Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Jurisdictional Issues in Cloud Forensics

M. James[1] and P. Szewczyk[2]

[1]Department of Defence, Australia
[2]ECU Security Research Institute, Edith Cowan University, Perth, Western Australia
e-mail: michael.james14@defence.gov.au

Abstract

Cloud computing is a remotely accessible, virtual environment where users have on demand access to processing resources, data, infrastructure and applications through the Internet. It has evolved to allow all sectors of the community access with some level of privacy, which depends on individual or commercial requirements and what the user or organization is prepared to pay. By virtue of the nature of the environment, cloud forensics must keep pace and evolve to meet the challenges presented by the requirements of the law. A digital forensics practitioner needs to understand the requirements of law, not only within their own jurisdictions, but those of other jurisdictions, should they require data that is stored within other states, territories or countries. The laws vary worldwide and in nearly all cases they contain little in the way of provision for the acquisition of data from a cloud environment. This paper highlights the ongoing challenges and issues pertaining to cloud centric jurisdictional forensics.

Keywords

Cloud forensics, cloud computing, jurisdiction, evidence, cyber crime

1. Introduction

In 1961, John McCarthy was the first individual to publicly voice the idea that interconnected computing would be used as a public utility (Garfinkel, 2011). John McCarthy's prediction became evident in 1999 when Salesforce.com began distributing applications to customers via the Internet (Blaisdell, 2011). In 2006, Amazon commercialised internet distribution services via its Elastic Compute Cloud. In 2009, the first iteration of browser based applications became available (Blaisdell, 2011) specifically Google Documents, Google Calendar and Gmail became mainstream to both consumers and organisations (Google, 2015).

In 2011, the National Institute of Standards and Technology (NIST) identified three (3) service model types; software, platform and infrastructure across four (4) deployment types (NIST, 2011) including:

- Public – cloud services available to all internet users;
- Private - cloud services dedicated to a single business or organisation;

- Community – similar to private offerings, but targeted towards multiple consumers sharing the same services; and

- Hybrid – offering consisting of a combination of two or more of the three models (public, private and community) (Goyal, 2014).

Initial cloud based services were based on Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The type of services provided in a cloud environment have been increasing in demand where there are now a plethora of services available. These services include cloud centred email hosting from Gmail, Hotmail or Yahoo (epic.org, n.d.), through to storage services including Dropbox, Microsoft's OneDrive and Google Drive, allowing users to store and access data across multiple devices (Rouse, 2014).

A cloud service comprises of five essential characteristics; on demand self-service, broad network access, resources pooling, rapid elasticity or expansion, and measured services (NIST, 2011). The ubiquitous, on demand and elastic nature of the cloud makes it difficult for the digital forensic practitioner to gather viable evidence whilst performing repeatable processes. Verifiable results being the core requirements of the digital forensics profession (Nelson et al., 2015).

2. Cloud Forensics

The core requirements of a digital forensics investigation are that all acquisitions, triage and analysis processes follow a reliable, repeatable and verifiable result based procedure. At the conclusion of a particular step in the analysis process, if repeated, that specific step should produce the exact same result. Nelson et al. stated that without repeatable findings forensic analysis has no value as evidence (Nelson et al., 2015). To access a cloud environment, the user requires some form of internet access, which leads cloud forensics to be considered a subset of network forensics (Cruz, 2012).

Data acquisition from the cloud is possible. F-Response released a Cloud Connector that when reviewed in 2013 was able to connect to and acquire evidence from a number of storage platforms for instance Amazon S3, HP Public Cloud and Windows Azure. The Cloud Connector was able to successfully connect to and acquire messages from webmail providers that support the Internet Message Access Protocol (IMAP) (Tilbury, 2013). Despite there being tools that can be used to acquire data from the cloud, these tools do not address some fundamental issues. For instance, how does the digital forensics practitioner attribute the collected data to a specific user? The multi-tenanted and elastic nature of a cloud environment makes establishing identity and linking an individual to evidence difficult. Further questions that remain unanswered; how are deleted items retrieved from a cloud environment, when the multi-tenant nature of the cloud could see data of interest deleted or overwritten by another user or process. NIST released a draft report in June 2014 identifying 65 cloud forensic challenges (NIST, 2014). A search of the NIST document repository showed that as at 31 August 2016 no further documentation had

been published that relates to these initially identified - 65 challenges (NIST, 2014). This indicates that identified challenges still exist and may threaten the admissibility of evidence acquired from the cloud, in a court of law.

Cloud Providers and Their Data Centres

The cloud environment by nature is multi-jurisdictional, given that not all countries will host a data centre related to a particular cloud service provider. Microsoft Azure has two data centres in Australia – Sydney and Melbourne (Corner, 2014). However, other major providers are not prepared to add Australia to their list of data centres. Google for instance has no intention of opening a data centre in Australia at this point in time (Palmer, 2016). Having a data centre in a host country will not guarantee data sovereignty, taking into account the ability for the cloud service provider to backup data to any data centre they own. This issue raises a subsequent question specifically; how does the digital forensic practitioner guarantee that the data that is being acquired is from a local data centre? These are just a few factors that present a potential jurisdictional issue in regards to the legal acquisition of the data.

Elaborating on the aforementioned issues, the location of the data centre that houses the data could also affect how it can be treated locally. The instruction of the United States of America's *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (the '*USA PATRIOT Act*') allows for a definition of how private data can be accessed by Government Agencies, in that if data is passed to a third person, the expectation of privacy is waived and falls outside the protection of the fourth amendment. This allows a government agency to access stored data without being subject to the conditions of a search warrant (Nicholls, n.d.). Even though this Act applies to data stored within the United States, it highlights an attempt at legislation that allows the digital forensic practitioner to legally access cloud based data.

Jurisdiction and Legal Issues

The United States use the Daubert Standard for the presentation of expert witness evidence in a court (Grispos et al., 2012). The Daubert standard is described by the UK Law Commission (Law Commission, 2009) using the following four points;

- A key question is whether the theory or technique in question can be (and has been) tested;
- A further pertinent consideration is whether the theory or technique has been subjected to peer review and publication;
- In the case of a particular scientific technique, the court should ordinarily consider the known or potential rate of error and the existence and maintenance of standards controlling the technique's operation; and

- Widespread acceptance can be an important factor in ruling particular evidence admissible, and a known technique which has been able to attract only minimal support within the relevant scientific community may properly be viewed with scepticism.

The Daubert Standard has been under scrutiny since it was introduced in 1993 as part of Daubert v. Merrell Dow Pharmaceuticals, Inc., where the US Supreme Court ruled on the admissibility of expert opinion. At the inaugural meeting of The National Commission on Forensic Science in Washington DC, Judge Harry T. Edwards stated that the Daubert standard did not work as expected in adversarial trials. Indeed, the US Supreme Court had described the standard as "flexible" in allowing Trial Judges greater discretion in the admission of scientific evidence (Edwards, 2014). Discretion does not mean a functional standard for the admissibility of expert forensic evidence.

The United States Second Circuit Court of Appeals has previously sided with Microsoft, in regards to emails stored in Ireland. The Court overturned an earlier ruling disallowing the US Government from compelling Microsoft to produce emails that are stored on a server located in Dublin, Ireland (Grace, 2016). The British Law Commission Consultation paper Number 190 (Law Commission, 2009) detailed four (4) requirements for the admissibility of expert evidence within the United Kingdom and Wales, including references to the legal frameworks in some Australian States:

1. Whether the subject matter of the opinion is such that a person without instruction or experience in the area of knowledge or human experience would be able to form a sound judgment on the matter without the assistance of a witness possessing special knowledge or experience in the area;

2. Whether the subject matter of the opinion forms part of a body of knowledge or experience which is sufficiently organized or recognized to be accepted as a reliable body of knowledge or experience, a special acquaintance with which by the witness would render his opinion of assistance to the court;

3. Whether the witness has acquired by study or experience sufficient knowledge of the subject to render his opinion of value in resolving the issues before the court; and

4. The expert must be capable of providing an impartial opinion, in recognition of the fact that an expert's overriding duty is to the court and not the party calling him or her to testify.

The second requirement has implications for the admissibility of evidence gathered from a cloud environment. The lack of verifiable and repeatable processes for the acquisition of evidence from the cloud is coupled with 65 cloud forensics challenges which are yet to be addressed (NIST, 2014) – updated 2016. If there is no

internationally recognised method, then there is no reliability in the process. The Australian *Crimes Act 1914* allows for the use of the suspect's personal equipment and applications to access the data stored within their cloud storage (Martini et al., 2016). From a legal standpoint, the requirement to use forensically sound methods to acquire and verify the collected evidence, which for cloud environments, proven and peer reviewed techniques have not been developed.

The European Union and the digital forensic practitioner is presented with 25 unique legal frameworks that govern the collection and presentation of electronic evidence in court (Rand et al., 2014). These frameworks have little information that pertains to the admissibility of evidence acquired from a cloud related environment, however most have an informal system of evidence, which includes that which is presented as electronic proof of a crime. This allows the presiding judiciary official to decide the value of the evidence that is presented "in accordance with his inner convictions" (Rand et al., 2014). Of the member states that do have some type of provision, they seem to be quite broad and the presented evidence may face persistent challenge. Only three European Union member states have provisions for the acquisition of electronic evidence stored abroad, these being Belgium, Estonia and Hungary. These frameworks do not provide any indication whether data stored outside of these sovereign borders is actually located within the boundary of the EU or much further abroad. The Netherlands is the only member state whereby searches for electronic evidence are not permitted to extend beyond territorial boarders. Table 1 provides detail on the provisions for digital forensic evidence in with EU member states:

Electronic Evidence –	**Evidence Regulated**	**No legal Provision relating to**
Cyprus	Czech Republic	Austria
Estonia	Greece	Denmark
Finland		Italy
France		Ireland
Germany		
Hungary		
Latvia		
Lithuania		
Luxembourg		
Malta		
The Netherlands		
Poland		
Portugal		
Slovakia		
Slovenia		
Spain		
Sweden		

Table 1: EU Provisions for Digital Forensics Evidence (Rand.Europe & Lawford, 2014)

When presented with the possibility of electronic evidence being stored in a foreign jurisdiction, the Australian Federal Police (AFP) can request that the country in

question to preserve the electronic evidence, through the use of preservation. ("Cybercrime Legislation Amendment Bill 2011," 2011). This order will allow time for the submission of a mutual assistance request through the Attorney General's Department.

Mutual Assistance Request

Law enforcement agencies have been known to make requests through diplomatic channels for assistance from a foreign law enforcement agency, when evidence of a crime is possibly available in that foreign jurisdiction. These requests are used because jurisdictional boundaries usually correspond to sovereign borders. In Australia, mutual assistance requests are made via the Attorney General's Department - Figure 1, when the request requires the acquisition of evidence through the use of coercive powers. In the initial stages of an investigation or to seek evidence where the use of coercive powers is not required, Australian law enforcement agencies are advised to seek Police to Police assistance (Attorney-General, 2017). These types of requests do have drawbacks, in that the time frame can be from days or weeks for an urgent case, to several months and even years, depending on the evidence required for collection.

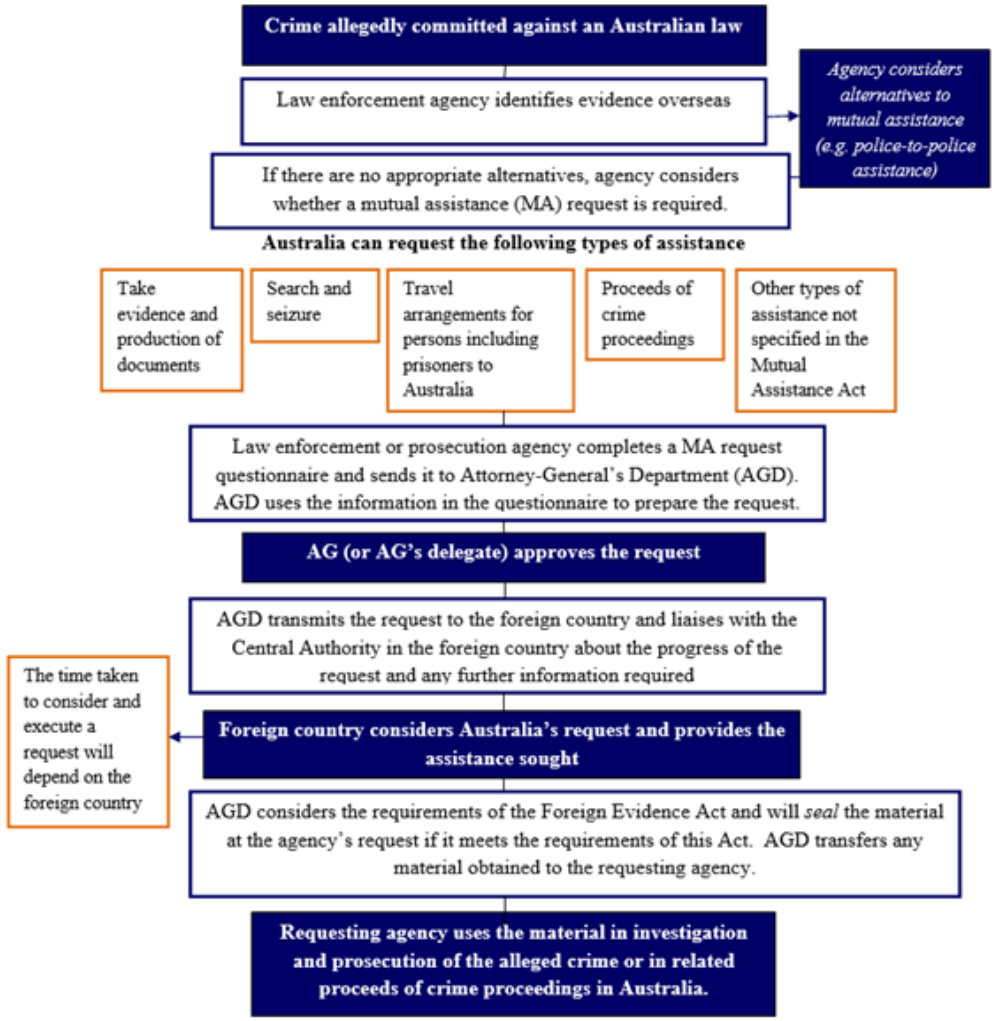

Figure 6: Mutual Assistance Request process for requests made by Australian Law Enforcement (AG, 2017)

The European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 1959) is used for the regulation of the mutual assistance requests between the member states. The convention states that assistance requests must flow between the Ministry of Justice within the respective member countries (Kubíþek, 2011). INTERPOL is often used for the transmission of evidence or information relating to criminal matters through the use of treaties (bilateral or multilateral) or international conventions (INTERPOL, 2017). Many Countries have instituted Mutual Legal Assistance Treaties (MLAT) with other countries on either a bilateral or multilateral basis, however, these MLATs struggle to keep up with technology. They are outdated and fail to account for the ability to transferred data through multiple jurisdictions, with law enforcement especially affected (AccessNow, n.d.).

3. Discussion

This paper highlighted the prominent issues for the digital forensics practitioner, these include the out-dated legislation and standards. For instance, the Guidelines for the Management of IT Evidence, published by Standards Australia. This document states that forensic evidence must be acquired using forensically sound procedures and "using a forensic standard of evidence collection" if there is a likelihood that the evidence will face legal scrutiny based on the methods used for collection of the evidence (Australia, 2003). Other jurisdictions face the same outdated documents. The United States Department of Justice published the Forensic Examination of Digital Evidence: Guide for Law Enforcement in 2004 (Hart, 2004). There is no real advice for the collection data stored in "remote storage". The document simply suggests that the remote storage be identified and details recorded. When you consider the 65 cloud forensic challenges identified by NIST, how can old standards provide valid guidance in this vital area? The two standards mentioned are at least 13 years old and still appear to be currently operational.

Large countries are not immune to the issues discussed in this paper. In making the ruling of the US Second Circuit Court of Appeal by Microsoft, Judge Gerard Lynch stated that the Stored Communications Act 1986 (SCA) became law at a time when there was no need to consider the international aspects of the type of case that involved data stored in another jurisdiction (Kerr, 2016). Furthermore, when emails transmitted through a Gmail account can be considered "outside" of the SCA due to technicalities, then the legislation is in serious need of updating to match current and future technology (Kattan, 2011).

Personal experience of one of the Authors (Michael James) shows that acquiring data from the cloud can be a daunting experience. A search warrant served in Sydney, Australia in 2015 contained provisions to acquire data from the suspect's business Google Drive. This was completed and included finding case relevant emails in the associated Gmail account. When the Australian Federal Police (AFP) officer asked the suspect for his personal Google credentials, the suspect refused as this provision was not included on the search warrant. In discussion with the investigator and the forensic practitioner (author), the AFP officer asked if it was possible to use one of the seized MacBook pro laptops to access the suspect's personal Google Drive. With an AFP video camera recording the process, a seized Apple MacBook was powered up and connected to the Internet automatically via the suspect's Wi-Fi service. The Google Chrome application was opened and one of the four tabs that opened was the suspect's Google Drive. These files where downloaded to the seized laptop for later analysis.

4. Conclusion

Digital Forensics in the cloud is a contentious issue for law enforcement, judiciaries and legislators, and until legislators get it right, digital forensic practitioners will find that their "expert" testimony may not be accepted. No standards appear to exist for the acquisition of credible evidence from cloud environments. NIST appears to be puzzled with forensics in the cloud demonstrated through the lack of supportive

documentation to guide practitioners. This of itself makes it much harder for governments to legislate for the acquisition of cloud centric data.

One world-wide body that may be of assistance is the United Nations (UN), with a membership made up of 193 sovereign states (UN, 2017). The Charter of the UN has provision that allows for action to be taken on issues that affect humanity in the modern world. Given that technology in the 21st century is advancing at an extremely fast pace and the legal processes of the world cannot hope to keep pace, the UN may be the only option. The establishment of some type of memorandum of understanding in regards to data stored in the cloud within the sovereign borders of member states, may go a long way towards alleviating the principle legal barrier of the gathering evidence from a cloud based environment. Another option is to allow countries that host globally accessed data centres the option to create data storage legislation equivalent to the Organisation for Economic Co-operation and Development Multilateral Competent Authority Agreements relating to the reporting tax evasion activities to member jurisdictions (OECD, 2014). A similar structure, where data can be stored without fear of compromise, but released to law enforcement through legally accepted methods of request, would greatly enhance the ability of law enforcement to gather evidence located within various jurisdictions.

5. References

AccessNow. (n.d.). "Mutual Legal Assistance Treaties. MLAT Info", https://mlat.info/policy-analysis (Accessed 10 June, 2017)

AG. (2017). Mutual Assistance https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Pages/default.aspx (Accessed 11 August, 2017)

Attorney-General. (2017). "Mutual Assistance", https://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/MutualAssistance/Pages/default.aspx (Accessed 14 June, 2017)

Australia, S. (2003). "Guidelines for the Management of IT Evidence" (Vol. HB 171 -2003). Sydney, Australia: Standards Australia International LTD.

Blaisdell, R. (2011). "A brief history of cloud computing" https://rickscloud.com/a-brief-history-of-cloud-computing-2/ (Accessed 11 July, 2017)

Corner, S. (2014, 27 October 2014). Microsoft Azure cloud launches in Australia. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/it-pro/cloud/microsoft-azure-cloud-launches-in-australia-20141027-11cagq.html

Cruz, X. (2012). The Basics of Cloud Forensics. *Cloud Times*.

Cybercrime Legislation Amendment Bill 2011, 43, House of Representatives (2011).

Edwards, H. (2014). *Reflections on the Findings of the National Academy of Sciences Committee on Identifying the Needs of the Forensic Science Community*. Paper presented at the National Commission on Forensic Science Washington DC. https://www.justice.gov/sites/default/files/ncfs/legacy/2014/05/13/harry-edwards.pdf

epic.org. (n.d.). Cloud Computing. *Electronic Privacy Information Centre*.

Garfinkel, S. (2011). "The Cloud Imperative" https://www.technologyreview.com/s/425623/the-cloud-imperative/ (Accessed July 3, 2017)

Google. (2015). "Our History in depth. Google Company" http://www.google.com.au/about/company/history/#2009 (Accessed June 14, 2017)

Goyal, S. (2014). "Public vs Private vs Hybrid vs Comunity - Cloud Computing: A Critical Review", *International Journal of Computer Network and Information Security*, Vol. 6 No. 3, pp20-29

Grace, S. (2016). "Microsoft wins landmark US appeal against search warrant for emails stored in Ireland", http://www.irelandip.com/2016/07/articles/cyber-risk-data-privacy/microsoft-wins-landmark-us-appeal-against-search-warrant-for-emails-stored-in-ireland/ (Accessed 13 June, 2017)

Grispos, G., Storer, T., & Glisson, W. (2012). "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics", *International Journal of Digital Crime and Forensics,* Vol. 4 No. 2, pp28-48.

Hart, S. (2004). "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Accessed 11 June, 2017)

INTERPOL. (2017). "Conventions mentioning INTERPOL" https://www.interpol.int/About-INTERPOL/Legal-materials/Conventions-mentioning-INTERPOL (Accessed 2 July, 2017)

Kattan, I. (2011). "Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud", *Vanderbilt Journal of Entertainment and Technology Law, 13*(4).

Kerr, O. (2016). "Second Circuit: Warrants cannot be used to compel disclosure of emails stored outside the United States" *The Washington Post*. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/14/second-circuit-warrants-cannot-be-used-to-compel-disclosure-of-emails-stored-outside-the-united-states/?utm_term=.da9a1c860300 (Accessed 14 June, 2017)

Law Commission. (2009). *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales*. Consultation Paper No 190. Untied Kingdom.

Strasbourg. (1959). "European Convention on Mutual Assistance in Criminal Matters" https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030 (Accessed June 12, 2017)

Martini, B., Do, Q., & Choo, K.-K. R. (2016). *Digital forensics in the cloud era: The decline of passwords and the need for legal reform*. Trends & issues in crime and criminal justice no. 512, (ISSN 1836-2206).

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations* (Fifth Edition ed.): Cengage Learning.

Nicholls, M. (n.d.). Cloud Computing: Transborder Data Flows and Jurisdictional Issues. *Nicholls Legal*, 3.

NIST. (2011). "Final Version of NIST Cloud Computing Definition Published", https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published (Accessed 14 June, 2017)

NIST. (2014). "NIST Cloud Computing Forensic Science Challenges", https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf (Accessed 26 July, 2017)

Palmer, D. (2016). "Google leaves Australia off cloud expansion list", https://delimiter.com.au/2016/03/26/google-leaves-australia-off-cloud-expansion-list/ (Accessed June 12, 2017)

Rand.Europe, & Lawford. (2014). "Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs" https://publications.europa.eu/en/publication-detail/-/publication/284df5ca-3f07-4532-a883-0c878aa4af73/language-en/format-PDF/source-24074263 (Accessed 10 June, 2017)

Rouse, M. (2014). "Cloud Storage. Tech Target, Search Cloud Storage", http://searchcloudstorage.techtarget.com/definition/cloud-storage (Accessed 25 June, 2017)

Tilbury, C. (2013). Cloud Forensics with F-Response. *Forensic Methods, Computer Forensics*.

UN. (2017). "United Nations Overview", http://www.un.org/en/sections/about-un/overview/index.html (Accessed 11 June, 2017)