


## Article

# Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal

Christos Karagiannis<sup>1,2</sup> and Kostas Vergidis<sup>1,\*</sup> 

<sup>1</sup> Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece; mli18039@uom.edu.gr

<sup>2</sup> Prosecutor of the Court of First Instance, 41222 Larissa, Greece

\* Correspondence: kvergidis@uom.edu.gr

**Abstract:** Fighting crime in cyberspace requires law enforcement authorities to immerse in a digital ocean of vast amount of information and also to acquire and objectify the evidence of criminal activity. Handling digital evidence is a complex and multifaceted process as they can provide critical evidentiary information in an unquestionable and irrefutable way. When digital evidence resides in a cloud storage environment the criminal investigation is faced with unprecedented contemporary legal challenges. In this paper, the authors identify three main legal challenges that arise from the current cloud-based technological landscape, i.e., territoriality (the loss of location), possession (the cloud content ownership) and confiscation procedure (user authentication/data preservation issues). On the onset of the identified challenges, the existing American, European and International legal frameworks are thoroughly evaluated. Finally, the authors discuss and endorse the Power of Disposal, a newly formed legal notion and a multidisciplinary solution with a global effect as a result of collaboration between technical, organizational and legal perspectives as an effective first step to mitigate the identified legal challenges.



**Citation:** Karagiannis, C.; Vergidis, K. Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information* **2021**, *12*, 181. <https://doi.org/10.3390/info12050181>

Academic Editor:  
Georgios Kambourakis

Received: 31 March 2021  
Accepted: 20 April 2021  
Published: 22 April 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** cybercrime; cloud storage; digital evidence; cloud forensics; power of disposal; legal challenges

## 1. Introduction

Daily life is increasingly moving to the “virtual world”, a 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 “cloud”, where all the data-information is stored and waits to be recalled by its users. This paper attempts to chart the basic problems that arise in situations where the aforementioned technological capability of remote-cloud storage of digital information gets criminally abused. The aim of the paper is 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” some electronic data that are essential to the criminal procedure. These data need to be obtained by law enforcement authorities in a systematic manner to fully and thoroughly investigate the case against the perpetrator. This work does not touch on cloud-stored publicly available (open source) data, since this kind of data is easily accessible to anyone around the globe. The challenging cases are the situations where law enforcement authorities try to spot, identify and acquire electronic data-digital evidence that is stored remotely and the person-of-interest does not necessarily facilitate their work.

Section 2 of this paper provides a brief discussion of the technological aspects of the matter at hand: the authors point out the specific features of electronic data/evidence. They log the distinct characteristics that set them apart from the rest of the evidence in

a penal procedure and register 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. The authors also present in a brief manner the architecture of "the cloud" and how it actually works, specifically the model of Software as a Service (SaaS). The refined area of Cloud Storage 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. Section 3 pinpoints the main practical and legal barriers that need to be overcome when law enforcement authorities try to cope with a technologically aware criminal, Section 4 showcases a specific legal case of the Greek Judicial System that puts the presented challenges in practical scope and Section 5 records the different international approaches to the actual acquisition of the data in question. In the last three sections, criticism is exercised to the corresponding legal theories and the road to new concepts is paved through concrete proposals. Finally, in Section 6, the authors discuss and put forward a newly formed legal notion by proposing the power of disposal as a multidisciplinary solution with a global effect as a result of collaboration between technical, organizational and legal perspectives.

## 2. Background

Fighting cybercrime i.e., crime in cyberspace [1] requires law enforcement authorities to immerse in a digital ocean of vast amount of information and try not only to acquire but also to objectify the evidence of criminal activity. Every piece of significant electronic data in criminal procedure is considered evidence that needs to be handled with certain scientific procedures for it to maintain its probative value. As long as each evident object is admissible, authentic, reliable and complete [2], a judge can assess it safely in order to reach his final conclusion and judicial rule. After all, in accordance with article 177 of the Greek Code of Criminal Procedure (Greek Law 4620/2019), the essence of criminal proceedings is having judicially available unshakable evidence that lead to fact-based judgments. Therefore, it is of the outmost importance that all of the electronic evidence acquired meet some standards aptly named "Rules of Evidence", which is a body of procedural rules and legal principles governing the use of evidence in legal proceedings. These rules establish the methods by which evidentiary information may be presented and determine what evidence must or must not be considered by a judge or a jury in reaching his or its decision [3,4]. However, when data moves to a cloud-storage environment, the aforementioned forensic tactics, which take for granted the engagement with a material object at hand's reach, are no longer relevant and new legal challenges appear. Law enforcement authorities need new ways of efficiently investigating online criminal incidents while balancing a suspect's right to privacy and due procedure.

### 2.1. The Nature and Challenges of Digital Evidence

According to article 1 Section 3.1.1 of the Budapest Convention on Cybercrime (European Treaty Series No. 185) [5] digital/computer data is the representation of facts, information or concepts in a form that an information/computer system can process (e.g., photo, video, sound, text). According to the National Standard ISO/IEC 27037:2012 [6], which provides guidelines for specific activities (identification, collection, acquisition and preservation in a way that strengthens their evidential value) in handling digital evidence, the latter are identified as information or data, stored or transmitted in binary form, which may be relied on as evidence and act as an extremely important tool for solving cyber-crimes [7]. Digital evidence are 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 confiscated, they can provide critical evidentiary information 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 usually it is done deliberately for backup and recovery purposes [8]. 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 and yet continue to function without a service interruption and most importantly without losing data or compromising safety [9].

According to SANS Institute for information security training and security certification [10], five rules must be followed when confiscating digital or electronic evidence and each rule corresponds to a counterpart property that evidence must have to be considered valid:

- *Admissibility*: Digital Evidence must be collected through a legally acceptable and allowed procedure, so they can be admitted in front of court.
- *Authenticity*: Digital Evidence must be tied positively and relate to the incident under investigation in a relevant way.
- *Completion*: Digital Evidence must be able to uncover every aspect of the incident under investigation, thus functioning both inculpatory and exculpatory.
- *Reliability*: Digital Evidence must be collected and analyzed in a way that confirms the evidence's authenticity and veracity. The applicable procedure must create a uniqueness and singularity that makes that specific piece of evidence morphologically and technologically recognizable and distinct from any other similar digital object.
- *Believability*: Digital Evidence must be presented in front of a court in a clear, understandable and believable manner.

In 2007, the Association of Chief Police Officers (ACPO) in the United Kingdom agreed to a good practice guide in investigating cybercrimes, which 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, which in reality is a legal procedure that collects, analyzes and presents the facts of a cybercrime scene in correlation with a certain suspect of criminal activity in cyberspace [11]. According to ACPO [12], every law enforcement personnel who may deal with digital evidence needs to abide by the following four principles:

1. 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-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, even before the user begins to use the electronic device in question.
2. If it is 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 or even destroyed if the files are encrypted and set as auto-destructive.
3. An audit trail or other record of all processes applied to digital evidence should be created and preserved forming a continuous and unbroken "chain of custody" [13]. 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.
4. A specific person who is leading the investigation has overall responsibility for ensuring the application of these principles and generally the law as well.

## 2.2. The Emergence of Cloud Storage

In 1963, Joseph Licklider envisioned everyone on the globe to be interconnected and accessing programs and data at any site from anywhere, as part of an Intergalactic Com-

puter Network [14]. His idea eventually evolved into the platform that the Internet as we know it today is based on. The next evolutionary step of interconnected devices came in the 1990s in the form of cloud computing as an informatics' model that enables 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 [15]. The resources present in the cloud can be self-served infinitely and on-demand by users, who, instead of setting up their own physical infrastructure, can 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 device and the only thing that is required in order to be able to access it is a simple web browser [16].

The Cloud technology is widely and publicly offered in three versatile models (Software, Platform and Infrastructure as a Service—respectively SaaS, PaaS and IaaS), with SaaS being the most frequently used among household users, who essentially use the provider's applications running on a cloud infrastructure. The applications run and store their data online and are 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.

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 two aforementioned concepts is that Cloud Storage focuses on data storage, whereas Cloud Computing is all about remote processing of data [17].

### *2.3. Digital Evidence in the Cloud: Cloud Forensics*

As previously discussed, handling digital evidence is a complex and multifaceted process. There are certain parameters to be taken into consideration for the electronic data at hand to become decisive components of a logical judicial rule. When this data moves from the presently material world to a cloud storage environment, the latter becomes criminally interesting and the focus shifts to a new area, whose investigation calls for a need to meet new technological and legal challenges. Cloud Storage is a widely and often freely offered online service that opens new doors of action to evildoers. Cloud Forensics brings forth the necessity of blending various technical, organizational and legal perspectives to effectively answer the need of combating new forms of criminal behavior. On the next sections, the authors focus on the legal aspects of Cloud Forensics and try to approach the main issues that arise through a comprehensive presentation of problems spotted and an analysis of accordingly established solutions.

### **3. Legal Challenges for Cloud Forensics**

In an investigative criminal procedure the first logical and most vital step is the acquisition of every available proof that a malfeasance was committed. For example, law enforcement authorities find and confiscate child pornography material (e.g., photos, videos) that is stored in a specific digital storage medium (e.g., hard drive, USB stick, CD-ROM). Nowadays, electronic evidence is necessary in 85% of criminal investigations and in two thirds of these investigations there is a need to obtain evidence from online service providers that are based in another legal jurisdiction [18]. Electronic data must be handled with certain scientific procedures in order to maintain their high probative value,

since their legal assessment will lead a judge to reach a final conclusion and his judicial rule for the case at hand. The authors have identified three main legal challenges that cloud-stored electronic evidence raise and through mapping the disadvantages of various theories, practices and legal frameworks, pinpoint the way to overcome obsolete standard procedures and notions and venture into currently-forming and newly conceived legal tools to be used in cloud forensics.

### 3.1. Data Territoriality—The Loss of Location Challenge (CH1)

The first challenge (CH1) deals with the “multilocation” of cloud-stored data and how this specific attribute of the evidence in question legally affects the local jurisdiction of the competent law enforcement authorities.

The cloud is in essence a collection of data storage servers that are constantly making internal and architectural repositioning of data in a handful of geo-dispersed locations and contribute directly to the challenge of identifying the exact physical location of digital evidence in the case of a criminal offence. Due to data redundancy and performance-latency optimization reasons, most Cloud Storage Providers employ several data servers scattered all around the globe. Every time a user uploads a file to the cloud, that same file is automatically multiplied and stored in at least two (usually three) separate geographical places and physical locations, usually in different countries [19]. This practice offers the advantage that the user data remain safe and intact in case of: (i) a technical malfunction (e.g., abrupt maintenance need, power disruption, malevolent security breach) or (ii) a catastrophic event (e.g., natural disaster, terrorist attack) that can lead to server failure and/or data loss in a particular data storage center. Additionally, whenever a user shifts location around the world, his data are available on-demand by the data center that is geographically closer with the lowest possible propagation delays. The authors have identified four approaches in relevant literature that deal with the challenge of the loss of exact location of digital evidence. Two of these approaches are territorial and two are extra-territorial in their nature:

#### 3.1.1. The Criminal Event Theory (Territorial)

The criminal event theory states that the legislation of the country one must apply is determined by the place where the criminal event occurs [20]. In the case of cloud storage, one must pinpoint where the digital data in question is stored, namely, 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.

#### 3.1.2. The Criminal Instrument Theory (Territorial)

The second territorial approach shifts the attention to the medium with which the crime has been committed. Applicable is the legislation of the country where the instrument that made the criminal event a reality resides, i.e., the physical location of the cloud provider corporate headquarters.

#### 3.1.3. The Direct Consequence Theory (Extra-Territorial)

The third approach to the data territoriality challenge takes into consideration the place where the actual direct consequence or final effects of the crime are realized, i.e., the location of the end-user. The core question here is if you can actually prosecute a person for a digital file that in reality is physically located in a different country.

#### 3.1.4. The Nationality Principle (Extra-Territorial)

The fourth approach employs as decisive criterion the nationality either of the perpetrator or the victim of the criminal act, regardless of the location that the crime took place.

Both territorial scopes have disadvantages, i.e., by deliberately choosing a specific data center or cloud provider, criminals can manipulate penal jurisdiction of the states, in-

dulging in “forum shopping”; the practice of having a legal case heard in the court thought most likely to provide a favorable judgment. This is called *jurisdictional arbitrage* and has been frequently utilized by transnational criminals to hinder attempts at governmental prosecution [21,22]. 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”, which is a legal doctrine stemming from Roman Civil Law and essentially is the equivalent of the modern-day double jeopardy (autrefois acquit). In effect, it means that “no 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 or cloud provider actually resides.

However, also the two aforementioned extra-territorial approaches are disadvantageous since they both completely disregard the fact that the perpetrator is in no physical contact or even proximity with the digital files and furthermore the latter tries to ground criminal responsibility on a general base that is objectively irrelevant with the specific act that is under criminal inspection. Thus arises the challenge of agreeing upon the matter of possession of digital evidence stored in the cloud.

### 3.2. The Challenge of Cloud Content Ownership (CH2)

The challenge of cloud content ownership (CH2) deals with the reference notion of possession and how its meaning changes conceptually when we move from a bricks-and-mortar world to the virtual environment [23].

The Cloud Storage Provider is, from a legal point of view, not in possession of any data [24]. According to the architecture of the Cloud, 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 do not 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. It has 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 [25]. 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 [26,27]. From a technician’s point of view, when the end-user recalls from the cloud server and views online 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 or erased, as soon as the end-user leaves the cloud platform and moves on to other business. Moreover, when the end-user views online 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 of the device, in order to facilitate faster viewing of it in the future. Unless the 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 or 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 [28]. The problematic point of this opinion is that an involuntary and automatic procedure leads to the general conclusion that “viewing” is actually a form of possession. RAM storage and web cache lack in duration and stability, since their finite storing capability ends when new and more recent user-generated data are loaded-written on them. In addition, RAM storage loses its content entirely 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 or web cache and is always available for access. Technically, the screen does not operate nor can be used as a storage medium. These procedures are objectively and technically distinct, independent and essentially different and theoretically can be carried out from different persons [29].

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. In reality, the next-level evolution stage of possession is access 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 equation 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 exploitation of children and child pornography [30] distinguishes the three concepts (“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. 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”. 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 the Cloud should be considered and legally treated as a virtual and remote external storage medium, that actually is an extension of every digital device that has access to it. 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 does not download the file in his computer and only views it online, he is liable for accessing it on his own free will.

### 3.3. *The Challenge of User Authentication and Data Preservation (CH3)*

The challenge of user authentication and data preservation (CH3) deals with the distinguishability of cloud-stored evidence that actually use a shared pool of computer resources and the need to quickly ensure their stable situation until the law enforcement authorities can actually grasp them.

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 does not 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 admission-in-the-penal-procedure issues that is unique to the cloud. 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 piece of 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 [31]. 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 is understandable that law authorities have to make certain that the data of interest remain intact. Articles 16 and 29 of the Budapest Convention on Cybercrime [5] state that signatory Countries are obliged to take legislative measures regarding a potentially expedited preservation of specified stored 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, thus making it the first multilateral legally binding instrument to regulate cybercrime [32]. Members of the European Union already tried to level things up and upscale their legal arsenal on matters of electronic evidence stored in foreign states with the Proposal for a Regulation of the European Parliament and of the European Council on European Preservation Order for electronic evidence in criminal matters, which will be presented in the next section.

### 4. **Judicial Opinions on Cloud Forensics from Greek Court Cases**

In practice, many legal professionals, whose expertise stems from a completely different academic background, are hesitant and find it difficult to fully grasp the technological aspects and features of cloud storage and as a result they attempt to meet the aforementioned legal challenges using legal doctrines of a former era. Based on the habits of the cloud-users and how they take advantage of this decentralized service while using laptops and other smart mobile devices, some judges in Greek Courts of Law argued that storing and moving files through the cloud's different servers is actually a form of communication and thus if a law enforcement authority wants to gain access to a cloud stored and penally interesting file, it has to utilize a special and procedurally very strict legislation that allows for the removal of the constitutionally enshrined communications' privacy (Law 2225/1994). This perspective is founded upon the assumption that a user's cloud-stored data is not accessible to other users who store their data on the same server and by creating



a personal account with a cloud storage provider, each user in reality agrees to an exclusive use of a specific volume of storage space that only they can access, after their identity has been electronically verified through their unique username and secret password.

The aforementioned judicial opinion found that this procedure of accessing cloud-stored data that are in no physical proximity with the user, actually constitutes a form of electronic “communication” with the cloud platform, through which the user comes in contact with his data and as the latter are part of a kind of communication, it is protected as such, regardless of their actual whereabouts [33]. Specifically, according to Ruling 613/2016 of the Misdemeanor Council of Athens (GR) [34] *“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 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 online or to download them on their electronic device. If downloading occurs then we move to the area of crystal clear “possession”. However, when the user simply “communicates” with the server and consequently views online 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”.

However, on the same matter and as a part of the same ruling, one of the judges of the aforementioned three-member Council found that using Cloud Storage is not a form of secret “communication” that needs to be constitutionally protected but rather it must be considered as using an added hardware element on the user’s main device. Being on the same page with the Prosecutor of the Greek Supreme Court [35] the third judge found that law enforcement authorities do not need to employ special legislation for the removal of the constitutionally protected communications’ privacy of the wanted file and are legally allowed to gain immediate access to Cloud Storage, acting as if the data in question is stored in an external hard drive or any other handy device. According to his opinion, *“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 extension 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 does not download the file in his computer and only views it online, 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. Ultimately, the minority judge’s conclusion seems to be much more in accordance with the way the Cloud works and resonates with the at first oxymoron notion that Cloud Storage is a tangible storage device that is virtually an extension of the locally handy electronic device of the end-user.

## 5. Existing Legal Frameworks for Capturing Digital Evidence in the Cloud

Despite the universal scale of the three challenges (CH1, CH2, CH3) described in Section 3, different legal philosophies and systems led to different international approaches to the matter of capturing-confiscating the cloud-based digital evidence. Evidently enough, the process of mutual legal assistance between countries with unrelated, unconnected and often incompatible legal systems was soon deemed as overly time- and resource-consuming and it

became apparent to every state that each one needed to find an effective way to self-address the newly conceptualized problem of accessing data in another not-fixed and not entirely predetermined country. This paper examines two main legal perspectives: the American perspective, as the USA is where cloud technology originated and corporately houses the vast majority of the main Cloud Storage Providers, and also the European approach.

### 5.1. The USA Legal Framework

In 1986, the United States of America enacted the Stored Communication Act and according to Title 18, Section 2703 of the United States Code for Crimes and Criminal Procedure the government is allowed and able to compel a Cloud Storage Provider to disclose customer content and non-content information. On the matter of extraterritorial jurisdiction, the United States of America law authorities were 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” [36]. As the years passed by, people and corporations 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. In 2013, Microsoft challenged a warrant of the US 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 [37]. Not willing to wait for a judicial ruling, in 2015 the US Government drafted the so-called LEADS (Law Enforcement Access to Data Stored abroad) Act 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 and is determinative only when dealing with a non-US citizen [38]. This Act, which ultimately failed to gain passage, applied the Nationality Principle and 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 [39]. In 2016, the US Court of Appeals for the Second Circuit released its decision No. 14-2985, 2016 WL 3770056 (2d Cir. 14 July 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 [40] and as a result called on the US Congress to clarify, update and essentially modernize the Stored Communications Act [41]. In 2017, the US Government drafted the International Communications Privacy Act (ICPA), which also failed to gain passage, stating that US-based technology providers who are legally asked for, are obliged to produce the requesting cloud data, while at the same time the US 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. Finally, in 2018 and while the “Microsoft Ireland” case was still pending in the Supreme Court of the United States, the US Government passed through the Congress the CLOUD (Clarifying Lawful Overseas Use of Data) Act, which amends the initial Stored Communication Act and acts as the culmination point of the two aforementioned bills that never came to be. According to the CLOUD Act federal law enforcement can compel US-based technology companies to provide requested data stored on servers, regardless of whether the data are stored in the US or on foreign soil [42].

### 5.2. The International/European Legal Framework

In 1997, the inter-governmental political forum called “The Group of Eight” (G8) established the Subgroup of High-Tech Crime in an attempt to thwart international criminal and terrorist incidents in cyberspace. G8 drafted and approved three main “Principles on Transborder Access to Stored Computer Data—Principles on Accessing Data Stored In A Foreign State” [43,44]:

- *Preservation of Data Stored In A Computer System:* Each State ensures 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.

- *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 execute the request as expeditiously as possible.
- *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 (i) accessing publicly available (open source) data, regardless of where the data is geographically located or (ii) 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.

Those principles essentially became the stone upon which the aforementioned 2001 Budapest Convention on Cybercrime was founded. The latter is the first international treaty that is already adopted by over 60 states worldwide, including the United States of America, where most of the main 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 authorization 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*”.

A point of contention is if the Law Enforcement Authorities are going to obtain cloud-stored digital evidence 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. The three main possible scenarios are:

- ❖ *Access with consent*: A person that is physically located on the territory that the Law Enforcement Authorities operate in, gives its lawful and voluntary consent, enabling the Law Enforcement Authorities and ultimately granting access to his computer data that is stored in another jurisdiction.
- ❖ *Access without consent but with lawfully obtained credentials*: Law Enforcement Authorities lawfully obtain a password for accessing and storing (downloading) computer data, regardless of their whereabouts.
- ❖ *Access without consent*: Law Enforcement Authorities must obtain technical information from a Cloud Storage Service Provider concerning a suspect, who does not facilitate access to his data.

In the last case, it must be clarified that Budapest Convention’s reference of “*the person who has the lawful authority to disclose the data to the Party*” may also refer/apply to 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. However, for a Cloud Storage Service Provider to be in line with Article 32b of the Budapest Convention on Cybercrime, it must also consider its contractual obligation to safeguard its clients’ privacy. Therefore, this means that any third-party private entity would usually only be possible to disclose technical data owned by itself, 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 [45].

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 [46]. 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 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 not obligatory but simply goal-setting Directive 2014/41/EU/3-4-2014 enacted by national legislation, with 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, being the prime source of relative difficulties one can easily conclude that an issued European Investigation Order might prove insufficient in the timely fight against easily committed, speedy, anonymous and borderless cybercrimes [47].

The increasing dissatisfaction 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 [48]. 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 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*” (Article 2 of the aforementioned Proposal for an EU Regulation). 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*” (Article 2 of the aforementioned Proposal for an EU Regulation). 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.

## 6. Discussion—The Power of Disposal

Abuse of the Internet and more specifically of the Cloud Storage Service for cyber-dependent 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 [49]. Cloud Storage puts into a new perspective the age-old notions of ownership and identification/authentication of digital evidence and how these technological procedures and terms are legally defined. Legal practitioners need to elevate their expertise and come to a thorough understanding of the specific technology, to be able to properly and efficiently address the newly arisen problems. The unaware and indifferent to the specific content Cloud Storage Provider is in charge only of maintaining and transferring electronic data of the end-user, who is the actual “owner” and controller

of them. The identification process used for accessing the not-in-a-specifically-and-fixed-allocated-space stored data in question (unique username and secret password) combined with the according metadata and log files prove in an irrefutable way the actual identity of the penalty liable person.

Cloud Storage's main characteristic, though, that seems to make today's legal doctrines obsolete is 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 [50]. 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 thinking that originate from a different era [51]. 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 disproportionately significant forces are used in order to find the necessary data, potentially including heavy decrypting capacities, if that was possible at all.

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 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 [43]. The power of disposal is actually a new tenet that blends and successfully addresses the issues that cloud storage raises concerning ownership, authentication and territoriality of digital evidence.

The notion of the power of disposal reinforces the existing legal toolboxes that are used to regulate and, if needed, thoroughly investigate the cloud storage medium. One could argue that the power of disposal can be acknowledged as the inexplicitly theoretical cornerstone of the USA CLOUD Act, which cements the ability of law enforcement authorities to reach out to data stored in the cloud, regardless of their physical whereabouts. Moreover, the power of disposal fortifies the proposed European Preservation and Production Orders and at the same time brings the USA and the International/European legal frameworks closer to dealing with the challenges posed by cloud storage uniformly. Digital evidence found in cloud storage environment can be transborderly accessed and, through the identification sequence, attached to the specific person who controls them. "Cloud Storage is a practice that requires International policy setting. Multinational co-operation and development of globally agreed legal doctrines are necessary steps towards finding solutions to the contemporary technology legal challenges".

It must be pointed out that, despite being bold steps in a demanding field, European Preservation and Production Orders 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 or 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. At the same time the rights of the service provider include the right to freely 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.

## 7. Conclusions

This paper provided a brief overview of the basic practical and legal problems that law enforcement authorities face when they investigate "cloud-based" criminal incidents. The main contribution of this work is that, by collecting several viewpoints and theories from different legal systems, it brings to light the basic spectrum of practical and legal issues that need to be met while venturing "into the cloud" and argues that the only effective way to deal with the cloud is an international scope of understanding and collaboration. 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, case law should 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. The authors acknowledge the urgency for effective mitigation of cloud-based cybercrimes by considering that the prefix "cyber" actually means "connected" and after man has conquered air, land, ocean and space, perhaps cyberspace truly is "the final frontier" that needs to be jointly explored and globally regulated.

**Author Contributions:** Conceptualization, C.K. and K.V.; Investigation, C.K.; Methodology, K.V.; Resources, C.K.; Writing—original draft, C.K.; Writing—review & editing, K.V. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data sharing not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Techopedia. What Is Cyberspace?—Definition from Techopedia. Available online: <http://www.techopedia.com/definition/2493/cyberspace> (accessed on 28 March 2021).
2. Richter, J.; Kuntze, N.; Rudolph, C. Securing Digital Evidence. In Proceedings of the 5th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2010), Oakland, CA, USA, 20 May 2010; Endicott-Popovsky, B., Lee, W., Eds.; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2010; pp. 119–130. [CrossRef]
3. U.S. Government Publishing Office. Federal Rules of Evidence. Available online: [https://www.uscourts.gov/sites/default/files/evidence-rules-procedure-dec2017\\_0.pdf](https://www.uscourts.gov/sites/default/files/evidence-rules-procedure-dec2017_0.pdf) (accessed on 30 March 2021).
4. Montrose, J.L. Basic concepts of the law of evidence. *Law Q. Rev.* **1954**, *70*, 527–555.
5. Council of Europe. Convention on Cybercrime. Available online: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> (accessed on 30 March 2021).
6. International Organization for Standardization. Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Available online: <https://www.iso.org/standard/44381.html> (accessed on 28 March 2021).
7. Lone, A.H.; Mir, R.N. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digit. Investig.* **2019**, *28*, 44–55. [CrossRef]
8. Talend. What Is Data Redundancy? Available online: <https://www.talend.com/resources/what-is-data-redundancy/> (accessed on 30 March 2021).
9. Varanasi, P. Understanding Fault Tolerance in Cloud Computing and Its Significance. Available online: <https://www.cloudcodes.com/blog/fault-tolerance-in-cloud-computing.html> (accessed on 30 March 2021).

10. Braid, M. Collecting Electronic Evidence After a System Compromise, Global Information Assurance Certification Paper for SANS Institute. Available online: <https://www.giac.org/paper/gsec/659/collecting-electronic-evidence-system-compromise/101519> (accessed on 28 March 2021).
11. Li, M.; Lal, C.; Conti, M.; Hua, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *J. Future Gener. Comput. Syst.* **2020**, *115*, 406–420. [CrossRef]
12. ACPO Good Practice Guide for Digital Evidence. 2012. Available online: [https://www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf) (accessed on 28 March 2021).
13. Ryder, K.; SANS Institute, Information Security Reading Room. Computer Forensics—We’ve Had an Incident, Who Do We Get to Investigate? 2002. Available online: <https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652> (accessed on 28 March 2021).
14. Licklider, J.C.R. Memorandum for Members and Affiliates of the Intergalactic Computer Network. 1963. Available online: <https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network> (accessed on 28 March 2021).
15. National Institute of Standards and Technology of United States Department of Commerce. The NIST Definition of Cloud Computing. Special Publication 800-145. Available online: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (accessed on 28 March 2021).
16. Kaur, R.; Kaur, A. A review paper on evolution of cloud computing, its approaches and comparison with grid computing. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 6060–6063.
17. Subashini, S.; Kavitha, V. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **2010**, *34*, 1–11. [CrossRef]
18. European Commission. 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. 2019. Available online: [https://ec.europa.eu/info/sites/info/files/recommendation\\_council\\_decision\\_eu\\_us\\_e-evidence.pdf](https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf) (accessed on 28 March 2021).
19. Microsoft. Azure Storage Redundancy. Available online: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy> (accessed on 30 March 2021).
20. Boas, G. *Public International Law: Contemporary Principle and Perspectives*; Edward Elgar Publishing: Cheltenham, UK, 2012.
21. Kshetri, N. Pattern of global cyber war and crime: A conceptual framework. *J. Int. Manag.* **2005**, *11*, 541–562. [CrossRef]
22. Adams, J. Virtual defense. *Foreign Aff.* **2001**, *80*, 98. [CrossRef]
23. Rogers, A. From peer-to-peer networks to cloud computing: How technology is redefining child pornography laws. *John’s Law Rev.* **2013**, *87*, 1–39. Available online: <https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=6662&context=lawreview> (accessed on 28 March 2021). [CrossRef]
24. Chima, R. Cloud Security—Who Owns the Data? Available online: <https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data> (accessed on 30 March 2021).
25. Caiapha-Gbady, M. Online Insults of Minors, Criminal Chronicles, P. N. *Sakkoulas* **2012**, *3*, 161.
26. Andreadis-Papadimitriou, P. The pornography of minors in the era of the cloud computing, Thoughts on the occasion of Greek Law 4267/2014, Criminal Justice. *Nomiki Vivliothiki* **2015**, *5*, 454.
27. Mixed Jury Court of Katerini (GR). Ruling 19-22/2009, Criminal Justice. *Nomiki Vivliothiki* **2010**, *10*, 1125.
28. Marin, G. Possession of child pornography: Should you be convicted when the computer cache does the saving for you? *Fla. Law Rev.* **2008**, *60*, 1–31. Available online: [http://www.floralawreview.com/wp-content/uploads/2010/01/Marin\\_BOOK.pdf](http://www.floralawreview.com/wp-content/uploads/2010/01/Marin_BOOK.pdf) (accessed on 28 March 2021).
29. Burmas, G. Efforts to conceptually define the possession of electronic data in child pornography cases, Criminal Justice. *Nomiki Vivliothiki* **2009**, *3*, 322.
30. 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. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093> (accessed on 28 March 2021).
31. Orton, I.; Alva, A.; Endicott-Popovsky, B. Legal process and requirements for cloud forensic investigations, information resources managing association (USA). In *Cloud Technology: Concepts, Methodologies, Tools and Applications*; IGI Global: Hershey, PA, USA, 2014; p. 332.
32. Clough, J. A world of difference: The Budapest convention on cybercrime and the challenges of harmonization. *Monash Univ. Law Rev.* **2014**, *40*, 1–39. Available online: [https://www.monash.edu/\\_\\_data/assets/pdf\\_file/0019/232525/clough.pdf](https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf) (accessed on 28 March 2021).
33. Kousouni-Pantazopoulou, A. Legal Dimensions of Cloud Computing, Media and Communications Law. *Nomiki Vivliothiki* **2012**, *2*, 177.
34. Athens Council for Criminal Procedure in Misdemeanor Cases. Ruling 613/2016 Criminal Justice. *Nomiki Vivliothiki* **2016**, *5*, 424.
35. Opinion of the Prosecutor of the Supreme Court (GR) 6/4.7.2008 Criminal Justice 2009, p. 185. Available online: <https://eisap.gr/%ce%b3%ce%bd%cf%89%ce%bc%ce%bf%ce%b4%cf%8c%cf%84%ce%b7%cf%83%ce%b7-06-2008/> (accessed on 19 April 2021).
36. Baum, S. In re Grand Jury Proceedings (Bank of Nova Scotia). *NYLS J. Intern. Comp. Law* **1984**, *5*, 2.

37. Brennan Center for Justice. The “Microsoft Ireland” Case (Amicus Brief) [Update]. Available online: <https://www.brennancenter.org/our-work/court-cases/microsoft-ireland-case-amicus-brief-update> (accessed on 30 March 2021).
38. GovTrack, S. 512 (114th): Law Enforcement Access to Data Stored Abroad Act. Available online: <https://www.govtrack.us/congress/bills/114/s512/text> (accessed on 30 March 2021).
39. Watney, M. Law enforcement access to evidence stored abroad in the cloud. In Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS, Munich, Germany, 7–8 July 2016.
40. Thomas, F.; Brier, J. Defining the limits of governmental access to personal data stored in the cloud: An analysis and critique of Microsoft Ireland. *J. Inf. Policy* **2017**, *7*, 327–371.
41. The Harvard Law Review Association. Microsoft corp. v. United States. *Harvard Law Rev.* **2016**, *130*, 769–776.
42. U.S. Government Publishing Office. One Hundred Fifteenth Congress of the United States of America. Available online: <https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm> (accessed on 28 March 2021).
43. Sachowski, J. *Digital Forensics and Investigations, People, Process, and Technologies to Defend the Enterprise*; CRC Press: Boca Raton, FL, USA, 2018.
44. Council of Europe. Principals on Transborder Access to Stored Computer Data. Available online: [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](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) (accessed on 28 March 2021).
45. 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. Available online: <https://rm.coe.int/16802e79e8> (accessed on 28 March 2021).
46. Directive 2014/41/EU/3-4-2014 of the European Parliament and the Council of Europe on the European Investigation Order in Criminal Matters. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041> (accessed on 28 March 2021).
47. Farmakidis, E.V. European production order and european data preservation order. The adaptation of judicial cooperation procedures in criminal cases in the digital age, *Criminal Justice. Nomiki Vivliothiki* **2021**, *1*, 28.
48. 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. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN> (accessed on 28 March 2021).
49. Daskal, J. The un-territoriality of data. *Yale Law J.* **2015**, *326*, 390.
50. Orin, S.; Foreword, K. Accounting for technological change. *Harvard J. Law Public Policy* **2013**, *403*, 403.
51. Spoelne, J. 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. Available online: <https://rm.coe.int/16802fa3df> (accessed on 28 March 2021).