Title	The End of effective Law Enforcement in the Cloud? - To encrypt, or not to encrypt
Authors(s)	Ryder, Steven; Le-Khac, Nhien-An
Publication date	2016-07-02
Conference details	9th IEEE International Conference on Cloud Computing (CLOUD 2016), San Francisco, USA, 27 June - 2 July 2016
Publisher	IEEE
Link to online version	http://www.thecloudcomputing.org/2016/
Item record/more information	http://hdl.handle.net/10197/8013
Publisher's statement	© © 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/CLOUD.2016.0133

The End of effective Law Enforcement in the Cloud? – To encypt, or not to encrypt

Steven Ryder

Europol
Steven.ryder@europol.europa.eu

Nhien-An Le-Khac
School of Computer Science
University College Dublin, Ireland
{an.lekhac}@ucd.ie

***Abstract*—With an exponentially increasing usage of cloud services, the need for forensic investigations of virtual space is equally in constantly increasing demand, which includes as a very first approach, the gaining of access to it as well as the data stored. This is an aspect that faces a number of challenges, stemming not only from the technical difficulties and peculiarities, but equally covers the interaction with an emerging line of businesses offering cloud storage and services. Beyond the forensic aspects, it also covers to an ever increasing amount the non-forensic considerations, such as the availability of logs and archives, legal and data protection considerations from a global perspective and the clashes in between, as well as the ever competing interests between law enforcement to seize evidence which is non-physical, and businesses who need to be able to continue to operate and provide their hosted services, even if law enforcement seek to collect evidence. The trend post-Snowden has been unequivocally towards default encryption, and driven by market leaders such as Apple, motivated to a large extent by the perceived demands for privacy of the consumer. The central question to be explored in this paper is to what extent this trend towards default encryption will have a negative impact on law enforcement investigations and possibilities, and will at the end attempt to provide a solution, which takes into account the needs of both law enforcement, but also of the cloud service providers. It is hoped that the recommendations from this paper will be able to have an impact in the ability for law enforcement to continue with their investigations in an efficient manner, whilst also safeguarding the ability for business to thrive and continue to develop and offer new and innovative solutions, which do not put law enforcement at risk.**

Keywords—Cloud platform, Legislation, Encryption, Cloud Storage;

I. INTRODUCTION

Cybercrime has been as old as the invention of the internet, and arguably even predates that [1]. Where there is opportunity, there is crime. And where there is technology available which can assist crime, it will be used for such, even if it is not its (primary) purpose [2]. The ever increasing advances in computer sciences and technology have always been increasing the challenges faced by law enforcement, not only from a technological aspect, but also from the required imagination of how certain technology may be used, and the understanding that nothing is necessarily what it seems.

The next advancement and almost routine step is encryption, which in an increasing amount of laptops, computers or storage devices is already enabled by default [3][4], to the frustration of law enforcement [5]. Encryption specifically can apply selectively to any and all storage devices either in their entirety or selected areas or even only selected files or folders. However, while encryption is indeed noticeable, further free tools are available, with minimum user capabilities, to create hidden and encrypted areas of storage, which on initial inspection, and unless actively being looked for, will be difficult to even detect (the concept of plausible deniability) [6]. In essence it also allows the entry of a second password, similar to a panic code on an alarm – which gives the impression of having deactivated, while in reality it received a different command.

Recently, with the development of Cloud computing platforms, cloud-based applications and new capabilities are emerging daily and bringing them lower cost of entry, pay-for-use processor and data-storage models, greater scalability, improved performance, ease of redundancy and improved of business continuity. Hence, more and more users, organisations select cloud computing as a solution of their IT platforms and services. However, this also raises challenges for digital forensic investigators. This could mean that for example a given collection of evidence such as illicit material is either stored on the servers of a cloud provider, or maybe even across multiple cloud providers. Bearing in mind as well though that the country of operation of the cloud provider does not necessarily allow conclusions about the geographic location of one or more of its servers, which could be hosted in multiple countries – let alone reflecting on the possibility that the original cloud provider himself has subcontracted its services to other providers [7]. This means in practical terms that the illicit material stored by the suspect is literally scattered in the clouds, and for all intents and purposes for gaining access to it, it may as well be from a law enforcement perspective, who would possibly be required to identify the various locations, issue specific and separate requests for mutual legal assistance, and then hope for a swift response from the various jurisdictions contacted [8]. The challenges also include in order of the discovery of a suspect / suspected activity, first of all the identification of the use of cloud services for storage. Should the use of cloud storage be suspected, and a specific provider is identified, the next challenge is the location of any stored material and its identification. Should the suspect not cooperate, the challenges increase – and increase to such an extent that the non-cooperation by the suspect as regards the

provision of passwords itself has been made a criminal offence in a very pragmatic manner in some locations.

The essential aspect to be examined and discussed in this paper is the scope to which extent the application of standard law enforcement investigative techniques and procedures of gathering evidence by use of e.g. court orders is indeed a sustainable approach. This can be questioned by comparing the uniqueness of the cloud service providers in question, and the often complex structure of the providers own network or platform, with those of other industry areas. A cloud service provider may as mentioned have stored the material in one location in its control, or may have spread it across multiple servers, or have no control at all about its whereabouts based on further subcontracting of the storage. In these situations it is hard to see what the best course of action is [9]. In this paper, we propose a solution to tackle these issues. The rest of this paper is organised as follows: Section 2 shows background research in this area. We present and discuss on law enforcement requirements in Cloud forensics in Section 3. We describe and evaluate our approach in Section 4. Finally, we conclude and discuss on future work in Section 5.

II. Background

Cloud storage is a massive business area and the biggest difference is the scale to which they outsource their own services and act more of an intermediary, rather than a full-service provider using their own infrastructure. The second difference is equally the size of their average client, and whether their primary business is the provision of entire servers to individual clients using high amounts of processing and / or storage, or whether the primary income is derived from services to the public (i.e. individuals), with a high ratio of clients to server (in which case naturally the removal of a server has a much bigger impact in the number of clients affected) [10]. This brings with it a number of specific challenges, when taking into account the need or even ability for private companies to be able to preserve or even access their own logs or infrastructure for forensic purposes. As the challenge is large enough already at present, to simply gain access if you own the entire infrastructure, let alone if you do not, as is the case when data storage is possibly further sub-contracted. Additionally, due to a large part presumably to the heightened public awareness concerning data retention and collection, following the revelations by Snowden, companies are actually profiling themselves by being unable to provide logs or forensic evidence to law enforcement - see for example in this regard Apple, a market leader and a brand with a strong image as trend setters, publicly claiming that they are unable to comply with law enforcement request, as they cannot access users data (anymore) [11]. From a conceptual level, this is achieved by basing the encryption key on the user's individual pass code, making every encryption unique. This naturally brought strong criticism from the FBI, and various sources of law enforcement, but possibly contributed to Apple's increased popularity (e.g. a rise of 67 percent from 2014) [12]. As a result, if this is the new standard that is being set, then other companies will need to follow. Equally, solutions such as what the author believes can be called pseudo-encryption, i.e. encryption, but with certain authorities possessing a master-key or backdoor, seem unsuitable as they would equally jeopardize the safety of all other material which is encrypted. It is also an unprecedented intrusion into the rights of all citizen, rather than a targeted approach intruding only on the liberties of one citizen, the suspect. Overall, it can be held that encryption in a number of industries, including law enforcement, is not only best practice, but a business essential, without which no real secure environment required could ever be established in any event. A final aspect to raise is that even though encryption on its own may be seen as dangerous for specific groups, such as law enforcement, it is one of the only efficient defences against an ever increasing number and styles of cyber-attack. Encryption is understood to be the last line of defence, and as such, it cannot be outlawed safely. And this is the final point about mandatory encryption being required – the biggest security risk to any system is actually the user. Ranging from poor password selections, to the level of general awareness and understanding of computers and the internet – the user is in essence the most resilient to positive change, while at the same time being the most important.

III. Problem Statement-Law Enforcement requirements

As always, law enforcement, arguably due to the nature of being a public authority, and usually always outmatched as regards financial resources and priorities, is always a step behind in the development of new technologies and their usage for committing or concealing crime, albeit also this is changing. See here for example also the interaction of LEA with private companies in the development of new products, e.g. SKYPE and Microsoft, but also compared with pre- and post Snowden – with Apple as a global market leader providing default encryption which it itself states it cannot unlock. As business needs are driven by perceived consumer demand, this is a remarkable step which will likely be followed by other market leaders. That genuine law enforcement needs are hindered to an extent that fears of privacy intrusion outweigh the need can also be seen as a public backlash. Overall, the law enforcement authorities, in order to effectively combat cybercrime specifically, require the ability to translate traditional methods of investigations, such as surveillance, eavesdropping, wiretaps, or intercepts, to be applicable to modern means of communication, i.e. email, instant messaging, chat rooms, and even cloud services themselves, for example the use of web based email systems for storage. While most countries are in a position to apply existing national legislation in analogy, and some have specific legislation to assist this (especially those party to the Council of Europe Convention, as elaborated above), what is lacking is the ability to implement these measures from a technical perspective. For cloud storage purposes, there are in essence two possibilities which open up, even though they may be generalized. Police may be dealing with a cooperative suspect, who provides them all the details about his account, from the provider, his username and password, and the location of any illegal material. In such a case, the forensic task is not as great, as armed with this information, the question is only concerning the recovery and the documentation of that access.

It becomes significantly more challenging, when dealing with a suspect who is believed to have access to cloud services,

but whose devices are fully encrypted, and neither a specific company, nor a user name is known – let alone a password. In these scenarios, it is a painstaking process, which may even end fruitless – dependent on the level of encryption or traces of his internet activity from the Internet Service Provider itself, if it even keeps those records.

In conclusion, the needs for law enforcement which should be contained in any feasible solution take into account the operative need to be able to reconstruct events from a historical perspective, to be able to identify and gain access to certain accounts, as well as be able to obtain a copy of the data stored, combined with ideally a log of all activity pertaining to that account.

IV. Proposed solution

Solving this problem, which is not exclusively related to the small snap-shot of cloud computing, but has significantly further reaching consequences as concerns general questions of moral values of a society, is not a simple undertaking. Rather, it requires a refined approach, and it also needs to reflect the fact that cloud computing specifically is cross-border, or most likely even without locatable physical locations – meaning a degree of global jurisdictional applicability is required [13]. In the below proposed solution, we will address and provide proposals focused on law enforcement and judicial aspects, but also provide solutions based on the business side of commercial cloud storage providers.

A. A clear legal environment in which the business operates

Taking into account the previous aspects raised as concerns the questions of jurisdictional applicability, any business needs to know the legal environment in which it operates. However, there are specific challenges for a cloud storage provider, or also a cloud service provider in more general terms, based on the geographic location of its actual storage facility. It would appear from the various terms and conditions applicable to the provision of services, that the majority of the providers nominate a court / jurisdiction applicable to the contract of service. However, this contract cannot override national law. And as such, a storage provider with multiple places of business, which most storage providers are, by virtue of the irrelevance of the physical location of its customer, will have to take into account multiple jurisdictions. As much as possible, this should therefore be avoided, and a degree of protection needs to be afforded to service providers, to know the terms of their engagement – and if need be, for example, have the liberty to exclude customers based in jurisdictions where the terms of engagement are not acceptable to the provider.

B. A clear legal environment for its interaction with law enforcement

A more specific subsection of legal clarity comes as regards the need to interact with law enforcement, and more specifically, what the possibilities for law enforcement are in that jurisdiction. It cannot be the case that a business, when assessing one of its biggest and mission critical risks, has to rely on policy decisions in force at the time, based on the discretion of a judge able to issue a warrant, or the practice of the respective prosecutor. If it were subject only to the question of individual preferences and discretion, rather than concrete and specific legislation, it would, if wise, either opt not to operate in that jurisdiction, or to see itself forced to cooperate in an anticipatory manner, for fear of losing the business.

As such it needs to be clear, and that can only be done by explicit legislation, applicable to the specific sector, what can and cannot be done. Relying on the interpretation of legislation in force significantly before the emergence of the various technologies, the internet itself, or as a result of ill-informed legislators (while having good intentions), creating laws which have no real direct bearing on the process.

C. A clear ability to maintain business continuity

Apart from the technical causes that may cause system outages, be it from electronic causes, events of nature, or a pipe bursts, etc., there should be no other threat emanating towards its business continuity, and especially not from the side of law enforcement. This all pre-supposes naturally that the services offered by the business are indeed legal, and that there is no criminal activity conducted by it, or condoned / supported / encouraged by it. However, as regards the concerns of business continuity, it cannot be the case that the suspected engagement of one of their customers is an inherent business risk to the provider.

D. A clear ability to provide services to clients, without being responsible for the content

Any responsibility for the content stored on the cloud provider's systems cannot be made the business's responsibility. The situation is clearer as regards for example internet service providers, telephone companies – infrastructure providers in general. The moment the cloud provider is by default responsible for matters hosted on its servers, will be the moment that the cloud will no longer be able to be used by businesses, law enforcement, or any other person with a legitimate need to protect their data from third parties.

E. A clear relationship of trust with the customer

The cloud provider needs to be able to assure the client that his data will be safe, inaccessible to third parties or the provider itself, and that the client can entrust his data to the provider, and see it in essence as an extension of his own desk or living room or garage – wherever else he may have stored the data otherwise.

If this trust is violated or not present to begin with, the company will not survive. And especially the possible pressure of advance or proactive compliance with law enforcement requests, for example those not supported by a warrant, damage such trust. Equally, data breaches and security breaches damage it – but not to a massive extent, if the data is encrypted.

F. Summary of needs of Storage Providers and Law Enforcement

It is easily summarized that the needs of a cloud provider (from a non-technical aspect, but limited to the scope of this paper), require clarity – simply and foremost: clarity on the

jurisdictional aspects, clarity on the abilities of law enforcement, and clarity on questions of liability. So any feasible solution must contain this one core ingredient. The outcome of the clarity may not be necessarily in the best interest from a business perspective, but at least then an informed decision can be made about the establishment of a branch or headquarters, or the provision of services to a specific country or area.

G. *Way forward*

We, upon reflection and the acknowledgement of all of the above discussed aspects, comes to the following proposed solution. This is primarily based on the realization of two aspects, namely that laws need to be seen to function, in the absence of which no meaningful policing can take place, and secondly, that with the advent of the internet, and the Snowden revelations just being a catalyst for this belated realization, a significant change has entered into the expectations of society, namely that a small part of our lives is governed by near anarchy, where anything goes and no one is accountable to anything, for anything or to anyone. This refuge from the daily laws and regulated life worked arguably fine, but has now become such a dominant part of our lives, that the status quo is not maintainable, as much as it may be desirable by some parties.

V. Conclusion and Future Work

The usage of cloud storage for criminal purposes is well known and will most likely not end. The eradication of crime is equally a noble cause, yet not one which seems a realistic prospect, and without any intention of entering into a philosophical discourse on human nature and societies. The fact that criminals and crime and their methods will continue to evolve in pace with and take advantage of technological development and innovations, is equally acknowledged. And the central aspect is that this is not necessarily an existential threat. As such, the proposed solution of moving away from expressing concerns about encryption, and moving towards individual responsibility and accepting the advancement of technology sometimes requiring an adaptation of law, should find less objection, as it specifically acknowledges the concerns about mass-surveillance and privacy of the individual, and makes the decryption an individualized order, rather than a mainstream standardization. Overall, the continuous development of cloud and virtualization services is permeating from a business exclusive aspect, to a mainstream consumer product. At the same time, encryption as demonstrated extensively above is equally advancing into a main stream feature. This has the potential to become a perfect storm for law enforcement investigations, at least as regards the currently deployed tactics. Equally, from a business provider's aspect, it is the ideal scenario, of being incapable of being blamed or held accountable for the abuse of its own services for criminal purposes, and that inability to detect it being in essence the fundamental business model.

With the proposed (re-)introduction of the superiority and binding nature of the orders of a court to any citizen in its jurisdiction, society will ideally be able to reflect and realize that indeed, the notion of mass surveillance is at least in its current format, coming to an end – and that the intention pursued by law enforcement is not to know everything, about everyone at any time, but rather to be in a position to tackle specifically organized crime and terrorism, which should not be thwarted based on business decisions by private industry. Will the proposed solution make everyone happy? No. Will it hinder law enforcement in their investigations of volume based child abuse material investigations? Probably yes. Is this however a price to pay, to lead police to adopt and focus their resources on higher value targets, and to provide a feeling of privacy towards the citizen, with the ultimate result hopefully being a commencement of the rebuilding of trust towards law enforcement and government? Yes, we feel strongly that this is the case, and is hopeful that the humble proposals made, the arguments advanced, and the overall value of this paper will see some discussion towards this goal. The solution proposed in this paper also helps us in developing a framework for mobile cloud investigation [14].

References

[1] R. Rosenbaum, "Secrets of the little blue box," Esquire, pp. 166 -182, October 1971

[2] Evidence Eliminator, "Welcome to the Evidence Eliminator™," Robin Hood Software, [Online]. Available: http://web.archive.org/web/20030216044138/http://www.evidence-eliminator.com/dis-information.d2w. [Accessed 10 6 2015].

[3] Apple.com, "Safety. Built right in.," [Online]. Available: https://www.apple.com/osx/what-is/security/ [Accessed 15 6 2015]

[4] Microsoft, "Uw bestanden beveiligen met apparaatversleuteling," Microsoft, [Online]. Available: http://windows.microsoft.com/nl-nl/windows-8/using-device-encryption. [Accessed 10 July 2015]

[5] A. Hern, "Apple defies FBI and offers encryption by default on new operating sytem," The Guardian, 17 October 2014. [Online]. Available: http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx. [Accessed 12 7 2015].

[6] Wikipedia, "Deniable Encryption," [Online]. Available: https://en.wikipedia.org/wiki/Deniable_encryption. [Accessed 04/2015].

[7] European Commission, "EU Expert Group on Cloud Computing Contracts - Questions for the Discussion on Subcontracting," [Online]. Available: http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion_paper_en.pdf .[Accessed 04 2015]

[8] J. Dykstra, "Seizing Electronic Evidence from Cloud Computing Environments," in Cybercrime and Cloud Forensics: Applications for Investigation Processes, Hershey, IGI Global, 2013, pp. 156-185.

[9] J. M. Cauthen, "Executing Search Warrants in the Cloud," 7 October 2014. [Online]. Available: https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud. [Accessed 12 5 2015].

[10] I. Drago, "Inside Dropbox: Understanding Personal Cloud Storage Services," in Internet Measurement Conference, Boston, 2012

[11] C. Timberg, "Apple will no longer unlock most iPhones, iPads for police, even with search warrants," The Washington Post, 18 September 2014.

[12] Millward Brown, "BrandZ Top 100 Most Valuabe Global Brands 2015," Millward Brown, New York City, 2015

[13] C. Timberg and G. Miller, "FBI blasts Apple and Google for locking them out of phones," The Washington Post, 25 September 2014

[14] M. Faheem, M-T. Kechadi and N-A. Le-Khac, "The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends", International Journal of Digital Crime and Forensics (IJDCF), Vol.7(2) pp.1-19