Cloud Forecasting: Legal Visibility Issues in Saturated Environments

Adam J. Brown[a,*], William Bradley Glisson[a], Todd R. Andel[a], Kim-Kwang Raymond Choo[b]

[a] *University of South Alabama, Mobile, Alabama, United States*
[b] *Department of Information Systems and Cyber Security, The University of Texas at San Antonio, United States*

Abstract

The advent of cloud computing has brought the computing power of corporate data processing and storage centers to lightweight devices. Software-as-a-service cloud subscribers enjoy the convenience of personal devices along with the power and capability of a service. Using logical as opposed to physical partitions across cloud servers, providers supply flexible and scalable resources. Furthermore, the possibility for multitenant accounts promises considerable freedom when establishing access controls for cloud content. For forensic analysts conducting data acquisition, cloud resources present unique challenges. Inherent properties such as dynamic content, multiple sources, and nonlocal content make it difficult for a standard to be developed for evidence gathering in satisfaction of United States federal evidentiary standards in criminal litigation. Development of such standards, while essential for reliable production of evidence at trial, may not be entirely possible given the guarantees to privacy granted by the Fourth Amendment and the Electronic Communications Privacy Act. Privacy of information on a cloud is complicated because the data is stored on resources owned by a third-party provider, accessible by users of an account group, and monitored according to a service level agreement. This research constructs a balancing test for competing considerations of a forensic investigator acquiring information from a cloud.

Keywords: cloud forensics, privacy, legal, evidence

*Corresponding author University of South Alabama, Shelby Hall, 150 Jaguar Drive, Mobile, Alabama 36608, United States

Email addresses: abrown@jagmail.southalabama.edu (Adam J. Brown), bglisson@southalabama.edu (William Bradley Glisson), tandel@southalabama.edu (Todd R. Andel), raymond.choo@fulbrightmail.org (Kim-Kwang Raymond Choo)

1. Introduction

The computer industry has been steadily moving away from the provision of goods to a service-based perspective [1]. Software distributors are increasingly servicing as opposed to selling, and consumers are purchasing the use of a product rather than a product to use. Cloud computing services offer computer users the option to execute diverse functions and tasks without installing software on their individual machines. Where personal computers and workstations perform independent calculations to generate results which may then be accessed across network resources, cloud computing services provide shared storage and computation power of a networked data center. Subscribers operate on a pay-as-needed basis allowing corporations to avoid purchasing expensive in-house infrastructure [2]. Rackspace estimates a 29% savings gain by shifting capital purchases to operating expenditures [3].

Through virtualization, computing environments can be created and managed efficiently and flexibly through automation. Because the capability and capacity of local machines are not necessary for the tasks performed by cloud services, subscribers have greater freedom in selecting devices to accommodate their needs. Scalability and elasticity of cloud services provide subscribers with options for operating under changing server loads. Organizations investing in cloud computing have become more capable of delivering expedited electronic services without relying on an internal specialized team for maintenance and support [4].

Corporate expenditures for cloud services have begun outpacing their traditional back-office system infrastructure [5]. Information officers recognize the potential profits from transforming information technologies into cloud perpetuated business technologies. A recent survey of technical professionals across a variety of industries indicated that 93% of the organizations use cloud services in some capacity [6]. The report goes on to state that, up by 10.8% from 2014, eighty-two percent of these organizations have adopted a hybrid cloud strategy [6]. Forecasting in 2014 cloud data center traffic to increase at a rate of 27.5%

compound annual growth between 2016 and 2018 reaching an estimated total of 6.5 zettabytes per year by 2018 [1], Cisco extended the projection in early 2018 holding that annual global data center traffic will reach 20.6 zettabytes per year by the end of 2021, up from the measured 6.8 zettabytes in 2016 [7]. By 2021, a predicted 94% of workloads will be processed by cloud data centers with an estimated quadrupling of cloud data storage capacity to 2.6 zettabytes between 2016 and 2021 [7]. Forrester analysts project revenue from public cloud services to reach $191 billion by 2020 [8].

Despite the numerous and significant advantages for including cloud services in an operational model, vulnerabilities of the provider system represent security threats for all subscribers [9]. Adversarial access to the hypervisor potentially compromises reliability and confidentiality of every image stored there [9]. Increasing threats and risks associated with session riding, a relatively small entropy pool, malicious insiders, etc reinforce the need for forensic investigations [10].

While recent research indicates that the use of digital evidence in criminal litigation is on the rise [11, 12], this paradigm shift to virtualized resources on a shared system poses intriguing issues for forensic analysts and law enforcement agencies. Researchers already question the adequacy of traditionally accepted forensic tools and methods to sufficiently obtain evidence from cloud environments [13, 14], due to the challenges faced in the process of gathering the fragile and elusive evidence, proving it has not been tampered with, etc. Beyond challenges when establishing a foundation for admissibility, the rights afforded to denizens and the duties obligated by investigators within a particular jurisdiction give rise to additional concerns.

In the United States, for example, the Fourth Amendment provides protection from warrantless searches by government agents or actors where there is a reasonable expectation of privacy. However, there are legitimate questions as to the extent of protection available for information to be retrieved by forensic professionals on a cloud server. Interpretation of the law changes depending on the nature and scope of an investigation. While the Fourth Amendment generically

preserves privacy interests, federal statutes such as the Electronic Communications Privacy Act of 1986 (ECPA) [15] pertain to the lawful acquisition of stored communications and data. Title II of the ECPA, the Stored Communications Act (SCA) proscribes accessing digital information without or in excess of authority, and it details rules relating to disclosures both voluntary and required of otherwise protected information. Though drafted when communications did not reside on remote servers indefinitely, the SCA has been broadly interpreted as the source of federal privacy protections of online resources and processes [16]. Because the same rules apply across divergent emerging technologies, there is a considerable question as to best-fit interpretations of the SCA in relation to cloud forensics.

In the aftermath of the hack of Google Apps which led to the Twitter breach in 2009 [17], the non-partisan research group World Privacy Forum advised caution to the mayor of Los Angeles when handling information stored on the cloud due to legal uncertainty relating to cloud privacy matters [18]. Disclosed web service vulnerabilities, like Heartbleed [19] and Shellshock [20], create an atmosphere of urgency to address these open inquiries before courts become flooded with complex legal issues. Lacking clear procedures for forensic analysts to follow that satisfy constitutional and federal privacy requirements, there is substantial risk of inconsistent judicial rulings based on potentially arbitrary factual and methodological distinctions among cases.

Even in nations with analogous culture, laws, and cases, the effects of *stare decisis* warrant each jurisdiction be treated entirely separately. At best, there is persuasive authority depending on the cases. Because privacy is considered well-settled in most nations with legal structures akin to the United States, a court of law would typically only consider international opinions when engaging in judicial activism. Unsurprisingly, this may diminish any predictive value of a series of statements regarding other jurisdictions without a considerable amount of text in support.

To those ends, the research investigates and the analysis scrutinizes digital forensics measures in cloud environments for acquiring admissible evidence in

criminal cases subject to federal jurisdiction in the United States of America. The measures are assessed based on their ability to gather evidence admissible under the Fourth Amendment. The underlying hypothesis of the research is that forensic investigators cannot analyze cloud computing servers providing software-as-a-service (SaaS) in a manner acceptable for federal evidentiary admissibility in a United States trial setting while maintaining full legal compliance with privacy restrictions. This research focuses on digital evidence gathering techniques pursuant to investigations supporting criminal, as opposed to civil, litigation, the scope of the research is further refined to a federal context in order to avoid lengthy discussion of state-specific court rulings that have eluded formal codification. Such discussion can be avoided, as the state common laws on this topic must meet the minimum standards as detailed in the United States Code and Constitution.

The paper is structured as follows: Section 2 describes current literature relating to cloud forensics; Section 3 provides a background of cloud computing and forensics in a SaaS environment; Section 4 discusses constitutional and federal privacy protections in the United States and how they can relate to the content on SaaS servers; Section 5 outlines likely issues encountered when presenting obtained information at trial; Section 6 considers potential challenges when balancing forensic evidence admissibility and the privacy rights of cloud subscribers; and Section 7 concludes the research and details future work.

2. Related Works

Where devices may be technologically capable of extracting information from cloud infrastructure, the multitude of layers gives rise to questions of trustworthiness [21]. Merely isolating a crime scene to investigate poses challenges for forensic investigators [22]. For all stages of the digital investigation process (DIP) model [23], issues that inhibit an analyst's ability to collect reliable data have been identified [24]. Investigators must take into consideration federal privacy protections. This need has prompted research into the relationship between

thorough data collection and individual privacy rights.

The Department of Justice [25] constructed a manual for attorneys providing a comprehensive overview of Fourth Amendment protections relating to computing services, of SCA standards for service providers, and of standards for admissible evidence. Goldfoot [26], in the Department of Justice's bimonthly periodical, outlines the ECPA rules for compelling disclosures from third-party online service providers. The chapter provides a thorough analysis of the procedures in the statute with respect to investigations on cloud devices.

Kerr [27] discusses applications of search and seizure doctrine for data acquisition, focusing on specific judicial methods and their appropriateness. In a separate article, Kerr [28] illustrates vital distinctions in physical searches and digital searches. Through these differences, the author demonstrates inconsistencies with the assumptions of the current warrant system and digital forensic investigations. Because warrants must be drafted with specificity, the context of broad digital investigations possibly conflicts with legitimizing the search. The author identified four aspects of the warrant process, which give rise to problems when gathering digital evidence.

Srinivasan [29] devises policy guidelines for forensic analysts to follow to better protect individual privacy rights without impeding investigatory progress. These policies combine recovery methods detailed in a paper series published by the Federal Bureau of Investigation with privacy-enhancing models of retrieval technologies. The article outlines a list of ten policy considerations, but forensic methods for complying with the listed items are not discussed.

In a special report, the National Institute of Justice [30] detailed digital forensic procedures of examination. In describing specific actions to be taken, the guide tailors a pathway for legal compliance. In another special report by the National Institute of Justice [31], procedures and guidelines are established for investigations involving networked services. The final chapter in the report reviews potential legal issues. Though neither document considers the obstacles when applying these methods to cloud environments, their coupling lends direction to a clearer understanding of the Department of Justice's preferred

methods for cloud forensics.

Orton et al. [32] analyzed the applicability of the existing legal framework for cloud investigations. Their research considers how the Fourth Amendment and the ECPA relate to content available through third party cloud resources. The authors regard how similar analyses employed in case law might affect future holdings involving cloud forensics, but the analysis of the authors' findings does not discuss splits in jurisdictions when assessing the extent to which the privacy of content should be protected on cloud resources.

Writing for the Congressional Research Service, Thompson [33] provides an exhaustive report on privacy protections for communication services. The document distinguishes communications in the physical world with those in both traditional and cloud computing environments. Robinson [16] identifies disparities in existing privacy protections when reviewed in the context of cloud computing. The article considers cloud computing as both an Electronic Communication Service (ECS) and a Remote Computing Service (RCS) under the SCA, but it does not apply the analysis to digital forensic methods.

Grispos et al. [13] specify difficulties encountered when gathering forensic evidence from cloud devices. The study analyzes authentication challenges with respect to applying existing forensic goals and methods to a cloud environment, but the analysis is limited to legal evidentiary standards in the United Kingdom. Similarly, the implications of cloud forensic investigations discussed by Hooper et al. [34] are limited to legal evidentiary standards in Australia. As noted by Martini et al. [35], it is important to take legal evidentiary standards factors into consideration when seeking to acquiring or accessing evidence stored or held remotely (e.g. in overseas cloud storage accounts) to ensure that there is no violation of a foreign law.

The National Institute of Standards and Technology (NIST) [36] describes cloud computing forensics generally and identifies challenges. In the report, sixty-five distinct challenges are enumerated across eight identified categories. Identifying a deficit in existing forensic practices for digital acquisition on cloud resources, Adams [37] proposed the Advanced Data Acquisition Model. The

model, comprised of three stages, combines elements from existing acquisition frameworks to address the difficulties in obtaining usable evidence from cloud resources. Martini and Choo [38] presented a four-stage cloud forensics framework, which is subsequently validated using ownCloud [39], Amazon EC2 [40], XtreemFS [41], vCloud [42], and other cloud services (see Daryabar et al. [43]; Dezfoulia et al. [44]; Shariati et al. [45]). More recently in 2015, Do et al. [46] and Azfar et al. [47] adapted the adversary model from the cryptography literature and presented forensically sound adversary models designed to facilitate forensic investigations involving cloud (and other) services on mobile devices.

Ruan et al. [48] provide a summary of digital forensics in cloud environments. In their article, they list practical complications that potentially interfere with the accuracy and authenticity of the collected data. The article does not extend the discussion to privacy issues that could arise if the identified authentication issues were to be resolved. It is also worth noting that techniques and challenges for forensics on the cloud (i.e. using cloud computing as a service to conduct digital forensics) and forensics in the cloud (i.e. cloud computing as an evidence source for forensic investigations) are mostly dissimilar, as pointed out by Martini and Choo [49].

Dykstra and Riehl [50] likewise consider practical difficulties when performing forensic investigations on infrastructure-as-a-service devices but do not research how to balance data accuracy and security with privacy protections. Wells [51] identifies how the nature of cloud computing resources creates uncertainty in applying Fourth Amendment privacy protections. Because cloud content is not necessarily strictly online nor is it strictly communication, there is no existing legal category that accurately applies. The author identifies public policy reasons for more specific privacy protections as he summarizes analogous law and policy while linking it to cloud applications.

The Scientific Working Group on Digital Evidence [52] has commented on legal requirements regarding the seizure of digital information. Where the working group members consider the balancing test for forensic investigators from a technical standpoint, the present research focuses on the balancing test for ad-

mitting the acquired information as evidence in a court of law. The two considerations are intrinsically linked, as the extraction techniques which must stand up to legal standards and scrutiny, are bound by technical and time constraints as well. The close relationship between the two topics underlines that technology does impact court decisions. Though legal matters are often abstractly phrased so as to not be narrowly tailored to context, judges may nonetheless ground their official opinions in pragmatism. If technological limitations of the modern day eliminate any other reasonable courses of action, judges in the United States have been more likely to err on the side of admitting evidence. However, if technology advances and extraction techniques do not, depending on the specific case at hand, a judge may deem previously admissible evidence as inadmissible because it fell outside of the threshold of care for the inferred standard based on the state of technological capability.

3. Cloud Computing and Forensics

The National Institute of Standards and Technology (NIST) defines cloud computing as a model possessing five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [53]. On-demand self-service refers to the ability of cloud users to adjust the properties of their subscription without interacting with a human. Cloud computing must be accessible over a network through standard means of connection. The model pools computing resources to provide services through a multitenant model. To meet subscriber demands for storage and processing, cloud services must be readily scalable. Finally, cloud systems need to automatically measure and account for resource usage [53].

Software-as-a-service (SaaS) describes a service model in which a subscriber utilizes cloud resources to execute an application, as opposed to more robust access to the underlying platforms or frameworks [53]. User access points are typically available on various devices through lightweight interfaces [53]. From the interface, subscribers can manage or control application features and ma-

nipulate content present on the cloud server. The SaaS model grants the lowest degree of freedom to a user, whose access privileges are limited to interaction with application data [53]. Rather, the provider retains the rights and responsibilities for managing the operating system and supporting framework. Greater third party control of applications permits broader access to data making it more difficult for forensic investigators to ensure continuity of possession and integrity of information.

Though investigators generally have discretion to determine the best avenue for searching for evidence [54], the product of cloud interactions potentially spreads across multiple servers. The nuanced characteristics of data storage and manipulation across varied servers and services gives rise specialized legal challenges to cloud forensic investigators. The Generic Computer Forensic Investigation Model (GCFIM), an abstracted construct representative of fifteen computer forensic process models, proposes five phases for investigators: pre-process, acquisition and preservation, analysis, presentation, and post-process [55].

For cloud systems specifically, the dynamic for pre-processing, acquisition, and preservation is considerably more in flux for forensic investigators. Because the number of involved parties and their relationships become more complicated relative to local systems and identifiable user groups, ensuring that the steps during pre-process and acquisition phases did not violate constitutional or federal privacy provisions become similarly complicated. Likewise, strict standards for the methods employed to acquire and preserve cloud data pose obstacles for ensuring data integrity in satisfaction of evidentiary requirements. How to balance the need for a secure cloud (and telecommunications) ecosystem and the rights of individuals to privacy against the need to protect the community from criminal exploitations (including serious and organized crimes and national security interests is an issue that has serious implications on the ability of governments to protect their citizens. This is an under-researched area due to the interdisciplinary challenges specific to this research.

Figure 1 illustrates the balancing act that investigators must consider when

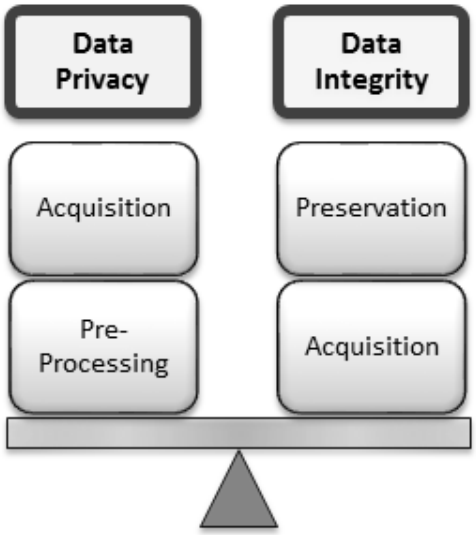

Figure 1: Concerns for Admitting Digital Forensic Evidence

collecting forensic evidence on cloud resources.

NIST has identified four distinctive attributes of pre-processing, acquisition, and preservation within cloud forensic process models: a search authority, a chain of custody, an imaging or hashing function, and validated tools for repeatable outcomes [36]. An analysis reveals a relationship between these attributes and the first two phases of the GCFIM as depicted in Figure 2. A search authority is a party authorized to access information owned by another for the purpose of an investigation. If the party acquiring or analyzing the data does not have the requisite legal permissions, any evidence yielded risks exclusion in a United States court of law. Guaranteeing the integrity of the data requires the presence of several additional attributes. A chain of custody provides a reference chronologically detailing all accesses to a set of data. During acquisition, an investigator can use imaging functions to duplicate or hashing functions to validate, and additional tools of validation may be employed for better assurance of reliability. Finally, to collect admissible cloud forensic data, any methods or

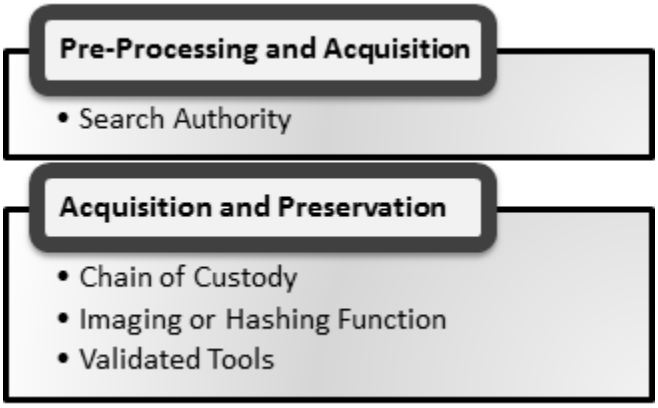

Figure 2: NIST Attributes of Digital Forensic Phases for Gathering Admissible Evidence Aligned to Initial Phases of GCFIM

functions used to gather the information should be repeatable and falsifiable. Forensic investigators must, therefore, have sufficient search authority to acquire reliable information by way of a repeatable process that sufficiently details the activities of all users who interacted with that data. In practice, resource concerns may place significant constraints on an investigator's ability to acquire the authority necessary for the level of search taking place.

4. Pre-Processing and Acquisition Phases

When conducting cloud forensics, establishing a search authority can be troublesome. To conduct any kind of search or seizure, an investigator must have legal authority to access the location to not risk the activity violating privacy protections guaranteed in the United States under the Constitution and federal law. Though cloud computing presumes multitenancy, parties other than the cloud service provider are unlikely to be authorized, and any authority to access subscriber content is contingent on interrelating factors such as the service provided, the use of the service, and the terms of the service.

4.1. Fourth Amendment

For a government intrusion to be considered a search under the Fourth Amendment, the activity must infringe upon a legitimate expectation of privacy [56]. This expectation of privacy must be both an actual subjective expectation and societally recognized as reasonable [57]. To conduct a valid search where there is a reasonable expectation of privacy, a warrant must be obtained that describes with particularity the place to be searched and the thing to be seized. An officer obtaining a warrant must demonstrate probable cause to believe that a search is necessary for an investigation [58].

When a search is unreasonable, the exclusionary rule suppresses the admission of the illegally obtained evidence [59]. Drafted to dissuade unconstitutional intrusions, the doctrine has been expanded to further exclude admission of any information discovered as a result of illicitly obtained evidence [60]. The rule encourages investigators to be mindful of the privacy of suspects lest they contaminate their evidentiary pool and weaken their case at trial.

4.1.1 Digital Searches. If not based on a probable cause showing and stated with particularity, a search warrant to obtain evidence in a criminal investigation is unenforceable. Because digital files are spread across a logical, rather than physical, space and their nature may not be immediately apparent from the metadata concerning the files, officers are presented with several obstacles when obtaining a valid warrant to search a computer. While a warrant stating the crime under investigation and specifying the types of files to be searched is enforceable [61, 62], a general warrant to seize and examine a computer in its entirety is not [63, 64]. Likewise, a warrant authorizing a blanket search or seizure of all computer storage media without statement of a reason or purpose is invalid [65, 66].

Courts generally regard a computer as a cabinet of documents; if an officer lacks authority to open a filing cabinet in a similar scenario, a search of the computer likewise exceeds authority [25, 67]. The warrant, not the discretion of the officer, limits the scope of the search [68]. Warrants are overly broad

if they omit limitations to setting and relationship [69]. Even when executed pursuant to a valid warrant, a search can nonetheless be invalidated for having been conducted in an unreasonable manner with respect to scope and intensity [70].

In *United States v. Carey* [71], a warrant was issued to permit a search of a computer for evidence relating to drug transactions. Upon finding files containing images relating to child pornography, the investigating officer began searching directories for similar images. The presiding court ruled that, because the scope of the search exceeded the particularity of the warrant, the discovery of the evidence resulted from a warrantless search [71].

Because the contents of unopened files are not "immediately apparent," the opening of each document is a manipulation tantamount to an independent search [72]. The Supreme Court recognizes, however, the potential need to open innocuous documents for a precursory scan to determine whether it can be used as evidence [73]. Flexibility is appropriate when the nature of the investigation requires exacting scrutiny in the collection of evidence [74, 75]. As long as an investigating officer does not unilaterally expand the scope of a warrant, the search will not be invalid [76]. Too loose of an interpretation of this standard risks morphing specific warrants in theory to general warrants in practice [27].

4.1.2 Digital Seizures. A seizure of property occurs when there has been a "meaningful interference" with the possessory rights of another person [77]. By this definition, copying digital information or even imaging a storage device may not constitute a seizure. In *Arizona v. Hicks* [78], the Supreme Court stated that recording the serial numbers of suspected contraband does not constitute a seizure. Relying on this holding, the court, in *United States v. Gorshkov* [79], permitted downloading online account information without a warrant because the data remained unaltered. Because the seized information cannot be searched without a warrant, the court's expansive interpretation of Hicks permits a government intrusion for copying data while denying the same degree of intrusion for observation.

The implications can be distressing. A strict adherence to *Hicks* would lead to an erosion of privacy as officers would be able to indiscriminately collect digital information as long as it is not being searched until an investigation is taking place. Some legal theorists express concern with a court's willingness to perceive copying data to subsist outside the scope of Fourth Amendment protections [27, 80]. This viewpoint is not without precedent. When concerning live surveillance, the Supreme Court ruled that the recording of information amounts to a seizure of intangible property [81]. A lower court, in *United States v. Comprehensive Drug Testing, Inc.* [65], has extended this interpretation to hold that copying digital data from a third party server constitutes a seizure.

Though conflicting judicial opinions create a grey area regarding seizures of digital information, the latter interpretation will likely prevail. This understanding is better both for public policy concerns and for consistency with Supreme Court precedent [27, 82]. Furthermore, copying computer data parallels a traditional seizure in that both preserve the state of the property being taken [82].

4.2. Stored Communications Act

Because cloud service providers are third parties storing data for their users, it would appear that the Fourth Amendment does not natively protect the information stored on cloud resources, despite the potential for a reasonable expectation of privacy. Although the Constitution protects the privacy of individuals regardless of their location [57] and extends to personal information stored on a computer [25], the knowing exposure of private information is held by courts to be the equivalent of a forfeiture of any expectation of privacy regarding the disclosed content [56]. To combat the erosion of privacy rights in an increasingly digital age, Congress enacted the SCA, Title II of the Electronic Communications Privacy Act of 1986 [83]. Drafted out of concern for the perceived deterrent effect of limited privacy with respect to the propagated use of emerging technologies, the Act regulates the ability of third parties to access electronic communications [84].

Section 2510(12) of Title 18 of the United States Code (USC) defines "electronic communication" to encompass the transmission of data by way of the Internet or a network affecting interstate commerce [83]. The SCA imposes limitations on electronic communication service providers to protect the privacy of the end users [15]. While private service providers may share subscribers' personal information at their discretion, entities that provide services to the public are forbidden under section 2702 to voluntarily disclose subscriber data unless one of eight narrow exceptions apply.

By contrast, section 2703 dictates permissible circumstances by which law enforcement can access electronic communications held by a service provider. Pending judicial process to permitting a search, section 2703(f) authorizes government actors to require service providers to preserve "records and other evidence" that may be relevant to an investigation. Records preserved must be retained for a period of 90 days, and a request for preservation can be extended for an additional 90 days for a maximum of 180 days.

Because the proscriptions in section 2702 are limited in scope by the treatment of electronic data, applicability of the doctrine to cloud providers may not be ascertainable without first considering the business model of the service. The Act distinguishes two degrees of due process that must be satisfied to access content protected records. These categories depend on the nature of the service provided, whether it is an electronic communication service or a remote computing service. Federal privacy protections for cloud users depend on which label can be applied to the cloud provider in a particular instance.

4.2.1 Electronic Communication Service. ECS providers are prohibited under section 2702(a)(1) from disclosing the contents of any communication held in electronic storage. Section 2510(17) defines "electronic storage" as temporary, intermediate storage incidental to a transmission or as storage being used for backup protection [15]. When performing an ECS, a provider does not typically store information indefinitely; rather, the contents of any particularly communication stored are presumably fluid.

Created by Congress in contemplation of email providers [83], an ECS transmits messages that are presumably clandestine. Courts consider the extent to which the public is authorized to view messages to determine whether privacy protections should be available for communications stored by an ECS. Certainly, it is logical that messages should not be privileged if they are found on forums, blogs, or bulletin boards accessible by the general public [85]. If access is restricted in some fashion, such as through contact filters available on social networking websites, however, the communications are included in SCA privacy protections [86].

Not meant to be revealed to the messenger, the contents of messages transmitted by an ECS are afforded a considerable amount of protection under the SCA. The extent of that protection depends upon how long the communication has been stored. Content stored for 180 days or less is accessible to any government investigators who obtain a warrant based on probable cause under section 2703(a). When the desired content has been stored for longer than 180 days, investigators need only obtain a subpoena or court order. Section 2703(d) requires the court order to be specific and articulate in its statement of facts to establish reasonable grounds for access to the communications.

The implications of these provisions have created several open questions for courts to consider in case-by-case analyses. To illustrate, consider email service providers. Unopened emails in storage for 180 days or less cannot be searched without a warrant. On the other hand, an email in storage for over 180 days, whether opened or not, can be accessed with a subpoena or court order. When regarding opened emails that have been in storage for 180 days or less, courts are split as to the privacy protections afforded [87, 88]. These judicially inferred principles, however, are subject to change depending on the passage of the bill for the Email Privacy Act, which was passed in the House of Representatives with 109 sponsors in February 2017 [89]. The bill, if formally signed into law, strengthens email protections regardless of the timeline. In so proposing and passing the bill, Congress has issued an implicit statement that privacy protections emanate from the content and purpose of a message, not

the formalities of its delivery or storage.

4.2.2 Remote Computing Service. RCS providers render networked storage or processing resources for subscribers. Section 2702(a)(2) prohibits an RCS provider from divulging the contents of any user communications "carried or maintained" [15]. Contrary to ECS providers, it is expected that RCS providers have access to subscriber information for extended periods of time. Because services are being performed on the data remotely, it is presumed that the information is being stored and is not merely conveyed to another location.

Congress created the RCS category to distinguish services that process and store data from the services that deliver messages. Data stored by RCS providers receive less protection than data stored by their ECS counterparts. Section 2703(b) permits governmental access to stored communications without notice if a warrant has been obtained or with prior notice if via a subpoena or court order. Presumptively, Congress reasoned that expectations of privacy are reasonably lower for data that is being given to a third party to handle or to store [90]. Prior to the enactment of the SCA, a subscriber had assumed a risk that the third party processor could disclose shared information [91].

As the degree of protection hinges on antiquated notions of electronic communications under the SCA, analysis becomes fact-dependent, leading the resulting judicial opinions vary considerably [16, 51]. At times, an ECS may take the form of an RCS depending on how a particular subscriber uses the service. The court noted in *United States v. Weaver* [88] that, if a user of Hotmail connects via a program that downloads the emails such as Microsoft Outlook, Hotmail would act as an ECS as it would be storing any downloaded emails as backups. In this case, however, the user only accessed and stored emails on allocated cloud storage, which prompted the Weaver court to regard Hotmail as an RCS [88]. Despite this precedent, the 2016 House passage of the bill proposing the Email Privacy Act suggests that, for other cloud services which function as both ECS and RCS, the stronger privacy protection available will prevail.

4.3. Cloud Privacy

There, however, remains a grey area within the Fourth Amendment framework with regards to cloud privacy. While it has been established that there is a reasonable expectation of privacy in data stored on a home computer [92] and no such expectation in non-content data over a network [93], courts have been hesitant to extend the same protection for the content of information given to third parties. But, even where a service is correctly categorized under the SCA to receive a lower threshold of protection, the Fourth Amendment represents a baseline for those protections. In a 2007 holding, the Sixth Circuit held that section 2703(d) violated the Fourth Amendment in that the provision authorized the seizure of content without notice [94]. Though the opinion was later vacated because the issue was determined unripe for adjudication [95], the Sixth Circuit partially returned to the issue in 2010 [96].

In *United States v. Warshak* [96], a subscriber has a reasonable expectation of privacy in email contents, meaning that an investigator must obtain a warrant in satisfaction of the Fourth Amendment. Under this holding, if investigators search or seize the contents of ECS user information, a subpoena or court order is insufficient leading to the suppression of any evidence obtained. According to the Warshak panel, insofar as the SCA permits such searches without a warrant, "the SCA is unconstitutional" [96]. The court in *Connor v. United States* [97] limited the Warshak decision to not apply to electronic content that has been publically shared. For cloud subscribers who control accessibility of content to other account users, the limitation identified in Connor does not apply.

The cloud service provider, Amazon, has a policy which states that only non-content information is released in response to subpoenas; to release content information, Amazon must not only receive a search warrant, but one that is validly constructed and legally binding [98]. When gathering evidence pursuant to an Arkansas first-degree murder investigation in late 2016, which garnered national attention due to police confiscation of smart devices including an Amazon Echo for data extraction, police were initially denied the requested content data by Amazon, which filed a motion in response to what was believed to be

an unconstitutionally broad search warrant [99, 100]. Before the constitutionality of the warrant could be established, however, the records in question were released after the defense attorneys consented on behalf of the content owner [101].

Orson et al. [32] composed a list based on existing case law and policy considerations to serve as a guideline to determine the likelihood of a court to find a reasonable expectation of privacy in a particular cloud scenario. The list includes questioning whether a user attempted to conceal the contents, whether the user voluntarily abandoned an expectation of privacy, whether the user created the documents in question, and whether the third party has access to the contents based on the terms in the user agreement [32]. Interpreted together, these elements present the fact-intensive analysis used by a court. If a court was to find a reasonable expectation of privacy on balance, the Fourth Amendment would demand a warrant be obtained to legitimize a search regardless of the potentially more permissive requirements of the SCA. Several other factors inherent to cloud computing may further serve to complicate efforts to acquire evidence. These include multitenant accounts, fluid cloud content, and service level agreements.

4.3.1 Multitenant Accounts. Though section 2708 of Title 18 explicitly excludes a suppression remedy for violation of the SCA, cloud providers can be subjected to monetary fines for infringing the privacy of a subscriber. Of course, if there is a reasonable expectation of privacy pertaining to the content, the evidence can also be suppressed. Note that potential claimants for an SCA violation of privacy can be any tenant on the account, not just the individual under investigation. Where the exclusionary rule only provides recourse if evidence is used against that individual, any cloud user whose privacy has been violated can file a civil claim under the SCA.

4.3.2 Fluid Cloud Content. Section 2703(f) of Title 18 requires cloud providers to preserve data requested pending the issuance of a warrant, subpoena, or court order. But, the fluid nature of content when multiple tenants have access risks

the manipulation of potential evidence by other users of the account. While the effects of such alterations should be reflected in the non-content data, the information may not be available as search limitations may preclude access to metadata pertaining to other account holders.

4.3.2 Service Level Agreements. Discerning whether a reasonable expectation of privacy exists requires a fact-intensive analysis of the circumstances relating to a specific account [102]. With regard to text messages, a provider is only required to disclose the content of stored communications if the policy authorizes the access [102].

In *Viacom Intern, Inc. v. YouTube Inc.* [103], the district court scrutinized the authorizations granted to YouTube by its terms of service agreement. Heavily relying on the scope of the contractual relationship for guidance, the court regarded YouTube as an RCS with respect to video content [103]. The court reasoned that the contract could not be construed as a subscriber giving consent under the SCA's exception to privacy protection [103].

Forensic investigators acquiring data, therefore, must take heed as to the limits of a provider's authority to access account content. Strict access restrictions prompt a court to more likely to find that a user had a reasonable expectation of privacy for the data contents. The terms of service agreement further supplies a court with a guideline to determine the extent of privacy protection available under the SCA.

5. Acquisition and Presentation Phases

After a search authority has been established for a particular set of data in the course of an investigation, the electronically stored information must be collected in a manner which ensures data integrity [104]. Authentication of digital evidence can be considered as the reliability of the combination of the tools and methods used to acquire the data and used to establish the chain of custody. Rule 901 of the Federal Rules of Evidence [105] requires sufficient supporting evidence that a piece of data is what it is presented to be. Courts

Figure 3: Points of Failure in a Cloud Chain of Custody

require proof of the reliability of the tools and techniques utilized in acquiring and assessing the information [104]. Codified in Rule 702, the *Daubert* standard requires that a method be falsifiable; the methodology employed should be peer reviewed and repeatable with known error rates [106]. For a technical process to be falsifiable, any evidence yielded must be able to be challenged. Evidence obtained via a method lacking a formal validation measure must be excluded lest a court risk admitting opinions as facts. The *Daubert* standard should be applied to authenticate both the process used to establish a chain of custody and the process to acquire the data from the cloud.

In addition to the methodology for acquiring data, the information itself needs to be authenticated with a proven chain of custody. Ensuring the integrity of information requires establishing continuity of evidence through documenting of how evidence has been controlled and manipulated prior to preservation. A chain of custody connects an analyst to a dataset so that the analyst can attempt to establish a connection between a user account and the data. Without that link, there would be no basis to admit the evidence at trial. For each additional link in the chain, there is a potential that information will be lost and that the chain will be broken. Long complex chains of custody carry a greater risk of insufficient documentation. Figure 3 lists potential points of failure in establishing usage and custody for data collected from cloud resources. Concerns endemic to cloud computing include the removal of access controls for maintenance from account owners, logical partitions and allocations for shared storage, and service level agreements dictating the relationship between provider and owner.

Native to a cloud environment, there exist multiple sources of frustration for a chain of custody before data ever leaves the cloud provider. Because the inner workings of many cloud services are private or even proprietary, acquisition procedures are not necessarily transparent. To validate the acquisition method, extensive documentation of the process is required, and either the process must satisfy the *Daubert* standard or an expert witness must be called to attest to the reliability of the acquisition methods. Matters become further complicated in consideration of shared storage among users of an account. Their diverse and persistent activity can complicate any static acquisition procedures, particularly if an investigation is time-sensitive. Furthermore, service level agreements limit a cloud provider's ability to track or store certain activity. Because the scope and details of each agreement differ among providers, there is a lack of consistency for meta-data which may be available for an investigation.

A foundational tenant of admissibility for evidence is that the probative value of the evidence must be greater than its potential prejudicial effect [105]. In a cloud environment, however, the probative value of digital evidence is lessened by the volatility of content stored on a cloud server. Low probative value of evidence decreases the likelihood that it will be admissible at trial. Establishing trustworthiness of any network accessible data presents a significant challenge [107].

Following a thorough analysis of cloud computing and forensic process models, NIST [36] identified sixty-five challenges arising from inherent attributes of cloud computing. Of these, thirty-nine items in the list affect data authentication [36]. Noting similar challenges, Orton et al. [32] expressed skepticism that existing process models are adequate to meet the *Daubert* standard for authentication. Because a service provider is the most likely party to have legal authority to search user content, forensic specialists retained by law enforcement will rarely have direct access for data acquisition. Lacking a standardized process that service providers must follow, reliability of the method used in each case will be difficult to establish.

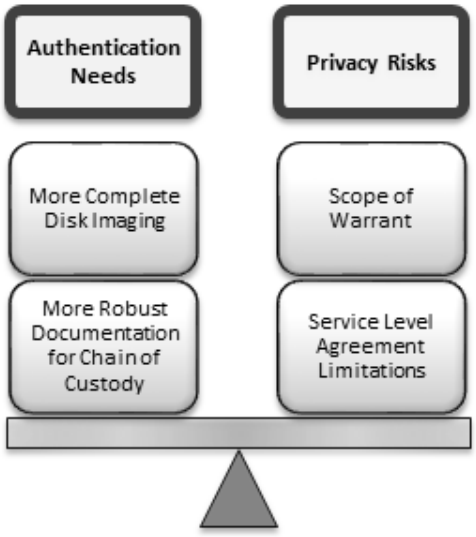

Figure 4: Balancing the Need for Authentication

6. Balancing User Privacy with Data Integrity

By its very nature, forensics of content stored by SaaS providers risk invading the privacy of suspects, other account users, and even unrelated service subscribers. Between the rigorous *Daubert* standards for general admissibility of technical evidence and the process to establish a chain of custody to authenticate a file, producing cloud content data to be used at trial as evidence is a challenging task for forensic analysts. If the data acquisition phase were more comprehensive, investigators could use their own processes to search through partitions, likely producing collaborating data for authentication. Figure 4 illustrates that the balancing test forensic investigators undergo in the face of nuanced acquisition processes used by cloud providers and the complex chain of custody generated in many cloud environments.

The availability of this option as a viable means to secure evidence must, nonetheless, be weighed against privacy considerations. Specifically, in situations in which there is a reasonable expectation of privacy, the requisite warrant

for a search or seizure must state with particularity the scope of the intrusion. To complicate matters, because courts have employed a fact-intensive analysis to ascertain the extent of privacy protections in a specific instance, assessing when a warrant is necessary may require specific knowledge of the content files to be searched. Depending on the nature of the service and the content, a subpoena or a court order does not necessarily grant legitimate access to the necessary information. When terms of service agreements prevent a service provider from supplying this information at the forefront, prudent investigators should obtain a warrant to not risk potentially crippling access restrictions.

Violation of the particularity requirement for a warrant does not necessarily prompt the Exclusionary Rule of the Fourth Amendment. Though an intrusion validated by an overly broad warrant is illegitimate, if law enforcement reasonably relied on the properness of the issued warrant, the good faith exception prevents suppression of evidence [108, 109]. However, where the warrant is facially improper, reliance is not reasonable, and the intrusion violates the privacy rights of the content owner. Therefore, as investigators try to capture data in a manner acceptable under *Daubert*, files are more likely to be obtained in excess of the scope of authority. Though courts are unlikely to require surgeon-like precision when copying cloud content for a search, caution should be exercised to minimize the likelihood of violating user privacy. Greater scrutiny for data acquisition, however, slows the progress of an investigation.

7. Conclusions

Nuances inherent to cloud servers are impacting the digital forensics landscape. The performance of forensic operations on SaaS servers presents numerous technical obstacles to investigators acquiring digital evidence for criminal cases. For example, existing digital forensic techniques are designed to collect evidential data from typical users. Cloud forensics, particularly extracting data from overseas cloud devices that provide advanced security not only for data at rest (which has now become commonplace across all smart client devices) but

also advanced encryption capabilities for data in transit (such as instant messages and emails being transmitted and received from cloud servers), are legally and technically challenging. For example, a cloud client device which has been configured securely is almost impossible to analyze using current prevalent forensic techniques and challenges faced by government agencies are compounded when anti-forensic techniques are added to a device via software/hardware manufacturers or individual device users.

These challenges make it substantially more difficult for the acquired data to be admissible and authenticated in a trial setting. For any content constitutionally protected, a search warrant is required by law enforcement when gathering evidence in a criminal investigation. Because a particular cloud service can be characterized as either an ECS or an RCS depending on the use of the service in a specific instance, the degree of privacy afforded by the SCA is largely dependent on facts. Furthermore, variability in service level agreements, server specifications, and acquisition techniques among third party cloud providers makes it difficult to craft a single policy or tool to satisfy all evidentiary requirements.

Conducting a fact-intensive analysis consumes valuable time and resources which creates a presumption that a warrant is necessary. Capturing the virtual disk may not be acceptable in several jurisdictions. Warrants must be stated with particularity, and limiting the scope of a warrant imposes restrictions on the acquisition of a comprehensive dataset. While more warrants can be issued to expand the breadth of data acquisition, every warrant issued must independently be supported by probable cause. An alternative, at this point, is not viable due to standing legislation, the potential for rampant intrusion into privacy through the use of data acquisition tools and the need for jurisdictions to turn a blind eye to comprehensive data capture.

Even in the event that a method resembling full imaging was implemented without violating privacy provisions, without formal regulation for the standardization of meta-data collection among cloud providers, service level agreements may present issues with many providers. Formal regulation may not be feasible however due to the cost considerations for many providers to redraft and im-

plement new agreements and data collection methods. As such, cloud forensic investigators are left with highly nuanced situations spanning multiple parties. More parties involved and the more complex the dataset make it increasingly difficult to balance the need to gather reliable evidence that can be authenticated with the privacy of any individuals whose information is involved in the investigation. Though no singular solution is available, awareness of potential evidentiary issues can serve to facilitate discussion concerning them.

A source of great frustration to the acquisition of usable datasets for evidence without infringing user privacy is present in sections of legislation like the SCA that are antiquated and ill-equipped to accommodate modern cloud structures. Privacy provisions were not drafted in contemplation of virtualized, remote, highly scalable service platforms controlled by third parties. Judicial attempts to shoehorn federal law into cloud computing models have led to inconsistent holdings that are dependent on a contextual analysis of circumstances. This inconsistency premised on antiquated notions of electronic information coupled with trends and tensions between data capture and privacy supports the hypothesis within the current legal environment.

The issues described in this paper affect practitioners gathering cloud resources for forensic inquiry in criminal investigations. While some practices garner information generally admissible in a current-day environment, this research investigates the attributes salient to courtroom decision makers. In understanding these issues, a balancing test has been constructed to inform forensic analysts of these concerns and considerations. Having acquired this knowledge, members in the profession can be better equipped to stay abreast of a potentially shifting legal climate due to advancement of technology or strengthening of privacy standards. For investigative practices, which have yielded admissible evidence but potentially fall short of the analysis presented in this research, questions arise as to whether those practices will continue to function as desired. This research puts forth these questions so that they may be answered prophylactically, not as a response mechanism after a court rejects presented evidence.

Future work for this research will assess existing solutions recommended for forensic investigators for more standardized data acquisition techniques on cloud servers. Each method will be weighed against existing case law to ascertain the likelihood that the method will infringe on the cloud subscribers' privacy rights. In a subsequent study, these findings can be applied to jurisdictions foreign to the United States. Beginning with a focus on nations with an analogous legal structure, the intended study would be a comparative analysis of privacy cases in both the abstract and the matter of cloud forensics. In so doing, the effects of technology and the nuances of the court room can be determined. If the context of specific cases can be used as a control across multiple nations, the effects of specific laws and of judicial consistency can be compared. Other research will consider the extent to which the privacy of account subscribers is protected when a search is conducted from the device of another user who has access to the same account. When cloud resources are seized from a local device rather than through a service provider, the probative value of the data extracted and the extent to which privacy protections exist may change considerably.

References

[1] Cisco global cloud index: Forecast and methodology, 2013-2018 (2014).
URL https://www.terena.org/mail-archives/storage/pdfVVqL9tLHLH.pdf

[2] A. Huth, J. Cebula, The basics of cloud computing, Tech. rep., United States Computer Emergency Readiness Team (2013).
URL https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf

[3] B. Kepes, Cloudonomics: the economics of cloud computing (2011).

[4] G. O'Donnell, M. Caputo, A. Mills, Cloud services are transforming your industryact now to thrive, Tech. rep., Forrester (2015).

[5] A. Bartels, A. LeClair, Us tech market outlook for 2015 and 2016: The bt agenda powers steady expansion, Tech. rep., Forrester (2015).

[6] RightScale, State of the cloud report (2015).
URL http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf

[7] Cisco global cloud index: Forecast and methodology, 2016-2021 (2018).
URL https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

[8] A. Bartels, J. R. Rymer, J. Staten, J. Clark, D. Whittaker, The public cloud market is now in hypergrowth, Tech. rep., Forrester (2014).

[9] K. Lee, Security threats in cloud computing environments, International Journal of Security and Its Applications 6 (4) (2012) 25–32.

[10] K. Munir, S. Palaniappan, Secure cloud architecture, Advanced Computing: An International Journal 4 (1) (2013) 9–22.

[11] K. Berman, W. B. Glisson, L. M. Glisson, Investigating the impact of global positioning system (gps) evidence in court cases, in: Hawaii International Conference on System Sciences, Kauai, 2015.

[12] J. McMillan, M. Glisson, William Bradley and; Bromby, Investigating the increase in mobile phone evidence in criminal activities, in: Hawaii International Conference on System Sciences, Wailea, 2013.

[13] G. Grispos, T. Storer, W. B. Glisson, Calm before the storm: The challenges of cloud computing in digital forensics, International Journal of Digital Crime and Forensics 4 (2) (2012) 28–48.

[14] D. B. Garrie, J. D. Morrissy, Digital forensic evidence in the courtroom: Understanding content and quality, Northwestern Journal of Technology and Intellectual Property 12 (2) (2014) 121–128.

[15] Electronic communications privacy act of 1986, pub l. no. 99-508, 100 stat. 1848 (oct 21, 1986).

[16] W. J. Robinson, Free at what cost?: Cloud computing privacy under the stored communications act, The Georgetown Law Journal 98 (2010) 1195–1239.

[17] N. Carlson, Twitter's secret growth projections exposed (screenshots) (jul 2009).
URL http://www.businessinsider.com/twitters-secret-documents-exposed-2009-7?op=1

[18] P. Dixon, Concerns about la's proposed contract for migration of los angeles city email (jul 2009).
URL http://clkrep.lacity.org/onlinedocs/2009/09-1714_misc_7-16-09.pdf

[19] R. Tehan, Cybersecurity: Authorative Reports and Resources, by Topic, Congressional Research Service, 2015.

[20] National Security Agency, Bash bug (shellshock) (2014).

[21] J. Dykstra, A. T. Sherman, Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, The International Journal of Digital Forensics & Incident Response (2012) 590–598.

[22] W. Delport, M. Kohn, M. S. Olivier, Isolating a cloud instance for a digital forensic investigation, in: Information Security South Africa Conference, Johannesburg, 2011.

[23] G. Palmer, A road map for digital forensic research, in: Digital Forensic Research Group, New York, 2001.

[24] G. Meyer, A. Stander, Cloud computing: The digital forensics challenge, in: Informing Science & IT Education Conference, Tampa, 2015.

[25] Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Office of Legal Education Executive Office for United States Attorneys, 2009.
URL https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[26] J. Goldfoot, Compelling online providers to produce evidence under ecpa, The United States Attorneys' Bulletin (2011) 35–42.

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

[28] O. S. Kerr, Search warrants in an era of digital evidence, Mississippi Law Review 75 (2005) 85–145.

[29] S. Srinivasan, Security and privacy vs. computer forensics capabilities, Information Systems Control Journal Online 4 (2007) 1–3.

[30] U.S. Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, National Institute of Justice, 2004.

[31] U.S. Department of Justice, Investigations Involving the Internet and Computer Networks, National Institute of Justice, 2007.

[32] I. Orton, A. Alva, B. Endicott-Popovsky, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Information Science Reference, 2013, Ch. Legal Process and Requirements for Cloud Forensic Investigations, pp. 186–229.

[33] R. M. I. Thompson, Cloud Computing: Constitutional and Statutory Privacy Protections, Congressional Research Service, 2013.

[34] C. Hooper, B. Martini, K.-K. R. Choo, Cloud computing and its implications for cybercrime investigations in australia, Computer Law & Security Review 29 (2) (2013) 152–163.

[35] B. Martini, Q. Do, Digital forensics in the cloud era: The decline of passwords and the need for legal reform, Trends & Issues in Crime and Criminal Justice.

[36] NIST Cloud Computing Forensic Science Working Group, Draft NISTIR 8006, NIST Cloud Computing Forensic Science Challenges, National Institute of Standards and Technology, 2014.

[37] R. Adams, Cybercrime and Cloud Forensics: Applications for Investigation Processes, Information Science Reference, 2013, Ch. The Emergence of Cloud Storage and the Need for a New Digital Forensic Process Model, pp. 79–104.

[38] B. Martini, K.-K. R. Choo, An integrated conceptual digital forensic framework for cloud computing, Digital Investigations 9 (2) (2012) 71–80.

[39] B. Martini, K.-K. R. Choo, Cloud storage forensics: owncloud as a case study, Digital Investigation 10 (4) (2013) 287–299.

[40] N. Thethi, A. Keane, Digital forensics investigations in the cloud, in: Proceedings of the 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, pp. 1475–1480. doi:10.1109/IAdCC.2014.6779543.

[41] B. Martini, K.-K. R. Choo, Distributed filesystem forensics: Xtreemfs as a case study, Digital Investigations 11 (4) (2014) 295–313.

[42] B. Martini, K.-K. R. Choo, Remote programmatic vcloud forensics: A six-step collection process and a proof of concept, in: Proceedings of the 13th IEEE Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014.

[43] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, K.-K. R. Choo, Forensic investigation of onedrive, box, googledrive and dropbox applications

on android and ios devices, Australian Journal of Forensic Sciencesdoi:10.1080/00450618.2015.1110620.

[44] F. N. Dezfouli, A. Dehghantanha, B. Eterovic-Soric, K.-K. R. Choo, Investigating social networking applications on smartphones: Detecting facebook, twitter, linkedin, and google+ artifacts on android and ios platforms, Australian Journal of Forensic Sciencesdoi:10.1080/00450618.2015.1066854.

[45] M. Shariati, A. Dehghantanha, K.-K. R. Choo, Sugarsync forensic analysis, Australian Journal of Forensic Sciences 48 (1) (2015) 95–117.

[46] Q. Do, B. Martini, K.-K. R. Choo, A forensically sound adversary model for mobile devices, PLOS ONE 10 (9). doi:10.1371/journal.pone.0138449.

[47] A. Azfar, K.-K. R. Choo, L. Liu, An android social app forensics adversary model, in: Proceedings of 49th Hawaii International Conference on System Sciences, Holoa, 2016, pp. 5597–5606.

[48] K. Ruan, J. Carthy, T. Kechadi, M. Crosbie, Advances in Digital Forensics VII, Springer Berlin Heidelberg, London, 2011, Ch. Cloud Forensics, pp. 35–46.

[49] B. Martini, K.-K. R. Choo, Cloud forensic technical challenges and solutions: A snapshot, IEEE Cloud Computing Magazine 1 (4) (2014) 20–25.

[50] J. Dykstra, D. Riehl, Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing, Richmond Journal of Law & Technology 19 (1) (2012) 1–47.

[51] R. B. Wells, The fog of cloud computing: Fourth amendment issues raised by the blurring of online and offline content, Journal of Constitutional Law 12 (2009) 223–240.

[52] White paper: Swgde comments on forced minimization requirements for the seizure of digital evidence, Tech. rep., Scientific Working Group on Digital Evidence (October 2016).
URL https://www.swgde.org/documents/Current%20Documents/SWGDE%20Comments%20on%20Forced%20Minimization%20Requirements%20for%20the%20Seizure%20of%20Digital%20Evidence

[53] P. Mell, T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Gaithersburg, 2011.
URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[54] Dallas v. U.S., No. 77-122 (1979).

[55] Y. Yusoff, R. Ismail, Z. Hassan, Common phases of computer forensics investigation models, International Journal of Computer Science & Information Technology 3 (3) (2011) 17–31.

[56] U.S. v. Miller, No. 97-3669SD (8th Cir 1998).

[57] Katz v. U.S., No. 35 (1967).

[58] 113th Congress, Federal Rules of Criminal Procedure, U.S. Government Printing Office, 2014.

[59] Weeks v. U.S., No. 461 (1914).

[60] Silverthorne Lumber Co. v. U.S., No. 358 (1920).

[61] State v. Askham, No. 21413-3-III (Ct of Appeals, Div 3, Panel Four 2004).

[62] U.S. v. Triumph Capital Group, Inc., No. 06-4970-CR (2d Cir 2002).

[63] Arkansas Chronicle v. Easley, No. CIV.A. 1:04cv110 (E.D. Vir, Alexandria Div 2004).

[64] U.S. v. Riccardi, No. 03-3132 (10th Cir 2005).

[65] U.S. v. Comprehensive Drug Testing, Inc., No. 05-50219 (9th Cir 2006).

[66] U.S. v. Longo, No. 97-CR-180S (W.D.N.Y. 1999).

[67] U.S. v. Andrus, No. 06-3094 (10th Cir 2007).

[68] Marron v. U.S., No. 185 (1927).

[69] U.S. v. Kow, No. 94-10258 (9th Cir 1995).

[70] Kremen v. U.S., No. 162 (1957).

[71] U.S. v. Carey, No. 98-3077 (10th Cir 1999).

[72] Minnesota v. Dickerson, No. 91-' (1993).

[73] Andresen v. Maryland, No. 74-1646 (1976).

[74] U.S. v. Christine, No. 81-2077 (3d Cir 1982).

[75] U.S. v. Hill, No. 05-50219 (9th Cir 2006).

[76] U.S. v. Grimmett, No. 05-3030 (10th Cir 2006).

[77] U.S. v. Jacobsen, No. 82-1167 (1984).

[78] Arizona v. Hicks, No. 85-1027 (1987).

[79] U.S. v. Gorshkov, No. CROO-SSOC (W.D. Washington 2001).

[80] S. W. Brenner, B. A. Frederiksen, Computer searches and seizures: Some unresolved issues, Michigan Telecommunications & Technology Law Review 8 (1) (2002) 39–114.

[81] U.S. v. New York Telephone Co., No. 76-835 (1977).

[82] O. S. Kerr, Fourth amendment seizures of computer data, The Yale Law Journal 119 (2010) 700–724.

[83] 99th Congress 2nd Session, S.Rept. 99-541 (1986).

[84] 99th Congress 2nd Session, H.Rept. 99-167 (1986).

[85] California v. Greenwood, No. 86-684 (1988).

[86] Crispin v. Christian Audigier, Inc., No. CV 09-09509 MMM (JEMx) (C.D. Cal 2010).

[87] Theofel v. Farey-Jones, No. 02-15742, 03-15301 (9th Cir 2004).

[88] U.S. v. Weaver, No. 09-30036 (C.D. Ill, Springfield Div 2009).

[89] 115th Congress, H.R. 387 (2017).

[90] Smith v. Maryland, No. 78-5374 (1979).

[91] O. S. Kerr, The case for the third-party doctrine, Michigan Law Review 107 (2009) 561–602.

[92] Guest v. Leis, No. 99-4115, 99-4176 (6th Cir 2001).

[93] U.S. v. Forrester, No. 05-50410, 05-50493 (9th Cir 2007).

[94] Warshak v. U.S., No. 06-4092 (6th Cir 2007).

[95] Warshak v. U.S., No. 06-4092 (6th Cir 2008).

[96] U.S. v. Warshak, No. 08-3997, 08-4085, 08-4087, 08-4212, 08-4429, 09-3176 (6th Cir 2010).

[97] Connor v. U.S., No. 2:10-CR-332 (S.D. Ohio, E. Div 2015).

[98] Amazon Web Services, Amazon law enforcement guidelines. URL https://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

[99] Circuit Court of Benton County, Search warrant (2016). URL https://www.courthousenews.com/wp-content/uploads/2016/12/amazon.pdf

[100] E. de la Garza, Prosecutors seek audio from amazon echo (2016). URL https://www.courthousenews.com/prosecutors-seek-audio-from-defendants-amazon-echo/

[101] M. Taylor, Prosecutor, police disagree on evidence after judge tosses amazon echo case (2017).
URL https://www.forensicmag.com/news/2017/12/prosecutor-police-disagree-evidence-after-judge-tosses-amazon-echo-case

[102] Quon v. Arch Wireless Operating Co., Inc., No. 07-55282 (9th Cir 2008).

[103] Viacom Intern, Inc. v. YouTube Inc., No. 253 FRD 256 (S.D.N.Y. 2008).

[104] Silong v. U.S., No. CV F 06-0474 LJO DLB (E.D. Cal 2007).

[105] United States Government, Federal Rules of Evidence, Michigan Legal Publishing Ltd., Grand Rapids, 2015.

[106] Daubert v. Merrell Dow Pharmaceuticals, Inc., No. 92-102 (1993).

[107] St. Clair v. Johnny's Oyster & Shrimp, Inc., No. Civ.A. G-99-594 (S.D. Tex, Galveston Div 1999).

[108] Massachusetts v. Sheppard, No. 82-963 (1984).

[109] U. S. v. Leon, No. 82-1771 (1984).