously mentioned is covered by FIPS 140-2 validation for their encryption key management and software applications. For data housed on AWS GovCloud servers the FIPS 197 standard is used to validate their encryption protocols utilizing AES 256-bit encryption.

National Institute of Standards and Technology (NIST):

NIST provides cyber security controls and security templates for FIPS and FedRAMP. NIST addresses the compliance requirements and security standards under NIST SP 800-53 (Rev. 4), and SP 800-171. NIST also provides their Cybersecurity Framework (CSF) whitepaper as an assessment of the security environment to help improve security measures.

Federal Risk and Authorization Management Program (FedRAMP):

Cloud service providers who seek to do business with the US government must demonstrate FedRAMP compliance under the NIST 800 series of publications which also covers FIPS compliance. As you can see the federal regulations are building blocks for information and data security, often relying on each other for cross platform security standards.

Department of Defense Cloud Computing Security Requirements Guide (DoD SRG):

Provides a standardized assessment and authorization process for cloud service providers (CSPs) to gain a DoD provisional authorization, so that they can serve DoD customers. The AWS provisional authorization from the Defense Information Systems Agency (DISA) provides a reusable certification that attests to AWS compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation in AWS. DoD SRG assesses the cloud storage provider and issues Impact Levels (IL) from 1-6. IL1 is the lowest classification for uncontrolled documents while IL6 is for documents or data marked "Secret".

Federal Information Security Management Act (FISMA):

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (DIACAP).

Health Insurance Portability and Accountability Act of 1996 (HIPAA):

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use the secure AWS environment to process, maintain, and store protected health information.

	CJIS	DoD SRG	FedRAMP	FIPS	FISMA	HIPAA	NIST
AWS GovCloud	✓	IL5	✓	✓	✓	✓	✓
Google Cloud	✓	IL4	✓	✓	✓	✓	✓
IBM Cloud	✓	IL2	✓	✓	✓	✓	✓
Microsoft Azure	✓	IL6	✓	✓	✓	✓	✓
Oracle Cloud	✓	IL5	✓	✓	✓	✓	✓

*There are currently no certificates of compliance for CJIS and HIPAA, as these standards are left up to the end user to maintain compliance, these cloud service providers adhere to the standards set forth by CJIS and HIPAA.

Which Cloud Storage Solution Are Used by State

This document is based around cloud storage solutions in general, but depending on the location of the laboratory, there may be restrictions or suggestions for a particular vendor of cloud services. Listed below are the services either recommended or used by individual State Information Technology Departments:

Alabama NSP: Fed. Compliance*	**Indiana** NSP: Fed. Compliance	**Nebraska** NSP: Fed. Compliance*	**South Carolina** *Unclear*****
Alaska Azure	**Iowa** AWS	**Nevada** NSP: Fed. Compliance	**South Dakota** NSP: Fed. Compliance*
Arizona AWS / Azure / GCP	**Kansas** NSP: No personal storage	**New Hampshire** *Unclear* / Azure*	**Tennessee** No Information Available
Arkansas *Unclear******	**Kentucky** NSP: Fed. Compliance	**New Jersey** NSP: Security on End User	**Texas** NSP: Fed. Compliance
California AWS / Azure / IBM / OCI	**Louisiana** AWS	**New Mexico** No Information Available	**Utah** NSP: Fed. Compliance
Colorado AWS	**Maine** NSP: Fed. Compliance	**New York** NSP: Fed. Compliance	**Vermont** NSP: Fed. Compliance
Connecticut AWS / Azure	**Maryland** NSP: Fed. Compliance	**North Carolina** NSP: Fed. Compliance	**Virginia** NSP: Fed. Compliance
Delaware NSP: Fed. Compliance	**Massachusetts** NSP: Fed. Compliance	**North Dakota** No State Policy	**Washington** NSP: Security on End User
Florida NSP: Fed. Compliance	**Michigan** NSP: Fed. Compliance	**Ohio** NSP: Fed. Compliance	**West Virginia** NSP: Fed. Compliance***
Georgia NSP: Fed. Compliance	**Minnesota** NSP: Fed. Compliance	**Oklahoma** Azure	**Wisconsin** NSP: Security on End User
Hawaii NSP: Fed. Compliance***	**Mississippi** *Unclear**	**Oregon** NSP: Fed. Compliance	**Wyoming** Azure / GCP
Idaho NSP: Fed. Compliance	**Missouri** NSP / State can provide	**Pennsylvania** NSP: Fed. Compliance	
Illinois NSP: Fed. Compliance	**Montana** No Information Available	**Rhode Island** NSP: Fed. Compliance	

-For state specific sources, see "Further Reading" section at the end of this document.

Abbreviations / Vendors:

AWS - Amazon Web Services

IBM - International Business Machines

OCI - Oracle Cloud Infrastructure

GCP - Google Cloud Platform

Azure - Microsoft Cloud

NSP - No Specified Provider

Fed. Compliance - (CJIS/DoD/FedRAMP/FIPS/FISMA/HIPAA/NIST)

"Personal Storage" - Dropbox/iCloud consumer level services

* - State IT Department may have to approve CSP.

** - May have to use/acquire State IT Dept. cloud services.

*** - Legislation pending in 2023 for adoption.

Local Server Failure & Cloud Migration

Real World Event: The Southern Virginia ICAC Task Force's Local Server Failure

The Southern Virginia Internet Crimes Against Children Task Force Headquarters (SOVA ICAC) is charged with fielding cases involving some of the most sensitive types of evidence, digital media depicting children being sexually exploited and abused (CSAM). Around 2015 SOVA ICAC began upgrading their local data storage servers, utilizing two on-site rack mounted servers with a total of 1 petabyte of storage available.

In April 2018 the SOVA ICAC data servers experienced a critical error reducing the data server from 1 petabyte to approximately 3 gigabytes which is less than a fraction of a percent of the original storage space (0.0003%). SOVA ICAC found that a configuration error caused this failure in the system as the IT contractor who configured the server did not enable deleted data to be overwritten. Due to the server failure, SOVA ICAC was not able to recover a majority of the case files and digital evidence from cases taken in 1998 through 2013 along with a large comparative image library SOVA ICAC collected over the years. The data recovery process took around 4 years to complete, and the unrecoverable data is unfortunately lost forever. This failure prompted SOVA ICAC to implement an off-site redundant back-up server that had to match the original server specifications. Between both on-site and off-site servers SOVA ICAC had to budget approximately $1,000,000 for the purchase of hardware, outside IT contractors to install and configure the servers, maintenance costs, and location rental for the off-site servers. One of the challenges faced by SOVA ICAC is since their Task Force office is comprised of multiple different agencies they do not fall under a singular agency or department to provide an IT infrastructure. This means that they do not have the support available to them from an established IT department to manage any of the backend networking, maintenance, or deployment of systems beyond their own work or hiring outside IT contractors. The hiring of outside IT contractors accounts for a large portion of the budget spent on these servers being installed and maintained over time.

As of April 2023, SOVA ICAC is using approximately 500 terabytes of storage out of the 1 petabyte available in their servers. The data housed on their local storage servers contains custom hash set lists, comparative image sets, case data, digital forensic evidence, etc. All of this data has been collected from around 2013 to 2023, which averages approximately 50 terabytes of data being retained per year. To assist in processing large data extractions from digital devices, SOVA ICAC deployed a digital forensic workstation in their laboratory that has 1 petabyte of storage at a cost of $250,000 to implement. Across the State of Virginia in their satellite ICAC offices they have 3 more of these 1-petabyte workstations in use for a total investment of $1,000,000.

Through the upgrade, installation, maintenance, and location rental for the servers SOVA ICAC currently has, along with the 1 petabyte digital forensic workstations, the total budget allocated is around $2,000,000. This is the upfront cost and does not factor in equipment replacement for lifespan cycles or failures and this figure is subject to change as time goes on due to equipment availability, and new technology.

Moving forward SOVA ICAC is taking the steps to migrate their storage to a cloud-based system on the Microsoft Azure cloud platform. In this move they have joined forces with a cloud management provider to establish management for their cloud storage and system needs. With SOVA ICAC's new cloud management program, they are taking multiple steps to secure this sensitive data through hardening initiatives such as physical security to access computer systems, an active geofence at their headquarters requiring the user to be on site to access their cloud storage, and multiple layers of two factor authentication to access live data and back-up data stored in their cloud. One of the two factor authentication programs used is if data is requested from the cloud storage, the cloud management provider will contact an on-duty supervisor with SOVA ICAC to request permission to release this data to the requestor. The cloud management provider is established to have no direct access to the unencrypted data stored but does have access to release the data as requested, given that the security conditions are met. To ensure data is perpetually backed-up the cloud management provider conducts encrypted back-ups of the data stored once a day, one weekly back-up, and one monthly back-up, which are stored in separate locations to ensure redundancy and data security. The cloud management provider SOVA ICAC has joined with holds their employees to the highest standards as they have Top Secret clearances through the United States government.

To start, SOVA ICAC will be securing 1 petabyte of storage within Microsoft Azure to migrate their current storage over and will have the ability to move older data to cold storage. All-in-all SOVA ICAC is looking at a yearly cost of the cloud storage and managed service provider coming in around $20,000 per year, and when compared to the $2,000,000 spent on local data servers and systems that must be maintained with ongoing costs and the potential for failure, it would take 100 years of the yearly fee to match the $2,000,000 price tag of local storage. Of the 1 petabyte of cloud storage secured, SOVA ICAC Task Force Officers will be provided with encrypted virtual hard drives for individual storage.

What are the future plans for SOVA ICAC's new cloud initiative? SOVA ICAC is planning on moving some of their evidence processing to the cloud to offset the cost for continual replacement of digital forensic workstations. SOVA ICAC is looking to implement multiple virtual machines to process digital devices, this means that they are utilizing the cloud service provider's hardware to run digital forensic processing software to conduct device extractions and analyzing the evidence. By using the cloud service provider's hardware to conduct digital forensic examinations they no longer need to purchase multiple expensive digital forensic workstations, all of which can be done on standard desktop computers through a virtual machine program. SOVA ICAC will be working with their cloud management provider to make this available to any ICAC affiliate across the United States at a minimal shared cost, where the only additional cost is for the amount cloud storage they request. An affiliate agency will be offered the same security standards as SOVA ICAC has in place for their own storage allotment through Microsoft Azure. If an affiliate agency chooses to participate, they would be given a separate instance of storage, meaning that no one but the affiliate agency will have access to the data they store.

The steps SOVA ICAC are taking are groundbreaking in the digital forensics field and they are leading the charge in cloud migration, setting an example for agencies across the nation to follow.

Flash Memory - USB "thumb" drives and Solid-State Drives

It is important to provide a brief explanation of flash storage technology used today. Consumer grade flash memory drives use NAND flash memory which is a type of non-volatile memory that allows for data to be stored on the drive and retain that data while not powered. NAND flash memory has evolved through multiple different technologies throughout the years that directly correlate with how many times they may be reused. The flash memory technologies are defined as Single-Level Cell (SLC), Multi-Level Cell (MLC), Triple-Level Cell (TLC), and so on. The way in which flash memory technology is categorized is by how much data in "bits" can be stored in a single cell of the flash memory. SLC allows for 1 bit to be stored per cell, MLC allows for 2 bits, and the classification continues through TLC for 3 bits per cell and so on. These levels can also calculate how many times a cell can have data stored on it, erased and new data to be written on it, this is called Program and Erase cycles (P/E cycles). SLC being the most robust as it allows for up to 100,000 P/E cycles, or times a cell can be written onto and erased. MLC reduces the P/E cycles to 10,000, and TLC down to 3,000 [7]. To put this into a basic perspective, if you have a 1gb flash drive with TLC NAND technology, and a 1gb file, that 1gb file can only be written to the drive approximately 3,000 times before the drive fails. Flash memory is susceptible to electrical damage through power surges that can damage the chipset, or in the case of "thumb" drives loss or physical damage.

Researchers Bianca Schroeder of the University of Toronto, Raghav Lagisetty and Arif Merchant from Google Inc. published a research document titled: *"Flash Reliability in Production: The Expected and the Unexpected"*. In this research, they documented flash memory reliability over 4 years and found that there was no evidence to support that SLC drives were "more reliable" than MLC drives or other NAND technology. This research concluded that flash drives have a significantly lower rate of replacement in the field but did encounter a higher rate of uncorrectable errors when compared to traditional hard disk drives with spinning magnetic disk platters. Out of the 4-year study the researchers found that between 20-63% of the drives encountered at least one uncorrectable error, and 2-7% developed bad blocks, if multiple bad blocks develop it would require that the drive undergo significant repair or replacement. [8]

Hard Disk Drives

When looking at how hard disk drives work, there are many components to analyze such as the hardware chips, motor to spin the disk platters and the access arm. These HDDs operate similar to a record player, as the disk spins the access arm reads the data on the disk through the magnetic charge that is on the disk. While flash memory holds the data inside the chipset, the HDD disk holds the data on the disk platter through the magnetic charge. These disks are housed within a unit that offers little to no magnetic shielding making this a potential point of failure if a strong enough magnetic field is present near the HDD. Another point of failure can be identified through mechanical failure, the motor that spins the disks, or the access arm movement, thus rendering the drive useless without significant repair, if at all possible. In a study conducted by Backblaze, a digital data storage company, found that in 2022, out of 230,921 drives they documented a 1.39% annualized failure rate for their hard disk drives (12,768 drive failures). [9]

How Much Does Local Storage Cost?

With the outlined issues of local storage being a finite resource, and the growing storage capabilities of consumer grade electronics, it begs the question, where can the digital evidence be stored? While there are solutions for local storage options, cloud storage solutions are paving the way for the future in digital forensics.

Exploring local storage options, one can look into several solutions and below are average costs outlined associated with implementing these solutions and ongoing cost of maintenance and upkeep.

**All prices listed in this document are current as of May 2023.*

USB Based Devices:

Keep in mind that generally when placing evidence onto a USB drive it is a “one and done” instance since that drive will be placed into evidence on a case and is locked in until the case disposition. Another factor to consider is the transfer speeds that limit data transfer to USB drives, large data sets can take several hours to move to a drive. In the event that data must be moved in an emergency, all of these data drives must be collected and moved, which presents a problem as they are small and susceptible to damage and loss.

Flash/Thumb Drive - Storage sizes 8gb-1tb

Price Averages (Reputable Manufacturers):

8gb / 16gb - $7.00/ea.

32gb / 64gb - $18.00/ea.

128gb / 256gb - $23.00/ea.

512gb - $50.00/ea.

1tb - $130.00/ea.

Shelf Life: 10 years (depending on usage, P/E cycles, and multiple outside factors)

Pricing Example:

100 total cases with evidence in a year with a mixture of drives needed for evidence submission would be an average of $2,000/yr. for evidence drive submissions alone.

USB Based Devices (continued):

External Hard Disk Drives - 1tb-22tb

Price Averages:

1tb - $55/ea.

5tb - $120/ea.

10tb - $180/ea.

16tb - $280/ea.

22tb - $630/ea.

Shelf Life: 3-5 years (susceptible to external magnetic interference and equipment failures)

These drives would be used for large evidence data sets that exceed “thumb drives”, or for back-up and long-term storage and still would need a medium to transfer the data into evidence.

Network Attached Storage (NAS):

A NAS is a housing unit that allows for multiple hard drives to be placed inside and will collectively pool all of the storage as one, for example 5 - 20tb hard drives will be combined as one storage location with 100tb available depending on configuration. This storage option offers faster transfer speeds than USB but must be configured properly as it is using a network location to connect to a computer/workstation and does not work off of a standard operating system such as Windows. A NAS is a physical box that must be moved in the event of an emergency and must be secured on a network to prohibit unauthorized access from other legitimate users within the network and outside intrusion. NAS units are classified by “Bays” and each bay is capable of holding 1 hard drive for storage. In the event you wish to expand storage or upgrade the drives within a NAS, all of the data must be removed from the drives, housed in another data storage location, and the NAS must be upgraded and “rebuilt” before placing the data back on the drives within the NAS.

Price Averages: (Excluding Hard Drives)

4-Bay NAS - $800 (w/ 10tb HDDs add +$800)

6-Bay NAS - $900 (w/ 10tb HDDs add +$1,200)

8-Bay NAS - $1,050 (w/ 10tb HDDs add +$1,600)

12-Bay NAS - $2,500 (w/ 10tb HDDs add +$2,400)

16-Bay NAS - $3,200 (w/ 10tb HDDs add +$3,200)

The hard disk drives that are optimal for a NAS are labeled as “NAS Drives” and cost more than a standard hard disk drive, 10tb NAS HDD - $200/ea. These drives would be used for back-up or long-term storage and still would need a medium to transfer the data into evidence.

On-site Data Server:

This local storage solution is the most intense as it would require a dedicated area or room to house the data server and is considered a Storage Area Network (SAN). There are several different types of “servers” to include workstations to rack mounted systems. Rack mounted storage solutions require the purchase of a server rack, a rack mounted computer, hard drive storage rack. After purchasing and installing these components, you have to choose an operating system that will be right for your application. Windows provides server class operating systems (OS) that cost substantially more than standard operating systems, or a Linux OS distribution may be considered as there are several free options available (these require Linux OS knowledge to establish and maintain). Once these options are selected, this solution would require a network connection and set-up similar to a NAS, cable management & installation but may require a network architecture overhaul depending on setup. To modify or change the storage drives presents the same issue as a NAS, as the data must be removed from the server and housed separately until the server storage array is rebuilt and reconfigured.

Price Averages (Rack Mounted):

Single Server Rack - $900

Rack Mounted Computer - $1,000

Rack Mounted Hard Drive Enclosure - (See NAS pricing as a guide)

Hard Drives - Can vary upon storage needs, baseline 10tb HDD - $200/ea.

Windows Server OS - $500

To implement a rack mounted server with 12 bays, 12x 10tb HDDs, and Windows Server OS would cost approximately $7,000, for the server alone, not including any installation, network changes or configurations.

SUMURI TALINO:

SUMURI’s TALINO systems offer several server-class workstations and full-sized servers that can be configured to the user’s specifications. Below is a list of their base server options available on their website.

Nano Server - $9,000 (24tb of raw storage and up to 10 drives total)

Super Server - $15,000 (160tb of raw storage and up to 16 drives total)

Ultra Server - $18,000 (160tb of raw storage including more features than Super Server and up to 32 drives total)

Hyper Server - $160,000 (Rack mounted unit built to spec, Min. 1,440tb of raw storage, Max. 5,280tb of raw storage or more as needed)

Local Storage Costs Considerations:

A factor to consider when establishing a NAS or server is the configuration of the storage array. In the event of a hard drive fault or failure on a server with 12x 10tb HDDs (120tb total) and one drive fails, if not configured correctly you could lose some if not all of the data housed. If configured correctly it will require one or 2 installed drives dedicated to ensuring the entire storage pool is safe. In a properly configured storage array the 12x 10tb HDD used, only 10 or 11 of these drives will be useable as storage.

No matter the digital forensic laboratory's purpose being in Law Enforcement or in the private sector for corporate security, e-discovery, or civil litigation the laboratory must remain ahead of the curve in evidence storage needs. By leveraging and implementing cloud storage solutions for digital evidence it can be used to free up initial equipment investments, ongoing maintenance costs, physical & digital security needs, and the need for contingency plans on moving physical data storage devices in the event of an emergency. By placing the burden of maintaining the physical storage onto cloud storage providers, this will allow digital forensic laboratories to focus on their main function, the examination of digital evidence and documenting their findings. This goal may be achieved by implementing cloud storage solutions as a primary resource for storing digital evidence, or solely as a back-up solution for long term storage. Either solution will benefit a digital forensic laboratory.

Using cloud storage solutions or a Digital Evidence Management System (DEMS) that is built on secure cloud storage as the backbone, digital forensic laboratories can utilize these systems to house digital evidence via the cloud to remove these hurdles and enhance the laboratory's capabilities. As discussed, several cloud storage providers comply with multiple federal regulation standards that meet or exceed compliance needs. With these regulations put into place, utilizing cloud storage should be considered a viable option for Law Enforcement or private sector use. With the recent push for body worn cameras (BWC) to become mandatory for all Law Enforcement agencies across the United States, multiple companies have stepped up in preparation to provide BWC based digital evidence management and cloud storage as solutions. This has spawned a new market in evidence management, focusing on digital evidence storage in the cloud. This market has rapidly evolved to encompass digital evidence well beyond BWC video and now caters to CCTV footage, other digital media, and electronic documents, creating the new DEMS market.

One element identified as an issue with using cloud services as a laboratory's primary storage solution is that data may easily be sent to the cloud for archiving at a low cost, but retrieving that data comes with financial burdens and wait times to be able to retrieve that data. An option to consider as a digital forensic laboratory would be implementing cloud-based DEMS solution. DEMS would allow for the laboratory to park data under a case file, manage that data, collaborate with other interested parties such as multiple agencies/departments, prosecutor offices, legal discovery requirements, and track chain of custody through audit/access logs.

What Is the Cost of Implementing Cloud Storage?

When looking into cloud storage as a solution there are some costs to implement but pales in comparison to the implementation costs of local storage. For example, to establish AWS S3 services for data storage alone on a small scale would cost under $250/yr. This estimate was built to allow for the monthly upload of 500gb and downloading 100gb, with the average size of a single file of 100gb to cover the common size of a mobile device extraction. AWS S3 storage comes with its own inherent flaws as data retrieval may be time consuming and requires a wait period for the data to be made available and the increased cost of data retrieval versus uploading prices.

In the pricing breakdown collected for AWS S3 Glacier Instant Retrieval calculator indicates the cost for this type of service would be approximately $35/mo. at a yearly cost of $420. The calculations made for this service factored in a monthly upload to the cloud storage of 1tb and downloading 250gb, with the average file size of 100gb. This calculation doubles the amount of data to be moved under the AWS S3 standard service as previously quoted. With the S3 Glacier Instant Retrieval service the wait times to access stored data are vastly reduced with a minimal cost increase.

While other services would increase the price such as access to AWS GovCloud, you can see the difference in either $250/yr. or $420/yr. to $10,000 for initial set-up of local storage server, not factoring in maintenance or up-keep costs of that server. To take these numbers a step further the average life span of a hard disk drive and/or a workstation computer is around 3-5 years before needing maintenance and up-keep, which may require full replacement. The next page will explore operational costs by year for different solutions.

Applying cloud storage to a DEMS solution, the cost will inherently increase as these solutions add features beyond the mere storage of data. The current focus of DEMS is that of video footage and other forms of digital data including scanned documents, case reports and anything else within a digital medium. Very few DEMS solutions factor in the storage of large files, for example mobile device or computer extraction images stored in evidence. Currently DEMS solutions on the market today have a varied cost of around $5,000 to $15,000 per year. These DEMS solutions create an environment to store data and evidence and allow for that data and evidence to be shared across the spectrum to build collaborative efforts and track the audit/access logs. There are several DEMS solutions on the market today that utilize secure cloud storage solutions as their storage medium, providing security offered through the aforementioned federal compliance standards.

Operational Costs Analysis for Different Storage Solutions

USB-Based Devices:

USB flash drives for evidence:	$2,000/yr.
x1 USB hard drives for back-ups (5tb for multi-year storage):	$120/ea.
First Year Total:	$2,120
10 Year Total (including maintenance):	$21,800

<u>Issues:</u>

- The USB flash drives are committed to evidence once submitted.
- USB flash drives are small and fragile, susceptible to loss and damage.
- USB hard disk drives and flash drives have slow transfer speeds.
- USB hard disk drives have a shelf life of 3-5 years, susceptible to magnetic fields and mechanical failure.
- USB solid state drives are faster and more reliable than HDDs but only have a finite number of files that can be written to and taken off of the drive and are more expensive than HDDs.

NAS for storage / USB for evidence transfer:

USB flash drives for evidence:	$2,000/yr.
8-Bay NAS w/ 10tb HDDs:	$2,650
First Year Total:	$4,650*
10 Year Total (including maintenance):	$26,900*

*Does not reflect any associated costs with professional installation, network management / configuration, network architecture changes or the physical routing of network cables if needed.

<u>Issues:</u>

- The USB flash drives are committed to evidence once submitted.
- USB flash drives are small and fragile, susceptible to loss and damage.
- USB flash drives have slow transfer speeds.
- If configured correctly total storage in NAS would be 60tb (not 80tb).
- Hard disk drives have a shelf life of 3-5 years, susceptible to magnetic fields and mechanical failure.
- Solid state drives are faster and more reliable than HDDs but only have a finite number of files that can be written to and taken off of the drive and are more expensive than HDDs.
- A NAS like a computer has a shelf life of approximately 5 years and will need to be replaced as it ages.

Data Server for storage / USB for evidence transfer:

USB flash drives for evidence:	$2,000/yr.
Rack Mounted Server w/ x12 10tb HDDs:	$7,000
First Year Total:	$9,000*
10 Year Total (including maintenance):	$33,300*

*Does not reflect any associated costs with professional installation, network management / configuration, network architecture changes or the physical routing of network cables if needed.

Issues:

- The USB flash drives are committed to evidence once submitted.
- USB flash drives are small and fragile, susceptible to loss and damage.
- USB flash drives have slow transfer speeds.
- If configured correctly total storage in the server would be 100tb (not 120tb).
- Hard disk drives have a shelf life of 3-5 years, susceptible to magnetic fields and mechanical failure.
- Solid state drives are faster and more reliable than HDDs but only have a finite number of files that can be written to and taken off of the drive and are more expensive than HDDs.
- All server components like a computer have a shelf life of approximately 5 years and will need to be replaced as it ages (server workstation / hard drive rack).
- If Windows Server OS is selected, it will need to be updated to the newest version every few years to maintain security.

Cloud Based Server for storage / USB for evidence transfer:

USB flash drives for evidence:	$2,000/yr.
AWS Cloud Services (average between S3 and Glacier Instant)	$335/yr.
First Year Total:	$2,335
10 Year Total (including maintenance):	$23,350

Issues:

- The USB flash drives are committed to evidence once submitted.
- USB flash drives are small and fragile, susceptible to loss and damage.
- USB flash drives have slow transfer speeds.
- Data stored within the cloud may not be immediately available.

Advantages:

- Data housed within cloud is safe from local events (natural disaster/emergency)
- Cloud storage can be expanded effortlessly.
- Data can be accessed via web portals anywhere.
- Can be configured to share digital evidence without the need for USB storage, without audit logs or chain of custody management.

DEMS Cloud Server for storage & evidence transfer:

DEMS Yearly License (averaged from several providers):	$10,000/yr.
10 Year Total:	$100,000

Issues:

- Higher cost than other solutions.

Advantages:

- Eliminates the need for USB devices for transfer and storage.
- No technical knowledge is needed to implement -or- maintain.
- No ongoing maintenance costs.
- No risk of local storage failures.
- Data housed within cloud is safe from local events (natural disaster/emergency)
- Cloud storage can be expanded effortlessly.
- Data can be accessed via web portals anywhere.
- Digital evidence can be transferred via web applications or portals.
- Provides a platform to organize digital evidence and associated case files and monitor chain of custody.
- Depending on the provider, it can provide a suite of tools for digital forensic investigations.

Conclusion - How Do We Move Forward in Digital Forensic Storage?

As demonstrated in this research, digital data storage is evolving and expanding in the devices that digital forensic laboratories are encountering daily. A storage architecture for handling the growing amount of digital data should not fall onto the shoulders of the laboratory to manage locally as this takes away vital time and resources that would be better served in the examination of digital evidence. In the case documented involving the Southern Virginia Internet Crimes Against Children Task Force Headquarters (SOVA ICAC), it is demonstrated that the investment of large sums of money into local storage arrays can be a fatal and puts an undue risk on digital evidence and case files. SOVA ICAC are leading the front on moving their storage capabilities to the cloud and are doing so at a fraction of the cost that local storage equipment requires.

Cloud-based services as a whole are moving into mainstream use within governmental operations. Law Enforcement in particular needs to make this move forward to accept cloud storage options to help leverage their digital forensic laboratories to produce more analyzed data, clear device back logs, and allow cloud storage and services to help manage the workload they intake.

Any public service agency needs to be held accountable for budgetary spending as it directly correlates to tax revenue being used to further ensure the safety of the citizens. A similar standard is held for private sector businesses being held accountable for spending under a budget review. Allocating funding for cloud storage and services can help to reduce budgetary spending so that these funds can be allocated elsewhere. In either application, if DEMS services are implemented, a demonstrated increase of collaborative efforts, data sharing, and increased workflow can be shown to justify the increased cost.

With the numerous and rigorous federal regulations in place surrounding information security applied to cloud storage and services it should help to build trust in using such services to house digital evidence. The regulatory compliance coupled with the collaborative abilities cloud services offer should prove to fit any Law Enforcement agency or private sector digital forensic laboratory’s needs to move them forward in this sphere. As outlined in this document, a majority of the States with the United States do not have a particular cloud service provider designated, only a need to meet federal or state compliance standards, which has been achieved by multiple cloud service providers, the remaining compliance standards fall on the end user to implement.

References:

[1] - Buchanan, M. (2013, June 14). *Object of interest: The Flash Drive*. The New Yorker. Retrieved February 2, 2023, from https://www.newyorker.com/tech/annals-of-technology/object-of-interest-the-flash-drive#:~:text=Trek%202000%20International%2C%20a%20Singaporean,only%20a%20few%20years%20ago.)

[2] - Kerekes, Z. (2019). *Charting the Rise of the SSD Market*. SSD market history - charting the rise of the SSD market (1970s to 2019) the original article on Storagesearch.com. Retrieved February 2, 2023, from https://www.storagesearch.com/chartingtheriseofssds.html

[3] - Romero-Chan, C. (2022, December 8). *Admit it, the 1TB iPhone 14 pro is the right version to buy*. Digital Trends. Retrieved February 2, 2023, from https://www.digitaltrends.com/mobile/apple-iphone-14-pro-storage-1tb-right-version-to-buy/

[4] - Athow, D. (2022, March 26). *The world's largest SSD just turned four and its 100TB capacity remains unmatched - but why?* TechRadar. Retrieved March 28, 2023, from https://www.techradar.com/news/the-worlds-largest-ssd-just-turned-four-and-its-100tb-capacity-remains-unmatched-but-why

[5] - Collins, C. (2023, February 1). *Digital Evidence Cloud Storage Survey*. SurveyMonkey. Retrieved February 9, 2023, from https://www.surveymonkey.com/results/SM-1xotQQ_2By5L2MoKyENUyxWA_3D_3D/

[6] - Amazon Web Services. *AWS Cloud Security Compliance Programs*. Amazon. Retrieved March 8, 2023, from https://aws.amazon.com/compliance/programs/

[7] - Allen, R. (2021, August 11). Nand and cells: SLC, QLC, TLC and MLC explained. TechRadar. Retrieved March 27, 2023, from https://www.techradar.com/news/nand-and-cells-slc-qlc-tlc-and-mlc-explained

[8] - Schroeder, B., Lagisetty, R., ; Merchant, A. (2016, February 22). Flash reliability in production: The expected and the unexpected. FAST '16 Presentation. Retrieved March 27, 2023, from https://www.usenix.org/conference/fast16/technical-sessions/presentation/schroeder

[9] - Klein, A. (2023, March 16). *Backblaze Drive stats for 2022*. Backblaze Blog | Cloud Storage & Cloud Backup. Retrieved March 27, 2023, from https://www.backblaze.com/blog/backblaze-drive-stats-for-2022/

Further Reading:

Federal Regulations and Compliance Standards:

Criminal Justice Information Services (CJIS) Security Policy

https://le.fbi.gov/cjis-division-resources/cjis-security-policy-resource-center

Department of Defense Security Guidelines

https://public.cyber.mil/dccs/dccs-documents/

Federal Risk and Authorization Management Program (FedRAMP)

https://www.fedramp.gov/

Federal Information Processing Standards (FIPS)

https://www.nist.gov/federal-information-processing-standards-fips

Federal Information Security Modernization Act (FISMA)

https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act#:~:text=Overview,OMB%20in%20developing%20those%20policies.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

National Institute of Technology and Standards (NIST)

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

https://csrc.nist.gov/publications/detail/sp/800-144/final

https://csrc.nist.gov/publications/detail/sp/800-210/final

https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

Cloud Storage Regulations by State (if available):

Alabama (Last Updated August 2018)

https://oit.alabama.gov/wp-content/uploads/2018/09/Policy_560-01_Cloud_Storage_Services.pdf

Alaska

https://oit.alaska.gov/home/service-catalog/datacenter/storage/

Arizona

https://aset.az.gov/resources/cloud-resources

Arkansas

https://www.transform.ar.gov/wp-content/uploads/2020/04/APPROVED-20190108_CloudStrategy.pdf

https://www.transform.ar.gov/information-systems/products-services/cloud-services/

California

https://cdt.ca.gov/services/off-premises-cloud/

Colorado

https://sites.google.com/state.co.us/oitservicecatalog/it-infrastructure/aws-cloud-products

Connecticut

https://portal.ct.gov/-/media/OPM/Fin-General/State-of-Connecticut-Information-and-Telecommunications-Strategic-Plan-FY21.pdf

Delaware

https://webfiles.dti.delaware.gov/pdfs/pp/Terms%20and%20Conditions%20Governing%20Cloud%20Services%20Policy.pdf

Florida

https://www.flsenate.gov/Laws/Statutes/2020/Chapter282/All

Georgia

https://gta-psg.georgia.gov/psg/data-location-and-access-ss-15-002

https://gta-psg.georgia.gov/psg/cryptographic-controls-ss-08-040

Hawaii

https://www.capitol.hawaii.gov/sessions/session2023/bills/SB284_SD1_.HTM

Idaho

https://purchasing.idaho.gov/wp-content/uploads/2019/01/Standard-Ts-and-Cs-for-Cloud-Services-010819.pdf

Illinois

https://www.law.cornell.edu/regulations/illinois/Ill-Admin-Code-tit-44-4400-app-F

Indiana

https://www.in.gov/iot/files/State-of-Indiana-Sept-2019-Cloud-Strategy.pdf

Iowa

https://ocio.iowa.gov/cloud-computing-administration

Kansas

https://admin.ks.gov/media/cms/ITsecurity_ab57995c31e98.pdf

Kentucky (Last Updated August 2012)

https://kdla.ky.gov/records/Documents/Cloud%20Computing%20Guidelines%20Version%201.pdf

Louisiana

https://www.doa.la.gov/doa/ots/services-we-provide/storage/

Maine

https://www.maine.gov/oit/policies/RemoteHostingPolicy.pdf

Maryland

https://doit.maryland.gov/Documents/Maryland%20IT%20Security%20Manual%20v1.2.pdf

Massachusetts

https://www.mass.gov/doc/icori-cloud-storage-guidelines/download

Michigan

https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013002-Acceptable-Use-of-Information-Technology-Standard.pdf

Minnesota

https://mn.gov/mnit/assets/Data%20Protection%20Categorization%20Standard_tcm38-323779.pdf

https://www.revisor.mn.gov/statutes/2020/cite/16E.03/subd/16E.03.2#stat.16E.03.2

Mississippi

https://www.sos.ms.gov/adminsearch/ACCode/00000679c.pdf

http://billstatus.ls.state.ms.us/documents/2023/html/SB/2700-2799/SB2717SG.htm#:~:text=25%2D53%2D201.,of%20policies%2C%20standards%20and%20guidelines.

https://www.its.ms.gov/sites/default/files/PublicationsPDFs/Statewide_ATD_Plan%20(1).pdf

Missouri (Last Updated April 2016)

https://oa.mo.gov/sites/default/files/State_of_IT_Report.pdf

Montana

No Information Available

Nebraska

https://nitc.nebraska.gov/standards/8-607.pdf

Nevada

https://it.nv.gov/uploadedFiles/itnewnvgov/content/Governance/Security/FINAL_S_5_06_01_Cloud_Services.pdf

New Hampshire

https://www.das.nh.gov/purchasing/docs/Notice_Of_Contract_SIGNED/8002855%20Microsoft.pdf

New Jersey

https://nj.gov/it/docs/ps/20-01-NJOIT_Enterprise_Cloud_Computing_Circular.pdf

New Mexico

No Information Available

New York

https://its.ny.gov/document/information-security-policy

North Carolina

https://files.nc.gov/dit/documents/files/Secure-Cloud-Storage-Policy.pdf

North Dakota

https://www.ndit.nd.gov/about-us/publications/statewide-it-plan/statewide-it-plan-2021-2023

Ohio

https://procure.ohio.gov/pdf/CSP901020_Supplement%20One.pdf

Oklahoma

https://oklahoma.gov/content/dam/ok/en/omes/documents/CloudComputingStandard.pdf

Oregon

https://www.oregon.gov/das/policies/107-004-150.pdf

Pennsylvania

https://www.oa.pa.gov/Policies/Documents/itp_sec040.pdf

Rhode Island

https://rigov-policies.s3.amazonaws.com/ETSS_Policy_10-17_System_and_Services_Acquisition__SA_.pdf

South Carolina

https://admin.sc.gov/sites/default/files/StateCloudComputingStrategy.pdf

South Dakota

https://bit.sd.gov/sys_attachment.do?sys_id=5123ef841b1ca950259ba932f54bcbb5&view=true

Tennessee

No Information Available

Texas

https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=27

https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm

Utah

https://le.utah.gov/~2020/bills/static/HB0218.html

Vermont

https://legislature.vermont.gov/statutes/section/09/062/02447

Virginia

https://www.vita.virginia.gov/technology-services/catalog-services/cloud-services/cloud-third-party-use-policy/

Washington

https://app.leg.wa.gov/RCW/default.aspx?cite=43.105.450

West Virginia

https://www.wvlegislature.gov/Bill_Status/bills_text.cfm?billdoc=sb734%20enr.htm&yr=2023&sesstype=RS&i=734

Wisconsin

https://publicrecordsboard.wi.gov/Documents/PRBoard%20Guidance_Cloud_Approved_05042012.pdf

Wyoming

https://ets.wyo.gov/services/cloud-operations

Acknowledgments

This research would not have been possible without the help and support of several people. These people have been invaluable in the collection of data, review of the research, providing information, and so much more.

I would like to express my gratitude to Jim Cole, Supervisory Special Agent (Retired), Homeland Security Investigations. Jim was vital in the beginning of this research in that we shared the same vision for getting this information out. Jim helped to spread the survey used in this article to multiple people from different digital forensic laboratories. Jim was also there to provide assistance in reviewing and proofreading this research throughout its conception.

This endeavor would not have been possible without the help and support of Adam Werner, Vice President of Marketing and Engagement for Cellebrite. Adam helped to build the vision and inspiration for this research. Adam and I began discussing cloud storage options for Law Enforcement in digital evidence management and the common barriers that are associated with the mere consideration of cloud solutions. In these talks with Adam, I found the inspiration to conduct this research to provide answers surrounding the viability of cloud solutions for digital evidence.

I am also grateful for the assistance provided by Debbie Garner, Solutions Evangelist for Grayshift. Debbie saw the initial survey for this research and immediately took notice. Debbie was able to share this research survey with her vast connections which helped build the data set I was able to use for the research. Debbie was also more than willing to help facilitate introductions with her connections to gather more information necessary for this research.

A special thanks I would like to extend is to Jessica Hyde, Founder of Hexordia. Jessica was immediately available to help guide me on a path to make sure the information in this research could be viewed by the digital forensic community and others. Jessica further lent her editorial skills to make sure this research documentation was fitting and proper prior to seeking publication. Without her tutelage I don’t see how this project could have made it to this point.

I’d also like to acknowledge the following people for helping with information and data collection from their respective digital forensic laboratories to include in this research, Tuan Pham - Lieutenant Investigator for the Harris County District Attorney’s Office Digital Forensics Unit in Texas, and William Shaw - Senior Cyber Specialist for the Gulf Coast Technology Center in Alabama, Sergeant Josh Dobyns and Captain Steve Anders with the Bedford County Sheriff’s Office in Virginia and attached to the Southern Virginia ICAC Task Force Headquarters.