
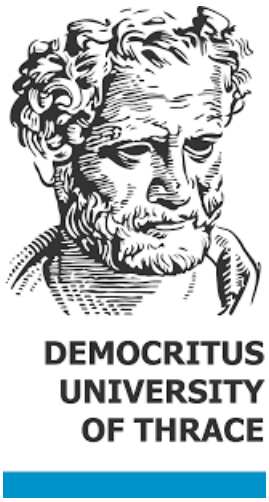


DEPARTMENT OF APPLIED INFORMATICS

FACULTY OF LAW

INTERDISCIPLINARY POSTGRADUATE PROGRAM

**Master of Science in "LAW AND INFORMATICS"**

# THE CHALLENGES POSED BY CLOUD STORAGE IN DIGITAL FORENSICS

Thesis of Christos A. Karagiannis

Thessaloniki, October 2020

# THE CHALLENGES POSED BY CLOUD STORAGE IN DIGITAL FORENSICS

**Christos A. Karagiannis**

B.Sc. in Law, Faculty of Law

Aristotle University of Thessaloniki, 2002

M.Sc. Thesis

submitted as a partial fulfillment of the requirements for

**THE DEGREE OF MASTER OF SCIENCE IN «Law and Informatics»**

Supervisor: Assoc. Prof. Kostas Vergidis

*Approved by examining board on 31 October 2020*

| | | |
|---|---|---|
| Assoc. Prof. Kostas Vergidis | Prof. Theocharis Dalakouras | Asst. Prof. Sofia Petridou |
| _____ | _____ | _____ |

## Abstract

Internet's ever-evolving capabilities make life easier for everyone, including people on the wrong side of the law. One of the most fascinating ideas of the last decade is having electronic data readily available and easily accessible, while their physical storage environment is kept away, protected and running by third parties that respect and safeguard the privacy of the content. This thesis details a comprehensive approach towards "Cloud Storage" and the practical obstacles that law enforcement authorities have to overcome when trying to uphold the law and protect a state's citizens, without compromising a criminal suspect's rights to privacy and due procedure. It examines different legal approaches to 3 main challenges (territoriality, possession, capture procedure) that arise due to the technological wonders that wrongdoers have at their disposal.



## Key Words and Phrases

Cybercrime, Cloud Model, Cloud Storage, Digital Evidence, ACPO Guidelines, Territoriality, Possession, Seizure, Transborder Access to Stored Computer Data, Power Of Disposal

## Acknowledgements

This thesis is the culmination of an intensive and personally challenging period of exploring a brand-new-to-me field of knowledge focusing on “Applied Informatics” and “Information and Communication Technologies”. I have the moral obligation to thank all the educational staff of this unique and cutting-edge Interdisciplinary Postgraduate Program, who opened new doors of the mind for me and other bright students. Even though we came equipped with a conceptually different academic background, they kindly and wholeheartedly provided us with the tools we needed to not only step up our academic status but also understand a little better the brave new world we live in.

Special thanks to my supervisor Associate Professor Kostas Vergidis. His benevolent character and his constructive feedback where the real beacons that made the completion of this research possible and his kind words function as a sprigboard for further academic exploration.

Finally, none of this would have been possible without the encouragement and active support of my beloved wife Dimitra and my precious boys, Tasos and Ilias. They are the true driving force behind my constant efforts to personally evolve and to change our vast world for the better, even by a single grain of sand.

“To Infinity and Beyond” – Buzz Lightyear

# Table of Contents

## Chapter 1: Introduction

"Space… the final frontier…". This is perhaps the most famous opening line in television history. On 8 September 1966, echoing the hopes of a generation aiming to surpass the confined boundaries of its planet, Captain James Tiberius Kirk's introductory monologue in the science fiction television series "Star Trek"[1], invited viewers to witness the wonders of the vast and still uncharted off-earth cosmos. Since then, space and the material world have been thoroughly investigated and people gradually shifted their attention to the "virtual world", a brand new non-tangible dimension that has the distinct characteristic to be easily accessible to everyone. Nearly every piece of information available is digitized and things move from paper to the so-called "immaterial world" (a conception that basically is not true, since digital information is stored in tangible mediums). One of the most fascinating technological developments of the last decade is the opportunity given to people to safely store vast amount of information in remote places that can be accessed on-demand from every corner of the earth. These interconnected "storing places" comprise the famous "cloud", where all the data-information flows and waits to be re-called by its users. This postgraduate-Master of Science thesis' springboard is the need to chart the basic problems that arise in situations where the aforementioned wondrous technological capability of remote-cloud storage of digital information gets criminally abused. It aims to provide a comprehensive approach to the practical and also legal issues that arise when a perpetrator of a criminal act "hides in the cloud" essential to the criminal procedure electronic data, that need to be obtained by law enforcement authorities in order to fully and thoroughly investigate the case against him. It will not concern itself with the cloud-stored publicly available

[1] https://en.wikipedia.org/wiki/Star_Trek:_The_Original_Series (accessed on 29-9-20)

(open source) data, since this kind of data is easily accessible to anyone around the globe under the self-evident choice of the "data-master" to display them so. The interesting cases are the situations where law enforcement authorities try to spot, identify and acquire electronic data-digital evidence that is stored "somewhere in the clouds" and the person-of-interest does not necessarily facilitate their work.

In order to complete the task at hand, it was evident that this thesis should be comprised of 2 main parts: the technological and the legal one. Chapter 2 presents an overview of the definition and the specific features of electronic data/evidence. It logs the distinct characteristics that set them apart from the rest of the evidence in a penal procedure and registers the way the law enforcement authorities handle them with conventional methods, while trying to equally balance the suspect's rights to privacy and due procedure and the need of a sovereign state to protect its citizens by fully grasping and examining every thread of evidence that is essential to a person's criminal treatment. Chapter 3 presents the architecture of "the cloud" and how it actually works. The description of this technology's enormous benefits sets the stage for the recitation of the central practical problems that arise when a person decides to actually make use of "the cloud" with ill and malicious intent. Chapter 4 gives an elaborate description of the main legal challenges that arise when law enforcement authorities try to cope with a technologically aware criminal. It pinpoints the main practical and legal barriers that need to be overcome and records the different international approaches to the matter, with a special reference to the Greek Penal System. At the same time criticism is exercised to specific legal theories and the road to new concepts is paved through concrete proposals. Chapter 5 concludes this thesis with a vote of confidence to already newly formed legal notions, assessing the current thesis' contribution to knowledge and the limitations of this researcher's

methodology, while at the same time discusses possible future research directions.

## Chapter 2: Conceptual Delimitation of Digital Evidence – Rules of Evidence

This chapter introduces the definition of electronic data/evidence. It elaborates on their distinct and unique characteristics compared to the rest of the evidence in a penal procedure and registers the conventional forensic methods applied to them by the law enforcement authorities, who must equally balance the suspect's rights to privacy and due procedure and the need of a sovereign state to protect its citizens by fully grasping and examining every thread of evidence that is essential to a person's criminal treatment.

### 2.1 Introduction

The past decades have seen constant and unparalleled growth in online usage by individuals, companies and states alike. More and more aspects of everyday life transcend from the actual world to the so-called cyberspace, i.e. the consensual hallucination experienced daily by billions of legitimate operators in every nation and consists of constellations of data[2]. Actually the term cyberspace refers to an interactive and virtual technological environment, and more specifically, to a global computer network made up of many worldwide computer networks that employ Transmission Control Protocol/Internet Protocol *(*TCP/IP*)* to facilitate online communication and data exchange activities[3]. Being able to transmit and receive every information from the palm of your hand and in the blink of an eye is absolutely fascinating and unprecedented in human history. As nature dictates though, along with benefits in every sector, there are also drawbacks. Crime is also part of life and having a window (sic) readily available and open to almost every corner of the world,

[2] William Gibson, Neuromancer (1984)

[3] http://www.techopedia.com/definition/2493/cyberspace (accessed on 29-9-20)

means that each user of an electronic device with an ill intent has a chance to move and hide (?) his criminal actions to a remote part of the world and thus make the work of law enforcement authorities much more complex.

Fighting crime in cyberspace (cybercrime) is like performing brain surgery with a blunt scalpel. The authorities must search “post crimen” for evidence “ante crimen” in a very peculiar crime scene. They need to immerse themselves in a digital ocean of vast amount of information and try not only to acquire but also to objectify the evidence of criminal activity. They need to attribute to the digital evidence the legal certainty it needs to have, so it can serve its purpose.

## 2.2 Digital Evidence - Rules of Evidence

One of the fundamental notions in the greek penal system is the so called “principle of moral proof”. The penal judge is not obliged to use any typical and predefined rules in the process of evaluating the evidence of the case at hand. As long as each evident object is admissible, authentic, reliable and complete, he can assess it freely in order to reach his final conclusion and judicial rule[4]. Therefore it’s crystal clear why it is of the outmost importance that all of the evidence acquired meet some procedural standards aptly named “Rules of Evidence”.

According to article 13 section ζ of the Greek Penal Code (Law 4619/2019) and article 1 section b of the Budapest Convention on Cybercrime (European Treaty Series No. 185) digital/computer data is the representation of facts, information or concepts in a form that an information/computer system can process (e.g. photos, videos, sounds,

[4] Article 177 of the Greek Code of Criminal Procedure (Law 4620/2019)

texts). According to the National Standard ISO/IEC 27037:2012[5], which provides guidelines for specific activities (identification, collection, acquisition and preservation in a way that strengthens its evidential value) in handling digital evidence, the latter is identified as information or data, stored or transmitted in binary form, that may be relied on as evidence. Digital evidence is by nature extremely fragile and durable at the same time. Their content and location can be easily and swiftly altered and at the same time if they remain at the exact same state and position in which they are found, they can tell crime fighting authorities everything they need to know in an unquestionable and irrefutable way. Moreover, destroying digital evidence requires a consistent effort and usually a hands-on approach to the physical medium that contains them, since information systems that carry the data have integrity assurance mechanisms through redundancy and fault tolerance. Data redundancy is a condition created within a data storage technology in which the same piece of data is held in two separate places. Sometimes, this can occur by accident, but is also done deliberately for backup and recovery purposes. Fault tolerance is a concept particularly important to data storage infrastructure and refers to the ability of a computer system or storage subsystem to suffer failures in component hardware or software parts yet continue to function without a service interruption and most importantly without losing data or compromising safety.

## 2.3 ACPO Guidelines

Five rules must be followed when collecting electronic/digital/computer evidence and each rule corresponds to a counterpart property that evidence must have to be useful:

[5] https://www.iso.org/standard/44381.html (accessed on 29-9-20)

a) Admissibility: Digital Evidence must be collected through a legally acceptable and allowed procedure, so they can be admitted in front of court.

b) Authenticity: Digital Evidence must be tied positively and relate to the incident under investigation in a relevant way.

c) Completion: Digital Evidence must be able to uncover every aspect of the incident under investigation, thus functioning both inculpatory and exculpatory.

d) Reliability: Digital Evidence must be collected and analyzed in a way that confirms the evidence's authenticity and veracity.

e) Believability: Digital Evidence must be presented in front of a court clearly, understandable and believable[6].

In 2007, the Association of Chief Police Officers (ACPO) in the United Kingdom agreed to a good practice guide in investigating cybercrimes, that even to this day is considered universally as one of the fundamental codes of conduct and practice for practitioners working in the field of digital forensics and is also acknowledged as such by the independent Hellenic Data Protection Authority[7]. According to ACPO, every law enforcement personnel who may deal with digital evidence needs to abide by 4 principles:

a) No action taken, should change data which may subsequently be relied upon in court. This way the integrity of the collected digital evidence is guaranteed. This applies especially to at the time of collection non-

[6] Matthew Braid, Collecting Electronic Evidence After a System Compromise, Global Information Assurance Certification Paper for SANS Institute (retrieved from https://www.giac.org/paper/gsec/659/collecting-electronic-evidence-system-compromise/101519)

[7] Ruling 70/2015 (retrieved from http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=240,58,77,254,51,40,191,175)

working electronic devices, since powering-on a digital gadget gives the operational system the opportunity to read and write and therefore alter a significant amount of data and metadata[8], even before the user begins to use the electronic device in question.

b) If it's necessary to access original data, this must be done by a person, who is competent to do so and is also able to give evidence explaining the relevance and the implications of his actions. This applies especially to at the time of collection working electronic devices, since powering-off a digital gadget gives the operational system the opportunity to modify a significant amount of data and metadata and is also possible that some information is lost[9] or even destroyed if the files are encrypted and set as auto-destructive.

c) An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. All digital evidence must meet the universally acknowledged criteria of auditability, repeatability, reproducibility and justifiability.

---

[8] Metadata is data that provides information about other data. It's a series of basic information about the main file that lets the operating system understand how to deal with it, its name, type, location, size, exact dates of creation and modification and even more.

[9] RAM (Random-Access Memory) is a form of computer memory that is typically used to store working data and machine code and allows the device to work really fast, since it allows data items to be read or written in almost the same amount of time, irrespective of the physical location of data inside the memory. The downside of its use is that it's volatile, i.e. it retains its contents while powered on, but if power is removed, the temporarily stored information is lost.

d) A specific person who is leading the investigation has overall responsibility for ensuring the application of these principles and generally the law as well[10].

As is easily understandable, the first logical and most vital step in digital forensics is the acquisition of the data of interest per se. Something that, at first, is considered easy and natural: someone who is committing the crime of possessing child pornography material (photos, sounds, videos) has everything stored in a specific digital storage medium (internal or external hard drive of a personal computer, Universal Serial Bus-USB flash drive, floppy/compact/digital video-versatile disc), that is hidden away in a drawer of a desk. In that case, the law authorities need to:

a) enter and search his house, after they have secured that there is probable cause for that and they are accompanied by a Public Prosecutor or Justice of Peace (JP).

b) find and capture-confiscate the aforementioned medium using competent personnel and applying specialized techniques that ensure and guarantee the time, place and condition it was found. The medium must be at all times be accompanied by an audit trail that forms a continuous and unbroken "chain of custody"[11], so that an independent third party can at all times pinpoint i) the exact person that came into contact with the medium, as well as ii) the exact place and analyzing procedure the medium underwent and thus creating a uniqueness and singularity that

[10] ACPO Good Practice Guide for Digital Evidence (March 2012) (retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

[11] Karen Ryder, SANS Institute, Information Security Reading Group, Computer Forensics – We 've Had an Incident, Who Do We Get to Investigate (2002) (retrieved from https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652)

makes that specific medium morphologically and technologically recognizable and distinct from any other similar digital object.

c) analyze the evidence-data gathered and make them part of the criminal procedure in a coherent, believable, understandable and accordingly presentable way.

What happens though when technology gives you the opportunity to have the data in question stored "faraway, so close"[12]?

## 2.4 Summary

This chapter presented a contemporary definition of electronic data/evidence, clarifying that every piece of significant electronic data in criminal procedure is considered evidence that needs to be handled with certain scientific procedures in order for it to maintain its probative value. The following chapter delves on the newly formed technology of "the Cloud", which in the end makes the above mentioned standard forensic procedures almost obsolete.

[12] "Faraway, So Close!" (In german "In weiter Ferne, so nah!") is a 1993 German fantasy film directed by Wim Wenders

## Chapter 3: From Cloud Computing to Cloud Storage

This chapter sheds light on what actually "the cloud" is. It presents the architecture of "the cloud" and how it works, thus setting the stage for the recitation of the central practical problems that arise when a person decides to actually make use of this wondrous technology with ill and malicious intent.

### 3.1 Historical evolution of Cloud Computing

Even though the birth of cloud computing is a relatively recent phenomenon, its basic idea and root can be traced back to the 1950s, when the concept of "time sharing" first emerged. "Time sharing" used to describe the technological ability to concurrently share a computing resource (mainly data and CPU time) among multiple users by means of multi-programming and multi-tasking[13]. The users could operate simultaneously and execute computations concurrently (during overlapping time periods) instead of sequentially, with one completing before the next starts. This concept, that apparently was first introduced by John Backus in 1954[14], planted the seeds in John McCarthy's mind, who in 1961 floated the idea of "utility computing", as the potentiality of providing computation as public service, just like any other service[15] and

[13] Peter Clark, DEC TIMESHARING, The DEC Professional, Vol. 1, Number 1 (1965)

[14] John Backus, Computer Advanced Coding Techniques, MIT (1954)

[15] Cloud computing implements the idea of utility computing but can also be compared to cluster computing, which views a group of linked computers as a single virtual computer for high-performance computing (HPC) or grid computing, where the linked computers tend to be geographically distributed to solve a common problem. (retrieved from https://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/)

also in Joseph Carl Robnett Licklider's (known simply as J.C.R. or "Lick") mind, who in 1963 envisioned everyone on the globe to be interconnected and accessing programs and data at any site, from anywhere as part of an Intergalactic Computer Network[16]. Lick's idea eventually evolved into ARPANET (Advanced Research Projects Agency Network) of the United States Department of Defense, the first wide-area packet-switching network with distributed control and implementation of TCP/IP protocol suite, that served as the platform that the Internet as we know it today was based on.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[17]. The resources present in the cloud can be used infinitely and whenever needed by users, who, instead of setting up their own physical infrastructure, prefer to use the resources as a service and thus shift and outsource the workload and consequently reduce the pressuring demand for more and better hardware and software, which is handled by other networks of powerful and readily available computers that form "the cloud". The Cloud is delivered to any internet enabled

[16] J. C. R. Licklider, Memorandum For Members and Affiliates of the Intergalactic Computer Network, April 23, 1963 (retrieved from https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network)

[17] National Institute of Standards and Tecnology of United States Department of Commerce, The NIST Definition of Cloud Computing, Special Publication 800-145 (retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)

device and the only thing that is required in order to be able to access it is a simple web browser (Mozilla Firefox, Google Chrome, Microsoft Edge, Opera, etc.)[18].

The Cloud model is generally composed of five essential characteristics, three service models and four deployment models.

## 3.2 Essential Characteristics

The Cloud model has 5 distinguishable characteristics that give the end-user high-end capabilities that usually correspond to bigger, more expensive and more powerful machinery:

A) **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

B) **Broad Network Access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (mobile phones, tablets, laptops and workstations).

C) **Resource Pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (continent, country, state

[18] Rajleen Kaur et al, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (5) (2014), 6060-6063

or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

D) **Rapid Elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

E) **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

## 3.3 Service Models

The Cloud technology is widely and publicly offered in 3 versatile models, each one meeting the perspective different needs of different end-users:

A) **Software as a Service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[19]. The applications run and store their data online and are

[19] A cloud infrastructure is the collection of hardware and software that actually enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

B) **Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

C) **Infrastructure as a Service (IaaS)**: The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly limited control of select networking components (e.g. host firewalls). Essentially, the consumer outsources the hardware needed not just for computing power, but for storage as well and ultimately combines compute and cloud storage.

## 3.4 Deployment Models

Depending on the end-users special needs the Cloud model can take 4 distinctive forms:

A) **Private Cloud**: The cloud infrastructure is provisioned for exclusive use by a single user (usually an organization) comprising of multiple consumers (e.g. business units). It may be owned, managed, and operated by the main user-organization, a third party, or some combination of them and it may exist on or off premises.

B) **Community Cloud**: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the users-organizations in the community, a third party, or some combination of them and it may exist on or off premises.

C) **Public Cloud**: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic or government organization or some combination of them. It exists on the premises of the cloud provider.

D) **Hybrid Cloud**: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g cloud bursting for load balancing between clouds).

## 3.5 Cloud Storage

Spawned from Cloud Computing and arguably as an interconnected service of it, comes “Cloud Storage”, a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers (sometimes in multiple locations) and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for

keeping the data available and accessible and the physical environment protected and running. The main difference between the 2 aforementioned concepts is that Cloud Storage focuses on data storage, whereas Cloud Computing is all about remote processing of data[20].

## 3.6 Summary

This chapter presented the different ways that the cloud is built and offered to the end-users. The description of its enormous capabilities acts as a prologue to the critical analysis of the central practical problems law enforcement authorities face, which can be found in the next chapter.

[20] Ian Johnson, Difference Between Cloud Storage And Cloud Computing, (Nov. 20 2019) (retrieved from https://medium.com/@ianjohnsonenn/difference-between-cloud-storage-and-cloud-computing-d95d3385ae9e )

## Chapter 4: Moving the evidence to the Cloud

This chapter gives an elaborate description of the main legal challenges that arise when law enforcement authorities try to cope with a technologically aware criminal. It pinpoints the main practical and legal barriers that need to be overcome and records the different international approaches to the matter, with a special reference to the Greek Penal System. At the same time criticism is exercised to specific legal theories and the road to new concepts is paved through concrete proposals.

### 4.1 Introduction

What happens when someone makes use of this innovative technology called cloud storage that actually allows him to have readily available a piece of digital evidence which is of criminal interest? There are 3 main issues raised in this case, that correspond to the specific attributes of the Cloud: territoriality, the notion of "possession" and the procedure of locating, preserving and capturing cloud-based digital evidence.

### 4.2 Territoriality

For data redundancy and performance-latency optimization reasons, every cloud storage provider uses several servers, scattered all around the globe. Every time a user uploads a file to the cloud, that same file is automatically multiplied (most of the time it's at least triplicated) and is stored and held in at least two separate geographical places and physical locations, usually not just in different buildings but rather in different countries and even in different continents. This way a) in the case of a temporarily massive technical problem (abrupt maintenance need, power disruption, malevolent security breach) or a catastrophic event (natural disaster, terrorist attack), that leads to wide server failure

and consequently possible data loss in one data storage center, the file in question remains safe and intact on the other servers and b) when the user shifts location and changes his whereabouts around the world, the file in question is always available on-demand by the data center that is geographically closest to him, efficiently delivering the file to the user with Quality-of-Service (QoS) guarantees[21] and the lowest possible propagation delay[22]. So, it's becoming clearer that when someone uses cloud storage, data behave like a little cartoon cloud that constantly follow the user and on the grounds of suffering enduring relocation, one can speak of an allegedly "bilocation" or "multilocation"[23] of data.

So what about territoriality in cyberspace? Where do digital evidence actually reside and which country's legal system is in play? How does the cloud, which in essence is a collection of storage servers constantly making internal and architectural repositioning of data in a

[21] Cloud Storage works in a Guaranteed-Service Model (GSM) that aims at delivering the requested file in optimal time without compromising the integrity and quality of it

[22] Propagation delay is the length of time it takes for a digital signal-packet-file to travel to its destination through a specific medium of transmission (copper wire, optical fiber, wireless communication channels) and it's equal to **d / s** (or vf), where **d** is the distance between point A and point B calculated in meters and **s** is the wave propagation speed (or velocity factor) of the transmission medium calculated in meters/second. It's actually clear that the longer the distance the data must travel, the longer it will take to reach its destination.

[23] The american sceptic and investigator of the paranormal Joe Nickell in his book "Looking for a Miracle: Weeping Icons, Relics, Stigmata, Visions & Healing Cures" (1993), defines "bilocation", or sometimes "multilocation", as an alleged miraculous ability wherein an object is located (or appears to be located) in two distinct places at the same time.

handful of geo-dispersed locations, affect the classic meaning of "on-site crime scene"?

A Cloud Provider's corporate headquarters may be located in one country, the Data Center may be located in another country and the End-User may be located in a third country. If you add to that already complex technological and legal mixture the fact that even neither the end-user nor the cloud provider know the exact location of each file any given time[24], it's pretty obvious that any law enforcement authority has a major territoriality problem to deal with.

One may offer various approaches to solve the aforementioned "loss of exact location" of digital evidence in the "cloud world". Two territorial and two extraterritorial in nature.

The first and most obvious one is also the oldest. According to the roman "lex loci delicti commissi"[25], in determining the legislation of the country one must apply, crucial is the place where the criminal event occurs ("Criminal Event Theory" based on the territorial principle of international law[26]). In the case of cloud storage one must pinpoint where the digital data in question is stored, viz the physical location of the Data Center that hosts the digital evidence. Since the file is hosted in multiple servers, all states that accommodate data centers may equally exercise their penal jurisdiction.

---

[24] The provider and the final user of cloud storage can agree to a restriction against offshore or generally outbound data flow to foreign countries, including a requirement that the data center, that hosts the files in question, be located within a certain country

[25] Latin proverbial phrase for "law of the place where the delict (tort) was committed"

[26] Gideon Boas, Public International Law: Contemporary Principle and Perspectives (2012)

The second territorial approach shifts the attention to the medium with which the crime has been committed. Derived from the ancient "lex loci rei sitae"[27] this version sets as applicable the legislation of the country where the instrument that made the criminal event a reality resides (Theory Of Criminal Instrument), viz the physical location of Cloud Provider's corporate headquarters or even its Sales Office.

Both territorial scopes alone are problematic though. A criminal surely wants not only to avoid his eventual prosecution, but also make sure that if caught red-handed, his penal treatment will be the most favorable to him. With that in mind and by using the aforementioned way the cloud storage works, criminals can actually manipulate penal jurisdiction of the states, indulging in "forum shopping", that is the practice of having your legal case heard in the court thought most likely to provide a favorable judgment or as is more aptly called jurisdictional arbitrage, which has been frequently utilized by transnational criminals to hinder attempts at governmental prosecution [28] [29]. Furthermore, within european boundaries and according to article 50 of the Charter of Fundamental Rights Of The European Union (2016/C 202/02) applies the acclaimed principal of "non bis in idem"[30], which in effect means that "no

[27] Latin proverbial phrase for "law of the place where the property is situated"

[28] Nir Kshetri, Pattern of Global Cyber War and Crime: A Conceptual Framework, Journal of International Management, 11(4), (2005)

[29] J. Adams, Virtual defense. Foreign Affairs (2001)

[30] Most of the times referred to as "ne bis in idem", it literally translates from Latin as "not twice against the same (thing)" and is a legal doctrine to the effect that no legal action can be instituted twice for the same cause of action. This legal concept originates in Roman Civil Law and essentially the equivalent of the modern-day double jeopardy (autrefois acquit) doctrine found in common law jurisdictions,

one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law". In addition, the application of the same principal at international level is governed by mutual treaties between sovereign states, thus making it harder not only to locate, acquire and penally assess a criminally interesting digital file, but also raises another set of problems involving a) the possible absolute absence of such an agreement on interstate mutual co-operation on criminal matters and b) the possibility of the content of the file not being penally outlawed or constituting a crime according to the legal system of the country, where the data center actually resides.

The third approach to the problem at hand and first of the ones extraterritorial in nature takes into consideration the place where the actual direct consequence or final effects of the crime are realized (Direct Consequence Theory), viz the location of the end-user. A criminal resides in Greece and the digital file in question is located in a data center in Nigeria. The core question here is if you can actually prosecute a person in Greece for a digital file that in reality is physically located in another country.

Finally, the fourth approach and second of the ones extraterritorial in nature uses as decisive criterion the nationality either of the perpetrator or the victim of the criminal act (Nationality Principle). What's important is not the place where the crime is committed but rather the legal bond that is formed between a nation and its citizens and the undisputed authority of a country to enforce its laws to the civilians who carry similar citizenship, regardless of their whereabouts.

---

prohibiting two simultaneously or consecutive criminal proceedings for the same criminal offence.

Both extraterritorial scopes alone are also problematic, leading to a more pressing question that cloud storage raises. How is possession defined in the era of the virtually limitless world? Who is in "possession of" and thus responsible for the illegal digital content that the law authorities are trying to apprehend?

### 4.3 Managing a digital file: "Viewing", "Possessing" and "Accessing" it

The concept of "possession" seems intuitive when one thinks of a physical object: holding something, touching it, feeling it, having it physically present. Therefore, mere viewing, even window-shopping, does not constitute possession of what is on the other side of the glass because one cannot hold it, touch it or feel it. In contrast, the somewhat elusive concept of "possessing digital files" is easily identifiable but hardly manageable using the classic way of thinking.

Possession is a reference concept, i.e. a notion that always refers to a specific object and its exact meaning changes like a chameleon, depending on the special attributes of the object and the ever-evolving need to protect it efficiently.

When someone stores data in the cloud, he is actually like using someone else's device, which in turn not only lies somewhere remote and physically inaccessible in relation to the end-user, but has a different person responsible and liable for its managing and preservation. Users do not download files on their own device or computer, because all storage is handled and maintained by the cloud server provider. Additionally a cloud user may permit shared access to his files by designated users and by doing so, others may access-see his data at any time. Moreover, due to their ever-shifting location, often is unclear if data are actually stored in a specific place or in transit to their next station of storage. This makes

clear that digital evidence (i.e. a child-pornography file-photo) can be found in a plethora of computer-information system[31] in many different ways.

At this point, it must be clarified that the Cloud Storage Provider is, from a legal point of view, not in possession of any data. According to the architecture of the Cloud as already described, the private entity-company provides the hosting service (IaaS) and is responsible for the maintenance of the physical medium that holds the data, but since the provider is not allowed to monitor the content of the data that is stored, one cannot make a case of criminally interesting possession against it. Some Cloud Storage Providers, while trying to uphold a public image with strong corporate social responsibility elements, are developing and employing filtering techniques to suppress access to potentially illegal digital files, but that does not change the fact that they don't have actual control over the user-generated content stored on their premises.

Initially one must determine the exact moment in someone's course of actions that having something readily available through cloud storage becomes penally interesting. If a person has a file stored away in a Cloud Server but never views it, can he be held liable for that? Can it be considered a crime, having something illegal stored but never coming in contact with it? Given that two of digital age's main characteristics are the vast amount of data being transmitted through electronic devices and the admittedly frequent cases where the end-user doesn't have full supervision over every single file that can be found at his disposal, it has

[31] According to N. Παρασκευόπουλος/Ε. Φυτράκης, Αξιόποινες Σεξουαλικές Πράξεις, Εκδόσεις Σάκκουλα, 2011 the definition "Computer-Information System" covers every desktop or portable digital device with the ability to store, project and process digital data and naturally includes tablets and smartphones

been argued that in order to hold someone accountable for "possessing" a specific file requires as a minimum the fact that he "viewed" it at least once[32]. Otherwise one cannot make a case nor about "possessing", neither about an ill knowledge and intent on behalf of the end-user. One must inevitably spot flow-transfer of data towards the end-user's specific and in-use electronic device, regardless if the user only temporarily views or additionally downloads the file in question, so he can have it under his direct command and can at any time verify that the data is there and can be administered according to his will[33] [34].

From a technician's point of view, when the end-user recalls from the cloud server and views on-line the file in question on his physically handy electronic device, the image-photo is automatically written on the device's RAM, from which it is again automatically removed-erased, as soon as the end-user leaves the cloud platform and moves on to other business. Moreover, when the end-user views on-line the file in question while connecting to the cloud using a web browser, the latter program generates a duplicate copy of that file and stores it on web cache[35] of the device, in order to facilitate faster viewing of it in the future. Unless the

[32] Μαρία Καϊάφα-Γκμπάντι, Διαδικτυακές προσβολές της ανηλικότητας, Ποινικά Χρονικά 2012, 161

[33] Παύλος Ανδρεάδης-Παπαδημητρίου, Η πορνογραφία ανηλίκων στην εποχή του υπολογιστικού νέφους, Σκέψεις με αφορμή το Ν. 4267/2014, Ποινική Δικαιοσύνη 2015, 454

[34] ΜΟΔ Κατερίνης [Mixed Jury Court of Katerini (GR), Ruling…] 19-22/2009, Ποινική Δικαιοσύνη 2010, 1125

[35] A web cache (or HTTP cache) is an information technology for the temporary storage (caching) of web documents, such as web pages, images, and other types of web multimedia, to reduce server lag. A web cache system stores copies of documents passing through it and subsequent requests may be satisfied from the cache if certain conditions are met.

end-user sets his browser not to store the so-called temporary internet files on web cache, this procedure takes place automatically and the duplicate temporary files are reserved until they are substituted by new ones due to the finite capacity of web cache, or until the end-user chooses to delete them. As a result, a file-an image that the end-user viewed on his screen but never downloaded on his device, remains stored in RAM and in web cache for a significant amount of time.

It has been argued that since the end-user, while "only viewing" the file, can manipulate the data according to his will, this short period of time that the file is written on RAM and/or web cache can constitute possession[36]. The problematic point of this opinion is that an involuntary and automatic procedure that is applied in every single electronic device leads to the general conclusion that "viewing" is actually a form of possession. It's like arguing that anyone who passes by a newspaper stand and reads the first page of the hanging newspapers, even for quite a long time, but eventually never buys them and returns home without actually "owning" them, in the end is in possession of them. RAM storage lacks in duration and stability, since its finite storing capability ends either when new and more recent user-generated data are loaded-written on it or when the power supply is disrupted voluntarily or by accident. The on-screen projection of data is just the medium needed so that the end-user perceives and comes "in contact" with data that is already stored beyond RAM and always available for access. Technically the screen does not

---

[36] Giannina Marin, Possession of Child Pornography: Should You be Convicted When the Computer Cache Does the Saving for You?, Florida Law Review, Volume 60 (2008) (retrieved from http://www.floridalawreview.com/wp-content/uploads/2010/01/Marin_BOOK.pdf )

operate nor can be used as a storage medium. Every on-screen projection prerequires data storage but in the end this mustn't be confused or identified with it. These are procedures that are objectively and technically distinct, independent and essentially different, while theoretically can be carried out from different persons[37].

Possession's defining characteristics are not just the longevity and/or the constancy of the power of command over the data. Possession is grounded not only on the simple legal or physical power over the physical medium of the storing device, but additionally on the actual ability and real opportunity of accessing and managing the data in question. Access is in reality the next-level evolution stage of possession and is mainly grounded on the acknowledgement that having a file readily available to absolutely manage and control it in any way possible is a notion that is not necessarily connected with the ability to master the physical storage medium. It must be pointed out though that in order to refrain from an excessive dilatation of the notion of "possession", one should add as a minimum parameter to the equasion at hand, the objectively found act of creating, preserving and ultimately accessing the data in question from the person of interest. If somebody knows that a specific file with illegal content is readily available through a cloud storage server and can freely access it, but in the end never opens or manages or even distributes it in any way, one cannot be held accountable for possessing the data.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual

[37] Γεώργιος Μπούρμας, Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας (με αφορμή τη ΣυμβΑΠ 810/2007, ΠοινΔικ 2007.813), ΠοινΔικ 2009.322

exploitation of children and child pornography[38] distinguishes the 3 concepts ("simply viewing" - "possessing" - "accessing") and while making the notion of "viewing" essentially irrelevant to penal procedures, it leaves "possessing" to its classic meaning, grounding it on actually having the file in question downloaded and stored in a physical medium, handily available to the end-user (Article 5§2). In addition, it outlines the concept of "accessing" stating that it should be considered that a crime is committed when a person knowingly obtains access to child pornography by means of information and communication technology. To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. The intentional nature of the offence may notably be deduced from the fact that it is recurrent or that the offence was committed via a service in return for payment (18th Preliminary Thought).

As already outlined Cloud Storage constitutes a questionable area that resides between the latter two concepts of "possessing" and "accessing", thus making it further more pressing to re-evaluate the former original notions through the lens of the ever-evolving technology.

According to Ruling 613/2016 of the Misdemeanor Council of Athens (GR)[39] "*Cloud Storage is not just a place to safely maintain digital data, but is mainly used for large files' transfer between electronic devices. On the grounds of having to create an account and use an appropriate password in order to access the storage service provided by*

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093 (accessed on 29-9-20)

[39] Συμβούλιο Πλημμελειοδικών Αθηνών 613/2016, Ποινική Δικαιοσύνη 2016, 424

*the company who actually owns the server, it is doubtful that cloud storage, whose technological facilities will most likely reside in another country, can be contemplated as an actual part of a specific electronic device*". The majority of the judges chose to approach the matter of Cloud Storage as a Service that is provided to the end-user, through which the latter accesses the data in question and has the opportunity to either view them on-line or even to download them on his electronic device. If downloading occurs then we move to the area of crystal clear "possession". But when the user simply views on-line and comes in contact with the illegal content only for a brief period of time, one cannot set it as "possession" but rather as penally indifferent "view". On the same matter and as a part of the same ruling, one of the judges of the aforementioned Council found that *"by using a cloud storage service, a user has the ability to store, access and process data, that can be found in remote locations and servers, namely "in the cloud". Considering the end-user, who through the use of an identification process (username and password) accesses the server that hosts his data, can, regardless the location of the server, manage (view, present, modify, transfer, copy, delete) his digital files at will, one can contend that since storing digital data in the cloud is the exact thing as if data were stored on a physically accessible medium. Cloud should be considered and legally treated as a virtual and remote external storage medium, that actually is an extention of the every digital device that has access to it"*. The minority judge found that the crucial element on which the criminal responsibility is founded is that of the willful and knowingly access to the files in question through personal and positive act. Even if the end-user doesn't download the file in his computer and only views it on-line, he is liable for accessing it on his own free will. The automatic technological procedure of the file/image being written on RAM or Web Cache is indifferent and

the decisive factor is that of the personal action of the user to make contact with a readily available file. The minority judge's conclusion resonates with the at first oxymoron notion that Cloud Storage is a tangible storage device that is virtually an extention of the locally handy electronic device of the end-user. This way of thinking leads to a step-by-step transformation of the notion of possession, which is slowly transcending from a bricks-and-mortar world to a virtual environment that itself constitutes the latest battleground between law enforcement authorities and criminals[40].

### 4.4 Locating - Distinguishing, Preserving and Capturing Procedure

The technology of the cloud has files stored in a shared pool of computer resources on the Internet, accessible from any computer.

#### 4.4.1 Locating – Distinguishing

This means that every server of the Cloud Storage provider handles and accommodates a really large amount of data coming from different users around the globe. For obvious financial reasons, each end-user doesn't have a specific server assigned to him but rather on the same system/server can be found data stemming from various users. The probably unused storage room of a server is harvested and reused as storage room for other guests of the same server. That immediately causes room for speculation over the ability to authenticate each digital file in question and emphasizes authenticity as one of the critical

[40] Audrey Rogers, From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws, St. John's Law Review Volume 87 (Fall 2013), Number 4, Article 5 (retrieved from https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=6662&context=lawreview)

admission-in-the-penal-procedure issues that is unique to the cloud. How can anyone attribute a specific file to a certain user? The answer comes from the way Cloud Storage works. When the end-user stores data in the cloud, a specific area of it is assigned to him and only he can actually access it, using a certain identification process (use of unique username and secret password). Each data that the end-user accesses has its own additional information (metadata and logs) and can be combined with the operating system that the Cloud Provider uses to logically allocate data to specific servers and individual users. This will result in a meaningful and irrefutable proof of authenticity connecting the digital evidence in question to a specific cloud customer/end-user[41].

### 4.4.2 Preserving

As already stated digital files/computer data are extremely volatile and through cloud storage technology one can alter them in a flash without even having to go near them. So it's understandable that after locating the data of interest and before they acquire them, the law authorities have to make certain that the data remain intact. Articles 16 and 29 of the Budapest Convention on Cybercrime (Council of Europe' s European Treaty 185/23-11-2001 that entered into force on 1 July 2004)[42] states that signatory Countries are obliged to take legislative measures regarding a potentially expedited preservation of specified stored

---

[41] Ivan Orton, Aaron Alva, Barbara Endicott-Popovsky, Legal Process and Requirements for Cloud Forensic Investigations, Information Resources Managing Association (USA), Cloud Technology: Concepts, Methodologies, Tools and Applications (2014), pp.332

[42] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed on 29-9-20)

computer data that have been stored by means of a computer system, located within their territory in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. In these cases an appropriate court order is issued by another country's requesting law authority that commands a person in the receiving country to preserve and maintain the integrity of specified stored computer data in the person's possession or control for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek their disclosure, through mutual legal assistance. As of September 2019, 64 states, including the United States of America, where the majority of the main Cloud Storage Providers reside, have ratified the convention, while a further four states had signed the convention but not ratified it, thus making it the first multilateral legally binding instrument to regulate cybercrime[43].

### 4.4.3 Capturing

Despite the universal scale of the challenges described in this thesis, different legal philosophies and systems led to different international approaches to the matter of capturing-confiscating the cloud-based electronic evidence in question.

A) **The United States of America approach**

[43] Jonathan Clough, A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization, Monash University Law Review Vol 40, No 3, (2014) (Retrieved from https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf )

The first legislative attempt to regulate the law authorities' need to capture stored computer data came from the United States of America in 1986 with the Stored Communication Act, codified at Title 18 of the United States Code, which is the main criminal code of the aforementioned federal government. Through a certain legal procedure the government is allowed and able to compel a Cloud Storage Provider to disclose customer content and non-content information[44]. On the matter of the application of the Stored Communication Act to extraterritorial jurisdiction, the United States of America's law authorities were supposedly allowed "to compel a company subject to U.S. jurisdiction to produce evidence stored outside of the United States if the evidence is within the company's possession, custody, or control"[45]. But as the years passed by, people became more aware of the novelties of the digital world and on the grounds of data protection concerns steadily rising around the globe, they started questioning the aforementioned power of their state. In 2013 Microsoft challenged a warrant of the U.S. federal government to turn over data of a target account that was stored in Ireland, where the company had its services located, stating that the law authorities' digital evidence acquisition's legal process has territorial limitations and could not extend to another country's soil, without using the international Mutual Legal Assistance Treaties. While a final judicial ruling on the "Microsoft Corp. v. United States" case was still pending, the U.S. Government drafted in 2015 the so-called LEADS Act (an acronym for Law Enforcement Access to Data Stored Abroad Act of 2015) according to which the location of the data in question is disregarded and is considered of no actual consequence in respect of a US citizen, but is determinative when dealing with a non-US citizen. This

[44] 18 U.S. Code § 2703

[45] In re Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984)

Act, that in the end failed to gain passage and was not enacted, applying the Nationality Principle[46], provided that a government may access the data of its own nationals stored abroad and therefore the cloud is deprived of territoriality but has nationality[47]. In the summer of 2016, the U.S. Court of Appeals for the Second Circuit released its decision No. 14-2985, 2016 WL 3770056 (2d Cir. July 14, 2016) for what has come to be widely known as the "*Microsoft Ireland*" case. The three-judge panel unanimously rejected the notion that the Government could obtain the contents of emails cloud-stored overseas through the provisions of the Stored Communications Act[48] and as a result called on the U.S. Congress to clarify, update and essentially modernize the Stored Communications Act for the brave new world[49]. In 2017, the U.S. Government, in a newer attempt to address the matter of transborder access to data stored abroad, drafted the International Communications Privacy Act (ICPA), that stated that U.S. based technology providers who are legally asked for, are obliged to produce the requesting cloud data, while at the same time the U.S. Government is required to notify the foreign country where the data resides of the procedure followed and the latter reserves the right to object it, if the procedure violates their laws. ICPA also failed to gain passage and was not enacted. Finally, in 2018 and while the "*Microsoft Ireland*" case was in its final stage and pending in the Supreme Court of

[46] See above under "4.2 Territoriality"

[47] Murdoch Watney, Law Enforcement Access to Evidence Stored Abroad In The Cloud, Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016, Hosted by Univesitat der Bundeswehr, Munich, Germany

[48] Thomas F. Brier, Jr, Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland, Journal of Information Policy, Vol. 7 (2017), Pen State University Press

[49] Microsoft Corp. v. United States, 130 Harvard Law Review 769 (2016)

the United States, the U.S. Government passed through the Congress the now-famous CLOUD Act (an acronym for Clarifying Lawful Overseas Use of Data Act), which acted as a way to amend the initial Stored Communication Act and as the culmination point of the two aforementioned bills that never came to be. According to the CLOUD Act federal law enforcement can compel U.S.-based technology companies to provide requested data stored on servers, regardless of whether the data are stored in the U.S. or on foreign soil[50].

B) **The International approach**

In 1997 the inter-governmental political forum called "The Group of Eight" (G8)[51] established the Subgroup of High-Tech Crime in an attempt to thwart international criminal and terrorist incidents in cyberspace. Aiming at ensuring that no criminal could take advantage of and find safe harbor in cyberspace, the G8 drafted and approved 3 main "Principles on Transborder Access to Stored Computer Data – Principles on Accessing Data Stored In A Foreign State".

[50] Retrieved from https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm

[51] G8 formed in 1997 as a group-summit of representatives of 8 of the most economically powerful, globally influential and industrialized countries of the world, comprising of Canada, France, Germany, Italy, Japan, Russia, United Kingdom and the United States of America. The European Union was always represented as well but as a "nonenumerated" participant that had the privileges and obligations of a membership. In 2014, following the annexation of the Crimean Peninsula, Russia's participation was suspended and the political forum changed its name to "Group Of Seven" (G7), nevertheless retaining its relevance as a "steering wheel of the West" (Stewart M. Patrick, The G8-It's Baaaaack! – retrieved from http://blogs.cfr.org/patrick/2011/05/24/the-g8—it's-baaaaack/)

A) Preservation of Data Stored In A Computer System: Each State shall ensure its ability to secure rapid preservation of data that is stored in a computer system, in particular data held by third parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another State.

B) Expedited Mutual Legal Assistance: Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible.

C) Transborder Access to Stored Data Not Requiring Legal Assistance: a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of accessing publicly available (open source) data, regardless of where the data is geographically located or accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data[52] [53].

Those principles essentially became the stone upon which the 2001 Budapest Convention on Cybercrime was founded. The latter is the first international treaty that is already adopted from over 60 states worldwide,

---

[52] Jason Sachowski, Digital Forensics and Investigations, People, Process, and Technologies to Defend The Enterprise (2018)

[53] Retrieved from https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf

including the United States of America, where most of the cloud storage providers maintain their business headquarters, and is seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques and increasing co-operation among nations. According to Article 32b of the Budapest Convention on Cybercrime "*a Party may, without the authorisation of another Party, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system"*. That provision presupposes that one knows for sure the exact physical location of the data and as we already argued that in not always easy to assess when dealing with cloud storage.

Another point of contention is the actual way that the Law Enforcement Authorities is going to get their hands on the cloud-stored digital evidence. Are they going to obtain them directly or via providers and other sector entities?

The most frequent scenario is that the competent Law Enforcement Authorities will have to co-operate with service providers or other private sector entities to obtain access to data cloud-stored abroad. It is understood that private sector entities operating in different countries are subject to the laws of multiple jurisdictions, and that compliance with legislation in one country may bring them in conflict with that of others. This includes in particular conflicts with human rights and rule of law principles[54].

[54] The concept of "Rule of Law" stems from the Greek philosopher and polymath Aristotle who in his "Politics" wrote that "it is more proper that law should govern than any one of the citizens", thus stating that every person is subject to the law, including people who are lawmakers, law enforcement officials and judges.

The 3 main possible scenarios are:

A) Access with consent: During criminal investigations Law Enforcement Authorities obtain the lawful and voluntary consent of a person to access computer data stored in another jurisdiction that may represent important evidence. In this case, the Law Enforcement Authorities of almost all States can access and secure (download) data, provided that the person giving, enabling and granting access to them is physically located on the territory that the Law Enforcement Authorities operate in.

B) Access without consent but with lawfully obtained credentials: Law Enforcement Authorities have lawfully obtained a password for accessing computer data with alleged illegal content or incriminating evidence. As with the first scenario, the whereabouts of the digital evidence is indifferent. Data can be accessed and secured (downloaded) and consequently used in a criminal investigation without problems.

C) Access without consent: During criminal investigations a law enforcement authority must obtain technical information from a Cloud Storage Service Provider concerning a suspect, who does not facilitate access to his data. In that case it must be clarified that "*the person who has the lawful authority to disclose the data to the Party"* may also be a Cloud Storage Service Provider or any other private sector entity holding data of an individual, only if the terms of service permit this or if the Service Provider has become the owner or has the power of disposal of the data. But for a Cloud Storage Service Provider to be in line with Article 32b of the Budapest Convention on Cybercrime, he must also consider his contractual obligation to safeguard his client's privacy. Therefore, this means that any third-party private entity would usually only be possible to disclose technical data owned by itsself, such as traffic data, subscriber information and other network data and in order to

administer to Law Enforcement Authorities any user-generated content the only possible way would be that of the time-consuming international mutual legal assistance mechanisms[55]. Attempting to speed things up and strengthen the ties between the different judicial systems towards European Integration, in 2014 the European Parliament and the Council of Europe adopted Directive 2014/41/EU/3-4-2014 regarding the European Investigation Order in criminal matters[56]. The European Investigation Order is a judicial request from one State to another regarding the collection of any kind of evidence, including the electronic ones, on behalf of the requesting State. Considering the aforementioned ability of the electronic evidence to rapidly shift state and location, combined with i) the economically understandable reluctance of the Cloud Storage Providers to retain their technical data and metadata for a very long time, ii) the sometimes time-consuming and surely different legal approach of each State on the matters of the guarantees provided, the standards met and the procedures that need to be thoroughly followed, in order for the competent Law Enforcement Authorities to obtain legal access to the content of the files per se and iii) the fact that, even within the boundaries of the European Union, not every State has the Directive 2014/41/EU/3-4-2014 enacted by national legislation[57] [58], one can easily

[55] Transborder Access and Jurisdiction: What are the options?, Report of the Transborder Group (ad-hoc sub-Group on Jurisdiction and Transborder Access to Data), adopted on 6 December 2012 by the Cybercrime Convention Committee (T-CY) of the Council of Europe (retrieved from https://rm.coe.int/16802e79e8)

[56] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041 (accessed on 29-9-20)

[57] A "Directive" is a legislative act that sets out a goal that all European Union countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals.

conclude that an issued European Investigation Order might prove insufficient in the timely fight against easily committed, speedy, anonymous and borderless cybercrimes[59].

Given that electronic evidence is needed in around 85% of criminal investigations, and in 2/3 of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction[60], soon became apparent that the European Investigation Order is not suitable for the gathering of electronic evidence. The increasing frustration among Law Enforcement Authorities led to the Proposal for a Regulation of the European Parliament and of the European Council on European Production and Preservation Orders for electronic evidence in criminal matters[61]. Like the European Investigation Order they are judicial requests that can be served directly on Cloud Storage Providers or on their legal representatives where they exist. The European

---

[58] Ireland, where, if not all, the majority of the Internet and Cloud Storage Service Providers have stationed their servers and usually their European Branch Corporate Headquarters or Sales Office, is not bound by the Directive 2014/41/EU, as it did not take part in the adoption of it.

[59] Ευάγγελος Β. Φαρμακίδης, Η Διασυνοριακή Πρόσβαση των Αρχών στα Ηλεκτρονικά Αποδεικτικά Στοιχεία σε Ποινικές Υποθέσεις, Διπλωματική Εργασία στα πλαίσια του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο και Πληροφορική» (2019) (retrieved from https://dspace.lib.uom.gr/bitstream/2159/23494/1/FarmakidisEvangelosMSc2019.pdf)

[60] European Commission's Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final (retrieved from https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf)

[61] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed on 29-9-20)

Preservation Order is the first logical step of the process where speed is of essence and is defined as *"a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production"*. Its main characteristic is that it may be issued for all criminal offences and helps prevent the removal, deletion or alteration of data, until is fully clarified if the data in question are relevant to a certain criminal investigation. If the data is deemed worthy of further investigation, then comes the issue of a European Production Order which is defined as "*a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence*". The technological model of Cloud Storage also paved the way for the interesting provision that in emergency cases or when there is a serious risk of loss of data, both Orders may be addressed to any establishment of the Service Provider in the European Union. As of June 2020, this Proposal is still going through the Ordinary Legislative Procedure of the European Union and thus the under discussion Regulation has not yet taken its final form.

## 4.5 Summary

This chapter gave an extensive critical description of the main legal challenges that law enforcement authorities face while trying to thoroughly investigate a "cloud-based" crime. It highlighted the different international approaches to the specific task, depending on the alternative legal systems and philosophies around the globe, with USA and Europe being on opposing sides of the dividing axis. The next chapter summarizes this endeavor and takes a standing point in favor of a

currently-forming and newly conceived notion that can be utilized in order to address the aforementioned problematic areas.

## 5. Discussion and Conclusions

This chapter concludes the thesis with a brief overview of the main issues that arise in "cloud forensics" and endorses an already proposed way-out of the previously described legal turmoil. Finally, it brings to light the limitations of this researcher's methodology and it presents more technologically relevant issues that need to be thoroughly examined in the future.

### 5.1 Overview

Abuse of the Internet and more specifically of the Cloud Storage Service for cyber-dependant and cyber-enabled crimes cannot be tolerated, since it may proliferate the probability of the states moving towards questionable choices in an attempt to sufficiently control the medium[62].

Cloud Storage has one main characteristic that seems to make today's legal doctrines obsolete: the loss of location of the data. Data are left in the cloud, in a non-territorial fixed state and the challenges posed by that condition urge for an alternate scope to the problem at hand beyond the classic principal of territoriality. The notion that, where digital evidence is concerned, location should play a significant matter is becoming rapidly outdated[63]. This new technological "elephant in the room" is present and we cannot simply ignore it and keep trying to evaluate, assess and confront novel situations, using laws and ways of

---

[62] Murdoch Watney, Law Enforcement Access to Evidence Stored Abroad In The Cloud, Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016, Hosted by Univesitat der Bundeswehr, Munich, Germany

[63] Jennifer Daskal, The Un-Territoriality of Data, 125 Yale Law Journal 326, 390 (2015)

thinking that originate from a different era[64]. While a raid on a company with the purpose of disclosing and confiscating needed paper documents would be a viable possibility, a raid on a data center (provided that the digital evidence in question is indeed gathered in total on a single data center and not scattered around multiple regions) would not bring similar (if any) results, unless disproportionally significant forces are used in order to find the necessary data, potentially including heavy decrypting capacities, if that was possible at all.

## 5.2 The Power of Disposal

A proposed modern and in another form already existing criterium that could be used as a legal connecting factor between the data in question and a specific person of interest can be found in the so-called power of disposal, i.e. the ability of a specific person to obtain sole or collaborative access and hold the right to alter, delete, suppress, render unusable or even exclude others from access and usage of that certain data. The power of disposal is completely detached from the parameter of physical location of the digital evidence and overcomes the already identified implications of legally defining the actual ownership of data. After all, the right of directly accessing user-generated data without any interference of third parties (private or governmental) is already recognized as a legally protected interest in articles 2 (Illegal Access) and 4 (Data Interference) of the Budapest Convention on Cybercrime[65]. The proposed European Preservation and Production Orders are a bold step

[64] Orin S. Kerr, Foreword: Accounting for Technological Change, 36 Harvard Journal of Law & Public Policy 403, 403 (2013)

[65] Jan Spoenle (Project on Cybercrime from The Economic Crime Division of the Council of Europe), Discussion Paper: Cloud Computing and Cybercrime Investigations: Territoriality vs the Power Of Disposal?, (2010) (retrieved from https://rm.coe.int/16802fa3df)

towards that direction, but also raise serious issues concerning the general fundamental rights of liberty and security as well as specific fundamental rights of the people and of the private entities-companies involved:

- The rights of the individual whose data is accessed, include the right to protection of personal data, the right to respect of private and family life, home and communications, the right to freedom of expression and assembly, the right to an effective remedy and to a fair trial, the presumption of innocence and the right of defense and last but not least the horizontal application of the principles of legality and proportionality of criminal offences and penalties.
- The rights of the service provider include the right to freedomly conduct a business and the right to an effective remedy.

All these globally renowned and applied rights must be efficiently safeguarded, since competing with criminals of the digital era cannot act as a Trojan Horse for affecting and undermining anyone's rights (criminal or law-abiding), nor can any democratic state sacrifice its principles and ultimately its soul, upon which it is founded, in the fight against cybercrime.

## 5.3 Conclusions

This thesis delved into the main legal challenges posed by Cloud Storage in digital forensics. It presented the wondrous technology of "the cloud" and pinpointed the basic problems that law enforcement authorities come up with in their task to investigate criminal incidents. By collecting several viewpoints and theories from different legal systems, it ventured to give the reader an understanding of the spectrum of legal issues that need to be met. Sadly, the strong language barrier prevented the research to be more analytic. Each legal system stems from its similar culture of its people and in order to fully understand and explore each

chosen option, one has to be able to read through tones of legal texts in many different languages, thus limiting this research to sources of english and greek language, that contain grouped references to other-language systems.

Cybercrime and digital evidence have already given law enforcement authorities multiple issues to address, beyond that of acquisition: what happens when the acquired electronic data/evidence is encrypted? does the evidence even "exist" in the physical world, without the decryption key? is it morally and legally acceptable to put pressure on someone to decrypt it? However, it all starts with gaining physical control over the evidence, a step that as already elaborated is not possible when dealing with "the cloud".

The ever-evolving cloud technology is the basis for the latest offshoot in digital forensics aptly called "cloud forensics", which calls for multidisciplinary solutions as a result of collaboration between technical, organizational and legal perspectives. As "the cloud" becomes more prevalent, we will begin to see case law develop around how cloud-based evidence is handled. Law enforcement authorities are currently moving in a legally grey area, applying national doctrines in an international matter, since no single state can declare that the entire "cyberspace" is at its disposal. Perhaps it should be considered that the prefix "cyber" actually means "connected" and after man has conquered air, land, ocean and space, cyberspace truly is "the final frontier" that need to be jointly explored and globally regulated.

## References

*(In alphabetical order)*

***Books, Articles & Papers***


1. Adams, J., Virtual defense. Foreign Affairs (2001)
2. Backus, John, Computer Advanced Coding Techniques, MIT (1954)
3. Boas, Gideon, Public International Law: Contemporary Principle and Perspectives (2012)
4. Braid, Matthew, Collecting Electronic Evidence After a System Compromise, Global Information Assurance Certification Paper for SANS Institute (retrieved from https://www.giac.org/paper/gsec/659/collecting-electronic-evidence-system-compromise/101519)
5. Brier, Jr, Thomas F., Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland, Journal of Information Policy, Vol. 7 (2017), Pen State University Press
6. Clark, Peter, DEC TIMESHARING, The DEC Professional, Vol. 1, Number 1 (1965)
7. Clough, Jonathan, A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization, Monash University Law Review Vol 40, No 3, 2014 (Retrieved from https://web.archive.org/web/20160430024621/https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf )
8. Daskal, Jennifer, The Un-Territoriality of Data, 125 Yale Law Journal 326, 390 (2015)
9. Gibson, William, Neuromancer, 1984
10. Johnson, Ian, Difference Between Cloud Storage And Cloud Computing, Nov. 20, 2019 (retrieved from

https://medium.com/@ianjohnsonenn/difference-between-cloud-storage-and-cloud-computing-d95d3385ae9e )

11. Kaur, Rajleen et al, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (5), 2014, 6060-6063
12. Kerr, Orin S., Foreword: Accounting for Technological Change, 36 Harvard Journal of Law & Public Policy 403, 403 (2013)
13. Kshetri, Nir , Pattern of Global Cyber War and Crime: A Conceptual Framework, Journal of International Management, 11(4), (2005)
14. Licklider, J. C. R., Memorandum For Members and Affiliates of the Intergalactic Computer Network, April 23, 1963 (retrieved from https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network)
15. Maillart, Jean-Baptiste, The limits of subjective territorial jurisdiction in the context of cybercrime (retrieved from https://link.springer.com/article/10.1007/s12027-018-0527-2)
16. Marin, Giannina**,** Possession of Child Pornography: Should You be Convicted When the Computer Cache Does the Saving for You?, Florida Law Review, Volume 60 (2008) (retrieved from http://www.floridalawreview.com/wp-content/uploads/2010/01/Marin_BOOK.pdf )
17. Nickell, Joe, Looking for a Miracle: Weeping Icons, Relics, Stigmata, Visions & Healing Cures, 1993
18. Orton, Ivan, Alva, Aaron, Endicott-Popovsky, Barbara, Legal Process and Requirements for Cloud Forensic Investigations, Information Resources Managing Association (USA), Cloud Technology: Concepts, Methodologies, Tools and Applications, 2014, pp.332
19. Patrick, Stewart M., The G8-It's Baaaaack! (Retrieved from http://blogs.cfr.org/patrick/2011/05/24/the-g8—it's-baaaaack/)

20. Rogers, Audrey, From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws, St. John's Law Review Volume 87, Fall 2013, Number 4, Article 5 (retrieved from https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=6662&context=lawreview)
21. Ryder, Karen, SANS Institute, Information Security Reading Group, Computer Forensics – We ’ve Had an Incident, Who Do We Get to Investigate, 2002 (retrieved from https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652)
22. Sachowski, Jason, Digital Forensics and Investigations, People, Process, and Technologies to Defend The Enterprise, 2018
23. Spoenle, Jan, (Project on Cybercrime from The Economic Crime Division of the Council of Europe), Discussion Paper: Cloud Computing and Cybercrime Investigations: Territoriality vs the Power Of Disposal?, (2010) (retrieved from https://rm.coe.int/16802fa3df)
24. Watney, Murdoch, Law Enforcement Access to Evidence Stored Abroad In The Cloud, Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016, Hosted by Univesitat der Bundeswehr, Munich, Germany
25. Ανδρεάδης-Παπαδημητρίου, Παύλος, Η πορνογραφία ανηλίκων στην εποχή του υπολογιστικού νέφους, Σκέψεις με αφορμή το Ν. 4267/2014, Ποινική Δικαιοσύνη 2015, 454
26. Καϊάφα-Γκμπάντι, Μαρία, Διαδικτυακές προσβολές της ανηλικότητας, Ποινικά Χρονικά 2012, 161
27. Κάτος, Βασίλειος, Ψηφιακά Πειστήρια, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2018

28. Μπούρμας, Γεώργιος, Προσπάθειες εννοιολογικού προσδιορισμού της κατοχής ηλεκτρονικών δεδομένων με χαρακτήρα παιδικής πορνογραφίας (με αφορμή τη ΣυμβΑΠ 810/2007, ΠοινΔικ 2007.813), ΠοινΔικ 2009.322
29. Νούσκαλης, Γεώργιος, Κατοχή και διανομή/διάθεση πορνογραφικού υλικού ανηλίκων (άρθρο 384 ΠΚ): Η νομολογιακή προσέγγιση κρίσιμων ζητημάτων ουσιαστικού και δικονομικού δικαίου, Ηλεκτρονικό Έγκλημα, Νομική Βιβλιοθήκη, 2018
30. Παρασκευόπουλος, Ν./Φυτράκης, Ε., Αξιόποινες Σεξουαλικές Πράξεις, Εκδόσεις Σάκκουλα, 2011 the definition "Computer-Information System"
31. Τσόγκας, Λάμπρος, Οι λειτουργίες του Δικαστικού Συστήματος αντιμέτωπες με τις προκλήσεις της τεχνολογίας, Η δικαιοσύνη στην Ελλάδα, Προτάσεις για ένα σύγχρονο δικαστικό σύστημα, έκδοση διαΝΕΟσις, 2020
32. Φαρμακίδης, Ευάγγελος Β., Η Διασυνοριακή Πρόσβαση των Αρχών στα Ηλεκτρονικά Αποδεικτικά Στοιχεία σε Ποινικές Υποθέσεις, Διπλωματική Εργασία στα πλαίσια του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο και Πληροφορική», 2019 (retrieved from https://dspace.lib.uom.gr/bitstream/2159/23494/1/FarmakidisEvangelosMSc2019.pdf)

***<u>Legislative and Legal Texts, Practical Guides</u>***

I. ACPO Good Practice Guide for Digital Evidence, March 2012 (retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)
II. Budapest Convention on Cybercrime (European Treaty Series No. 185) (Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561)
III. Charter of Fundamental Rights Of The European Union (2016/C 202/02) (Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE)

IV. CLOUD Act (Retrieved from https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm)

V. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093)

VI. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041)

VII. European Commission's Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final (retrieved from https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf)

VIII. Greek Code of Criminal Procedure (Law 4620/2019)

IX. Greek Penal Code (Law 4619/2019)

X. National Institute of Standards and Technology of United States Department of Commerce, The NIST Definition of Cloud Computing, Special Publication 800-145 (retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf)

XI. Principles on Transborder Access to Stored Computer Data (Retrieved from https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf)

XII. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN)

XIII. Transborder Access and Jurisdiction: What are the options?, Report of the Transborder Group (ad-hoc sub-Group on Jurisdiction and Transborder Access to Data), adopted on 6 December 2012 by the Cybercrime Convention Committee (T-CY) of the Council of Europe (retrieved from https://rm.coe.int/16802e79e8)

XIV. U.S. Code (Stored Communication Act)

XV. Hellenic Data Protection Authority, Ruling 70/2015 (retrieved from http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=240,58,77,254,51,40,191,175)

XVI. In re Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984)

XVII. Microsoft Corp. v. United States, 130 Harvard Law Review 769 (2016)

XVIII. ΜΟΔ Κατερίνης [Mixed Jury Court of Katerini (GR), Ruling…] 19-22/2009, Ποινική Δικαιοσύνη 2010, 1125

XIX. Συμβούλιο Πλημμελειοδικών Αθηνών 613/2016, Ποινική Δικαιοσύνη 2016, 424

***<u>Various Links</u>***

i. http://www.techopedia.com/definition/2493/cyberspace

ii. https://www.iso.org/standard/44381.html

iii. https://en.wikipedia.org/wiki/Star_Trek:_The_Original_Series

iv. https://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/