Holes in the Cloud

Weaknesses in Applying Digital Forensic Processes to Cloud Computing

Computer Security
Tufts University
Elizabeth Arford
elizabeth.arford@tufts.edu
Mentor: Ming Chow

Abstract

Cloud computing is an expanding field with wide reaching applications. The qualities that make it so attractive to users and providers, it's multi-tenancy and distributed nature, also make it difficult to apply standard digital forensic practices within. This paper is concerned with identifying the most imminent legal and practical concerns in the application of forensics on cloud computing systems, highlighting current case law pertaining to the practice of cloud-related forensics, and offering suggestions which could lead to the development of normative or legislative remedies to the difficulties in applying digital forensics to cloud computing.

Introduction

Cloud computing has arrived and is here to stay. Forbes predicts that cloud computing will be a 500 billion dollar industry by 2020.[1] Gartner has released research stating that, "By 2020, a corporate "no-cloud" policy will be as rare as a "no-internet" policy is today."[2] While 'the cloud' has become a colloquial buzzword, for the purpose of this paper, cloud computing will be defined as, "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[3] The advent of cloud computing brings with it a multitude of opportunities for innovation and advancement not offered by traditional data management systems, but it also presents significant obstacles concerning forensic investigations. Computer crime has grown as the use of computers has expanded; this is a path which can be expected to be mirrored in case of cloud computing. While a robust system of professionals, guidelines, best practices and legal procedure has been developed to equip law enforcement in the evidence gathering and prosecution of digital crime cases, this system is simply unequipped to handle the possibilities presented by cloud computing.

Cloud computing is itself a broad term; three commonly identified categories of cloud services are *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), and *Software as a Service* (SaaS).

1. **Software as a Service (SaaS):** Client purchases use of provider's applications over a network. The customer does not control the infrastructure of the cloud (network, servers, operating systems, storage, application capabilities, etc).
2. **Platform as a Service (PaaS):** Client provided with the tools (programming languages, libraries, etc) to deploy their own created or acquired application onto a cloud infrastructure. The customer does not control the infrastructure of the

---

[1] Alex Conrad. Report: *Cloud Market Cap To Pass $500 Billion By 2020*. Forbes: Jun 18.

[2] *Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today.* Gartner: Jun 2016

[3] Mell, Peter, and Timothy Grace. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology: 2011.

cloud (network, servers, operating systems, storage, application capabilities, etc), but has control over their deployed applications.

3. **Infrastructure as a Service (IaaS):** Client rents cloud infrastructure which includes processing, storage, network capacity, and other fundamental computing resources. The physical infrastructure of the cloud may not be under the customer's control, but operating systems, storage, and deployed applications are within customer control.

Each of these models provides a consumer with different level of control and transparency. Additionally, the manner in which cloud services are deployed can categorized as Private, Public, Community or Hybrid.

1. **Private cloud:** Cloud infrastructure owned or operated exclusively by a single enterprise: in house, within firewall, physical infrastructure likely to be localized.
2. **Community cloud:** Shared infrastructure for specific community: indeterminate data localization and distribution of infrastructure. Ex. academic clouds.
3. **Public cloud:** Cloud use is sold to the public: large scale mega-structure and distribution of infrastructure likely. Ex. Amazon Elastic Compute Cloud, Google AppEngine, Dropbox.
4. **Hybrid cloud:** Combination of distinct public, private and/or community clouds: allows for flexibility while maintaining control over critical resources. Ex. Amazon AWS, NetApp NPS.

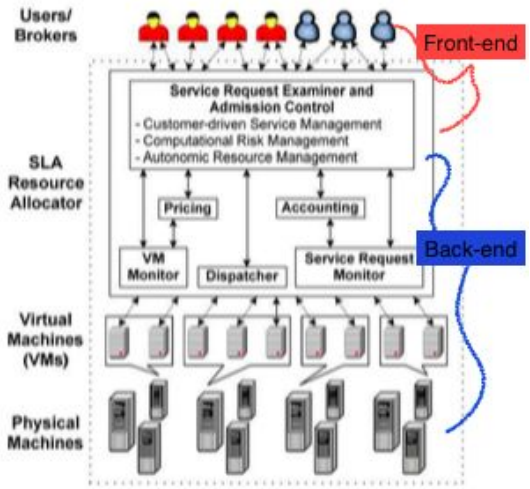

Figure 1. Cloud computing system[4]

The front end of a cloud computing system is the content accessed by users: a web-page or app; this varies little between cloud models. The back end of the cloud system presents a more complicated structure. Control over the physical machines and data storage, as well as the virtual machines and the service level agreement layer may be spread out physically and/or distributed between multiple entities.

[4] Reilly, Denis, Chris Wren, and Tom Berry. *Cloud Computing: Pros and Cons for Computer Forensic Investigations.* IJMIP: 2011.

In the field digital forensics cloud computing offers several unique challenges. Computer forensics is based around the identification, recovery and analysis of evidence, and is conducted in a manner which is verifiable and repeatable so to be able to be presented in a court of law.[5] To this end a thorough scientific process has been developed to ensure the legality of digitally procured evidence. This process involves authorization by a proper and lawful search authority, respect for the chain of custody, use of repeatable mathematics to provide validation of content, emphasizing the necessity of proper understanding of the process at each step so that it can be explained if the evidence is presented at trial.[6] The NIST Cloud Computing Forensic Science Working Group has defined this process in eight steps:

1. Search authority. In a legal investigation, legal authority is required to conduct a search or seizure of data.
2. Chain of custody. In legal contexts, chronological documentation of evidence handling is required to avoid allegations of evidence tampering or misconduct.
3. Imaging/hashing function. When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.
4. Validated tools. When possible, tools used for forensics should be validated to ensure reliability and correctness.
5. Analysis. Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.
6. Repeatability and reproducibility (quality assurance). The procedures and conclusions of forensic analysis should be repeatable and reproducible by the same or other forensic analysts.
7. Reporting. The forensic analyst must document his or her analytical procedure and conclusions for use by others.
8. Possible presentation. In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience.[7]

These procedural steps are necessary in order for evidence pertaining to cloud computing to be presentable in court. Traditional forensics relies on the centralization of information technology systems, allowing an investigator to maintain simultaneous complete control over router logs, process logs and hard disks. In cloud computing these forensic artifacts are distributed amongst both users and providers. Depending on the service and deployment model of a cloud, access to forensic data may or may not be accessible through the client-side

.

---

[5] Department of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. National Institute of Justice: April 2004.

[6] Ken Zatyko. *Defining Digital Forensics*. Forensic Magazine: 2007.

[7] National Institute of Standards and Technology. *NIST Cloud Computing Forensic Science Challenges*. Information Technology Laboratory: 2014.

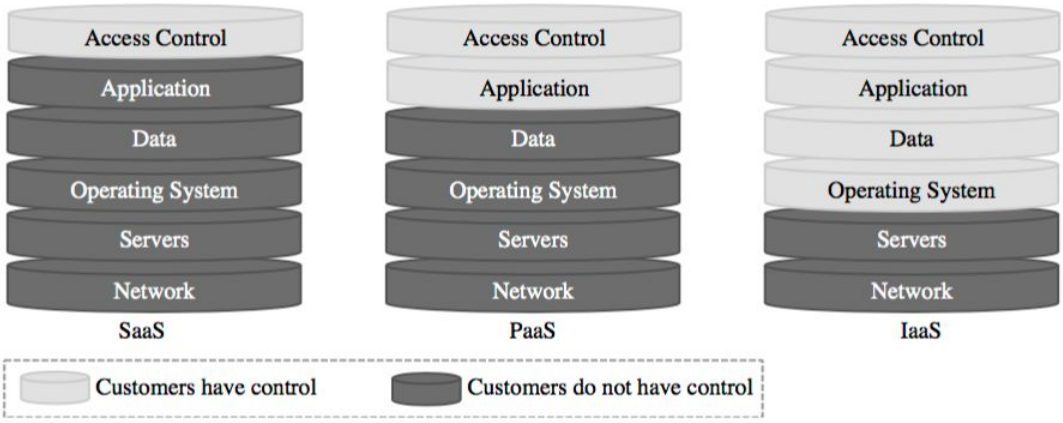

Figure 1. Access to system infrastructure[8]

Relying on the Cloud Service Provider (CSP) to access the the necessary data requires a warrant with respect to locality which is difficult, if not impossible in certain circumstances, to ascertain in a cloud computing system. Furthermore, within a cloud system the data itself is likely to be stored in a fragmented manner: parts of one user's data stored alongside pieces of other users' data. This creates difficulties in gathering, isolating and processing evidence without violating civil liberties of uninvolved parties. In a hypothetical examination of cloud computing forensic cases, Dykstra et al. demonstrated an additional obstacle faced by forensic investigators when interacting with CSPs.[9] After procuring a warrant for specific data, a technician trained in the CSP's system may be required to access the data due to the proprietary and/or complex nature of the cloud storage system. In this case, the technician may not be trained forensically, and thus any evidence acquisition she is involved with has the potential to be questioned in court.[10]

The use of logs in criminal investigations is vital. In a cloud environment, these logs may not exist, or may be decentralized and volatile. User logs may be spread out amongst servers, and the logs of different service layers may only be available to certain stakeholders. The concept of a root does not exist in entirety in many cloud computing systems: a web app developer may have the required logs and privileges for their proprietary material, while the CSP administrator may have access to the logs involved with the infrastructure of the cloud. A cloud client may maintain absolute control over their material in certain areas; this material may not be accessible to a CSP system administrator as it is the property of the client. In a forensic investigation, root privilege is often necessary to obtain a valid forensic artifact, so a purely client-side or CSP-side search process may not be forensically sound. Additionally, the use of logs in the hypervisor/virtual machine monitor (VMM) layers of cloud systems are not

---

[8] Hasan, Ragib, and Shams Zawoad. *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*. Cornell University Library: 2013.

[9] Dykstra, Josiah, and Alan T. Sherman. *Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies*. *Cyber Defense Lab*: 2011.

[10] Ibid.

standardized. Depending on the operating system of the VMM events may be logged differently, or not logged at all.[11] Thus even with access to both a client's logs and the logs of the CSP, the who, what, when, where and why traditionally granted to forensic investigators through log access may not exist.[12]

The service contract contract between a client and a CPS dictates the mandate of their relationship. The cloud computing industry has not yet developed standards which would regulate the criteria pertaining to jurisdiction and data seizure in these contracts.[13] A lack of consumer and provider awareness exists regarding the ramifications for these contract specifications in terms of a forensic investigation. Data seizure for an individual user has the potential to affect the usability of the platform for other users, and.or to violate the privacy of other users within the cloud system. Not ensuring that the data-storage structure is transparent in a service contract leads to multi-tenancy and multi-jurisdictional issues when a forensic investigation is pursued. This is especially prevalent in multi-national cloud computing organizations, where different privacy and privilege rights exist. Additionally, when data is physically stored or accessed outside the legal jurisdiction of the user, jurisdictional conflict may arise concerning what entity has the right to pursue an investigation and prosecute a case.

To the Community

Attempting to apply existing norms and practices to cloud-related forensic procedures can only provide inadequate investigative methods and does not constitute a legally sustainable practice. As the use of cloud computing expands, it is imperative that the problems within the current system are acknowledged, and that steps are taken to pursue solutions which will maintain respect for the rights of stakeholders and be effective in allowing law enforcement to pursue forensic investigations.

The dearth of regulation and legislative attention paid to specifically cloud-based criminal procedures is understandable. The “cloud” is a relatively new technology; it is lucrative, innovative and underlies a rapidly expanding field. Congress is a slow and methodological beast at its best, and the hesitation to place constraints on a digital concept is not unhealthy. While the application of wiretap warrants to email was a logical and mostly natural procedural step,[14] attempting to regulate cloud usage with a piece of legislation designed before the internet was publically available is laughable at best. Recent case law reflects the in-transability of established legal precedent in cases where cloud-computing is involved.

Concerning Jurisdiction:

Within the present system there exist two types of warrants used in criminal searches: a traditional search warrant authorized under *FED. R. EVID. P. 41*, and *18. U. S. C. §2703,* which is traditionally used to access communication accounts through an

---

[11] *NIST Cloud Computing Forensic Science Challenges*.

[12] R. Hasan, and S. Zawoad.

[13] Ruan, Key, Joe Cathy, Tahar Kechadi, and Mark Crosbie. *Cloud Forensics: An Overview*. *Centre for Cybercrime Investigation*. University College Dublin.

[14] 18 U.S.C. Chapter 121 §§ 2701–2712

service provider. Warrants issued under §2703 can be applied to information held within multiple distincts when served to a service provider. On a cloud computing network where data is known to be stored internationally the FBI is required to go through the legal process of the country physically hosting the data using Mutual Legal Assistance (MLA) request.[15]

Federal Rules of Criminal Procedure: Rule 41

The traditional warrant applied for under Rule 41 is applicable to most forensic searches, and is issued to a particular location from a magistrate within the jurisdiction. Recent rulings concerning the illegality of Rule 41 warrants in cases where jurisdiction is unknown, as is likely in cloud computing cases where data is distributed across different physical data centers, have prompted the Department of Justice to issue a procedural amendment to the rule

Proposed amendment:
Rule 41. Search and Seizure

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Cases cited in Rule 41 amendment:

United States v. Levin

- ❑ Investigators tracking down users of a child pornogrpahy site (within a website platform) who obscured their physical location using anonymizing software were denied a warrant to place surveillance software on the site which would identify users because the targets of the surveillance were not within the jurisdiction (or could not be assumed to be

[15] John M. Cauthen. *Executing Search Warrants in the Cloud*. FBI: 10 Sept. 2014.
To note: The proposed changes to Rule 41 would circumvent this in the case of remote searches, potentially violating rules of sovereignty.

within the jurisdiction) of the magistrate to whom the warrant was presented. [16]

In Re Warrant to Search a Target Computer at Premises Unknown

- ❏ Texas Judge denied a request from the FBI to install sophisticated surveillance software to track someone suspected of attempting to conduct a "sizeable wire transfer from [John Doe's] local bank [in Texas] to a foreign bank account."[17] on the grounds that the warrant request was overbroad and too invasive and failed to meet the Fourth Amendment's requirement of "place to be searched, and the persons or things to be seized." [18]

The proposed changes to Rule 41 are currently under Congressional review. Without Congressional interference these changes will take effect in 2017,[19] and will enable law enforcement to apply for a remote access warrant from any magistrate in cases where the location of a digital object is hidden or indeterminable.[20] While the proposed change is a judicial amendment and did not involve congressional action, it carries widespread implications concerning cloud-computing.

While The Department of Justices cites the logistics of a botnet investigation as impetus for the inclusion of section 6.B in the proposed amendment, cloud computing related crimes are readily applicable within the parameters of the proposed change. "Damaged" as legal term refers to a definition given in the Computer Fraud and Abuse Act, and applies to "any impairment to the integrity or availability of data, a program, a system, or information."[21] If a cloud server were to be corrupted, or if five or more virtual machines within the server were to be "damaged," due to the distributed nature of storage within cloud systems, this article would likely allow investigators to access the data contained within these machines, whether or not the users connected to the data-accessed were actually involved in the crime. This process is a demonstration of the potential path judicial processes concerning cloud computing may take if these issues are not considered pre-emptively. As opposed to development of a thorough, original piece of legislation, previous judicial standards may be forced to accommodate law enforcement's needs at the sacrifice of individual rights.

---

[16] Crocker, Andrew. *Why the Warrant to Hack in the Playpen Case Was an Unconstitutional General Warrant.* Electronic Frontier Foundation: 28 Sept. 2016.

[17] In Re Warrant to Search a Target Computer at Premises Unknown. United States District Court Southern District of Texas: 22 Apr. 2013.

[18] Ibid

[19] Supreme Court. *Proposed Amendments to the Federal Rules of Criminal Procedure*. 28 Apr. 2016.

[20] Ibid

[21] 18 U.S.C. § 1030(e)(8)

Stored Communications Act: Article 18 U.S Code §§ 2703

Section 2703 of the Stored Communications Act (SCA) allows the government to request electronic content and metadata[22] from an "Electronic Communication Service" (ECS) which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[23] or a "Remote Computing Service" (RCS) which is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[24] Cloud computing services fall within both of these definitions, so under certain conditions CSPs can be compelled to release client information under § 2703. The SCA is a subsection of the Electronic Communications Privacy Act, and was passed in 1989 to extend Fourth amendment privacy rights to computer communications. A recent ruling in the Second Circuit Court of Appeals concerning the application of a warrant on cloud computing data held outside the country has set a precedent making § 2703 only applicable domestically.[25]

Case concerning § 2703 Precedent:
Microsoft v. United States

- In the course of a drug investigation the government sought the contents of an cloud-based Microsoft email account through a § 2703 warrant. The actual emails were stored on a Microsoft data server located in Ireland. The Second Circuit ruled that the actual conduct in this case fell outside U.S. jurisdiction, and thus, that the warrant was invalid.[26]

Following the precedent set by the Microsoft case, forensic investigators engaging with internationally distributed cloud computing systems would be required to utilize a Mutual Legal Assistance request. The United States currently holds fifty-six Mutual Legal Assistance Treaties (MLAT) with various foreign states, including every member of the European Union.[27] Traditionally an obscure aspect of international law, following the revelations of Edward Snowden and the widespread institutionalization of encryption, MLATs have risen to prominence as a stick with which to advocate for mandatory encryption backdoors and dat localization. MLATs are inherently unwieldy,

---

[22] John Dykstra. *Seizing Electronic Evidence from Cloud Computing Environments.* IGI Global: 2013. Pg 163.

"Flagg (2008) states that "[The Stored Communications Act] lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to subpoena or court order." This decision on communication and the SCA provide drastically different protection for data storage in an ECS versus a provider of RCS, where 18 U.S.C. §2703(b) allows a cloud provider acting as a provider of RCS to disclose the contents of an account used for remote storage without a warrant, and without notifying the customer or subscriber."

[23] 18 U.S.C. §2510

[24] 18 U.S.C. §2711

[25] Nora Ellingsen. *The Microsoft Ireland Case: A Brief Summary.* Lawfare: 15 July 2016.

[26] Ibid

[27] Swire, Peter, and Justin D. Hemmings. *Re-Engineering the Mutual Legal Assistance Treaty Process. NYU Law and PLSC Conferences*. Georgia Institute of Technology: 14 May 2015.

and in the case of time-sensitive investigations with volatile data considerations, can be remarkably obstructive to the path of an investigation. In December of 2014, the Council of Europe's Cybercrime Convention Committee assessed the functionality of MLATs amongst European Member States and their treaty partners, finding that:

> The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.[28]

The adverse affects of the MLA request process have promoted the case for data-localization, a disturbing and potentially liberty-threatening trend that seeks to disrupt the enfranchising, free flowing and global nature of the modern internet. MLATs have also been linked to the "going dark" debate popularized amongst law enforcement in the Post-Snowden era of routine communication encryption.[29] While it is true that encryption makes traditional wiretaps less likely to yield informative results, investigators are now able to access a vast and unprecedented amount of unencrypted information and metadata stored on the cloud.

Accessing cloud-based communication from a cloud computing system data-source avoids the necessity of wiretaps, but, as shown in the Microsoft case, is often accompanied by extra-jurisdictional obstacles. When legislation or cloud-computing service contracts do not specify the jurisdictional control of consumer data MLA requests may be the only recourse available to forensic investigators. The paucity of guidelines, both from a governmental and commercial standpoint, concerning the logistics and legal framework of cloud computing presents a critical weakness in the ability of digital forensics in criminal investigations related to cloud computing.

Use of cloud computing will only grow in the years to come, and with this growth the problems concerning the lack of regulatory norms in cloud-forensics will only grow more exigent and problematic. As demonstrated by the proposed amendment to Rule 41, crisis-based patches can be dangerous, and other ad-hoc remedies may not set satisfactory precedents. These issues require full consideration by invested stakeholders in order to formulate the norms which will set legal precedent as cloud-computing grows and evolves.

Action Items

There is no clear or simple fix to the problems facing the application of digital forensics and existing legal codes in relation to cloud-computing. What is simple is that

---

[28] *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*. Cybercrime Convention Committee: 2014.

[29] Ibid

something must be done, and that this is an important topic whose treatment will have lasting ramifications. Ad-hoc patches and procedural changes will not build a framework that will be able to protect rights while allowing for the pursuit of justice as cloud-computing becomes further integrated across society.

Service contracts provide the quickest and simplest method of preventing future legal quandaries in cloud computing investigations. The development of an industry norm that contracts between providers and subscribers needs to be clear and exact in specifying ownership of information, jurisdictional particulars and avenues of access to structural and log information. These contracts do not need to be a one fit all solution. Saas, IaaS and PaaS services are all based on different user needs; contracts should be aware of the service offered, but also of the potential for forensic investigation. While, hypothetically, current service contracts provide these guidelines, there has been no central or formal push from industry leaders to mandate a realistic awareness of forensic procedures as a norm in service contracts. This should be done so immediately.

A far more difficult to implement, but perhaps more important regulatory norm can be set through legislation. While governmental control is not necessarily an effective tool and may present difficulty in maintaining relevance to a rapidly innovating field, legislation does offer the most profound method of ensuring legality in cloud-forensics. A working group drawn from industry leaders, academics and elected officials should be formed to consider possible top-down procedural and judicial reforms. Legislative change is not something that should be haphazardly applied, and the implications of cloud computing are so far-reaching that governmental action cannot be described as limited to regulating procedure, and as such, by law, will require congressional consideration.[30]

Even in best case scenario, where the majority of jurisdictional conflict is pre-determined through rigorous service contracts, the distributed nature of cloud computing as well its inherent multi-tenancy, will most likely result in some level of jurisdictional conflict. A revisal of MLAT procedures, ensuring a smoother, quicker and less cumbersome result, is entirely necessary. In the short term, this can be addressed by creating an accelerated process within the the Office of International Affairs in the Department of Justice, training specific legal professionals to deal exclusively with MLA situations, and allocating more funding to these processes. In a long term, legislation of an entirely new process, streamlined to approve MLA requests from nations with similar forensic standards could serve a similar purpose in lessening the growing pressure on the Office of International Affairs in the Department of Justice that that the institution of the Visa Waiver System did in relation to U.S. Consular Offices.[31]

The field of cloud computing presents a indistinct and fast moving target to the establishment of best practice forensics. The logistics of cloud computing create inherent holes in the currently established digital forensic practices. In order to ensure trust in the judicial system's treatment of cloud computing related crimes, a separate

---

[30] 28 U.S.C. § 2072(b)

[31] *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime.*

format for forensic investigation must be grown to deal with cloud computing's unique particularities, one that can evolve and adapt in parallel to the industry. An iterative approach to cloud computing forensics that allows for multiple, simultaneous forensic processes to build upon each other has been suggested by the Information Assurance Research Group & Forensic Computing Lab in Australia.[32] This approach would build upon the initial identification of evidence, creating a new process of forensic procedure when analysis dictates that there exists another layer to a cloud-based investigation. This would protect the preserve the chain of custody and enable simpler explanations of outside involvement (i.e. a CSP technician) in an investigation. While an iterative approach does not solve all the issues in cloud-related forensic procedures, it offers more flexibility and can be utilized as a first step in building a more formal approach.

A final possibility to note has already been organically cultivated within the field of cloud computing. Filling an apparent vacuum of expertise, cloud forensics has attracted third party cloud computing services who offer cloud forensic services. While these services are unlikely to be effective on a broad scope, they present pre-developed forensic structures specially designed to deal with specific cloud computing models and deployments. An example of this is Deloitte, who has developed a forensic process specially for Google Apps.[33] Third parties with pre-set procedures for forensic investigations within major cloud providers would substantially decrease the range of extrajudicial cloud-computing services.

Conclusion

Cloud forensics is a field that has not yet been truly challenged, but will almost certainly be as cloud-based services continue to grow. With this understanding, the immediate consideration of realistic proposals for improvements in the processes relating to cloud computing forensics becomes expedient and necessary. Pre-emptive action will prevent ad-hoc fixes to legal situations which are inevitable considering current industry trajectory. Beyond establishing the regulations, norms, procedures and principles which will protect the integrity of the judicial system, addressing the deficiencies in cloud-forensics will protect the integrity of the internet as a whole. Encryption benefits private, governmental and corporate internet stakeholders alike. If law enforcement is unable to access cloud-based data they will continue to push for the installation of backdoors and hardcoded keys, both of which are inherently destabilizing to current internet practice. Judicial overreach as a result of poorly considered patches to holes in the forensic framework of cloud computing is a definitive possibility. Raising public awareness of cloud-users and introducing norms which protect forensic processes in cloud computing situations will shield both industry and individual interests. As more and more users enter this field, there exist ever extending possibilities within it; it is imperative that the scope of legal and investigatory abilities is not overrun by innovation. Cloud-computing may offer new frontiers, but it should not be allowed to turn into a wasteland of digital forensics.

---

[32] Martini, Ben, and Kim-Kwang Raymond Choo. *An Integrated Conceptual Digital Forensic Framework for Cloud Computing.* Digital Investigation: 2012.

[33] *Google Cloud Collection and Forensic Services*. Deloitte United States.

Citations

Crocker, Andrew. "Why the Warrant to Hack in the Playpen Case Was an Unconstitutional General Warrant." *Electronic Frontier Foundation*. N.p., 28 Sept. 2016.

Dykstra, John. "Seizing Electronic Evidence from Cloud Computing Environments." IGI Global, 2013. 156-85.

Dykstra, Josiah, and Alan T. Sherman. *Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies*. *Cyber Defense Lab*. University of Maryland, 2011.

Ellingsen, Nora. "The Microsoft Ireland Case: A Brief Summary." *Lawfare*. N.p., 15 July 2016.

"Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today." *Gartner: NewsRoom*. Gartner, 22 June 2016.

"Google Cloud Collection and Forensic Services." *Deloitte United States*. Deloitte Touche Tohmatsu Limited.

Hasan, Ragib, and Shams Zawoad. *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*. *ArXiv.org*. Cornell University Library, 26 Feb. 2013.

In Re Warrant to Search a Target Computer at Premises Unknown. No. H-13-234M. United States District Court Southern District of Texas. 22 Apr. 2013.

Konrad, Alex. "Report: Cloud Market Cap To Pass $500 Billion By 2020." *Forbes*. Forbes Magazine, 18 June 2015.

Martini, Ben, and Kim-Kwang Raymond Choo. "An Integrated Conceptual Digital Forensic Framework for Cloud Computing." *Digital Investigation* 9.2 (2012): 71-80.

Mell, Peter, and Timothy Grace. *The NIST Definition of Cloud Computing*. Rep. no. 800-145. Computer Security Division, National Institute of Standards and Technology. Gaithersburg: n.p., 2011. NIST Special Publication.

Reilly, Denis, Chris Wren, and Tom Berry. "Cloud Computing: Pros and Cons for Computer Forensic Investigations." *International Journal Multimedia and Image Processing* 1.1 (2011)

Ruan, Key, Joe Cathy, Tahar Kechadi, and Mark Crosbie. *Cloud Forensics: An Overview*. *Centre for Cybercrime Investigation*. University College Dublin.

Swire, Peter, and Justin D. Hemmings. *Re-Engineering the Mutual Legal Assistance Treaty Process*. *NYU Law and PLSC Conferences*. Georgia Institute of Technology, 14 May 2015.

T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime. Rep. Cybercrime Convention Committee, Council of Europe. 12th ed. Strasbourg: 2014.
United States of America. Department of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. 2004 ed. Vol. April. Washington: National Institute of Justice, 2004. NIJ Special Report.

United States of America. Supreme Court. *Proposed Amendments to the Federal Rules of Criminal Procedure*. By John G. Roberts. 28 Apr. 2016.

United States of America. U.S. Department of Commerce. National Institute of Standards and Technology. *NIST Cloud Computing Forensic Science Challenges*. Vol. 8006. Gaithersburg: Information Technology Laboratory, 2014. NIST Cloud Computing Forensic Science Working Group.

United States of America. Federal Bureau of Investigation. *Executing Search Warrants in the Cloud.* FBI Law Enforcement Bulletin. By John M. Cauthen. N.p., 10 Sept. 2014.

Zatyko, Ken. "Commentary: Defining Digital Forensics." *Forensic Magazine*. Advantage Business Media, 1 Feb. 2007.