TALLINN UNIVERISTY OF TEHCNOLOGY
School of Business and Governance
Department of Law

Filip Pásztor

DATA POSSESION IN CLOUD COMPUTING

Master's thesis
Programme Law, specialisation Law and Technology

Supervisor: Agnes Kasper, PhD

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 22045 words from the introduction to the end of summary.

Filip Pásztor ……

(signature, date)

Student code: 163718HAJM

Student e-mail address: filip.pasztor@gmail.com

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Cloud Computing has become part of our daily life, whether it is in the form of social media, emails or instant messaging. This has caused problems, as this reality has to be reflected by the law, but this was not always the case. In recent period, countries were increasingly seeking ways how to obtain , in criminal proceedings, information and data stored abroad. Normally this has to be done thought cooperation process that is long and not always accurate.

Both US and EU has recently reacted to this by introducing new legislation covering access to data abroad. EU has so far only proposal for new E-evidence framework, consisting of Directive and Regulation proposal. It targets provider that offer services to EU citizens. US have taken bit different route with CLOUD Act, as it allows access to all data stored by US companies, regardless of the place where the data is stored and regardless of the citizenship of the targeted person. Trough analysis of provisions of mentioned legislations, applied on the field of Cloud Computing over-the-top instant messaging services WhatsApp and Facebook Messenger, this work tackles the biggest issues that arise from potential application of said provisions in the reality.

Trough the doctrinal, comparative research and interdisciplinary research of the Cloud Computing over-the-top instant messaging services, indicates that certain provisions of the CLOUD Act may be in contrary with EU privacy and data protection framework lead by the new General Data Protection Regulation.

Keywords: Cloud Computing, CLOUD Act, E-evidence Regulation, over-the-top services, GDPR

LIST OF ABREVIATION

CLOUD Act	Clarifying Lawful Overseas Use of Data Act
Commissioner	Irish Data Protection Commissioner
ECS	Electronic communications service
E-evidence Regulation	Regulation on European Production and Preservation Orders for electronic evidence in criminal matters
ENISA	European Union Agency For Network And Information Security
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ISP	Internet service providers
OTT	Over-the-top
Representative Direction	Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
SLA	Service Level Agreements
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TSP	Telecommunication service providers

INTRODUCTION

Rapid development in the field of Information and Communication Technology (further only ICT) have enabled emergence of many new technological solutions in recent years, that pushed our perception of ICT into new directions. And one of those new solutions, that emerged in past few years, is Cloud Computing, although it doesn't represent new technology but kind of new delivery model[1]. Cloud Computing become popular solution that allowed convenient handling of data, as it allows companies and individuals not only to store data, but also access, share, manage and edit the data[2] remotely in that mythical "Cloud". Cloud Computing has gain big popularity among enterprises and also among the individual users, as it offers affordable and effective data management solution to masses without actual need to invest in own ICT equipment, "*trough effective utilization of shared resources",*[3] that are remarkably scalable and elastic.[4] Company Oracle is predicting that by 2025, 60%[5] of critical system management will be moved to Cloud solutions. Cloud Computing brings efficiency and possibilities to data management, that were not imaginable before, but also complicates and widens the structure of subjects dealing with the data in question.

When it comes to topic of Cloud Computing many questions are arising even among experts in various fields. Cloud Computing does not have only pros, as with sharing of resources with another users, there also comes disadvantages, in the form of giving up some part of control over data, as the user cannot control all the equipment and software that is used to run Cloud Computing solutions. Companies providing Cloud Computing solutions invest in security and data and access management solutions, that would not be implemented by many clients of theirs otherwise, it still is discussion topic when it comes to providing such services. European Union Agency For Network And Information Security (further only ENISA), in it's 2017 paper "Security aspects of

---

1 Curran, K. (2012). *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments.* US: IGI Global. p 12

2 Samarati, P., Capitani di Vimercati, S. (2016). Cloud Security. - *Encyclopedia of Cloud Computing* (eds.) Murugesan, S., Bojanova, I. Chichester, UK: John Wiley & Sons, Ltd, 205-219. Accessible: http://spdp.di.unimi.it/papers/sd-cloud_security.pdf, 10 March 2018. p 1

[3] Khan, M. A. (2016). A survey of security issues for cloud computing. - *Journal of Network and Computer Applications*, Vol. 71, p. 11 - 29. West Yorkshire: The Science and Information (SAI) Organization. Accessible: http://www.sciencedirect.com/science/article/pii/S1084804516301060?via%3Dihub (10 March 2018). p 26

[4] Hashem, I. A. T., Yaqoob I., Anuar, N.B., Mokhtar S., Gani, A., Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. - *Information Systems*, Vol. 47, p. 98-115. John Wiley & Sons. Accessible: http://www.sciencedirect.com/science/article/pii/S0306437914001288 , 10 March 2018. p 99

5 *Cloud Predictions 2017*. (2017). Oracle. Available: http://www.oracle.com/us/solutions/cloud/top-10-predictions-cloud-3436083.pdf , 11 March 2018. p 6

virtualization", ENISA shows how losing control over data, or parts of Cloud solution, may affect other aspects as the "*users deploying a service in the cloud lose full control over their data and applications, which are fully or partially in the hands of cloud providers.*" [6] This is connected not only to data management itself, but also to security, data privacy and data integrity[7], that all of them are interconnected and one has impact on each other.

Thanks to complexity, there are many additional factors that can have impact on level of control available to the users. Maybe the biggest question looming over the Cloud is the question of data localisation, as the very nature of the Cloud is global. Most of the successful ICT companies are based US or are directly from there. Especially big companies are trying to build regional data centres, so they provide services tailored for regional markets also being closer to customers allows companies to enhance performance of its services. Recently we also witnessed new legislations all over the world pushing companies to store at least some of the data locally, where the measures have different character as some measures require prior consent in order to transfer data, another requires storing copies of the data locally, some prevent transfer of certain data at all and some even tax the transfer[8]. These steps taken by countries are not only mere attempts to strengthen their outreach over Clouds, it was also reaction to the "Snowden" revelations about widespread surveillance done by US agencies that affected also non-US citizens or residences. AS subsequent reaction, after court case and proceedings, EU cancelled Safe Harbour arrangement with US, that allowed transfer of private data and information of EU citizens to US. It took some years of negotiations to find solution, where US and EU made new arrangement called Privacy Shield.

Despite this anxieties over surveillance, countries are also facing the problems in the field of national security and crime prevention, as with these global services provided by Cloud, they are losing the control over the data and it's proving to be difficult, sometimes even impossible, to effectively use data stored on Cloud outside of country as part of criminal proceedings. That is why US and EU come up with new legislative solutions that will allow respective countries to

[6] European Union Agency For Network And Information Security. (2017). *Security aspects of virtualization.* Accessible: https://www.enisa.europa.eu/publications/security-aspects-of-virtualization ,11 March 2018.
[7] Zhang, Y, *et al.* (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. - Information Sciences, Volume 379, Pages 42-61. Elsevier. Accessible: http://www.sciencedirect.com/science/article/pii/S002002551630250X , 19 March 2018.
[8] Chander, A., Uyen P. Le. (2014). Breaking the Web: Data Localization vs. the Global Internet. Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378. Available at SSRN: https://ssrn.com/abstract=2407858 , 11 March 2018. p. 3

access data outside of their borders. The EU solution[9], yet only proposal is more EU oriented, with new institutes allowing for fast production and preservation of electronical evidence EU-wide. US solution[10], however deals with access to data of US citizens and residences outside of EU, where also discussing the possibility of international cooperation allowing to use such procedure by other countries vice-versa.

As illustrated above, Cloud based solutions present complex environment, that allows the users to engage in various and complex relationships with provider of Cloud Computing services and other various actors. Aim of this paper is to bring more clarification into problematics of data possession in Cloud Computing, identifying the actors and applicable law and map the actual state of the problematics at this time, while trying to tackle the hypothesis that "**new cooperation rules in the criminal procedure in the US and the new rules proposed in the EU, explained on the example of the selected Cloud service, may not provide desired effect**."

Methods used to discuss presented hypothesis will be doctrinal research, comparative research and interdisciplinary research of the Cloud Computing and related topics, with main goal to bring clarity to actors, relations, data and legislation, that are part of the Cloud related services, leading to answering the presented hypothesis. Main objective of doctrinal research in this paper will be analysis and interpretation of privacy, data protection regulations and their relationship to new evidence rules introduced in US and EU, with aim to determine obligations arising to individual actors from legislation. Comparative research is used in this work to compare, mainly EU and US legislation and identify differences between legislations. Interdisciplinary research is in this work used to combining knowledge of legal, IT and cybersecurity fields.

The first chapter of this paper discusses problematic Cloud Computing in more details, especially bringing attention to detailed explanation of various models of deployment and Cloud service providing models, as they are important factors impacting both factual and contractual data possession. Also involving discussion about specifics of the data in the Cloud computing, discussing selected problems in depth.

[9] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters. 2018/0108 (COD)
[10] S. 2383 - Clarifying Lawful Overseas Use of Data Act or the ''CLOUD Act'

In second chapter there will be discussion about legislation in the field of privacy, evidence obtaining and international cooperation in criminal proceedings. This chapter is divided into two sub-chapter, where the first sub-chapter will be present discussion about evidence gathering and international cooperation in criminal proceeding regulations in the US, as many popular and widely used Cloud solutions are based in the US. The last sub-chapter EU regulation of evidence gathering and cooperation proceedings.

The third will be analysis of selected providers of the Cloud services, with SaaS model deployed on public Cloud. Reason to choose this limited sample is that public SaaS Clouds are solution giving the user least amount of control and also Terms and Conditions of public SaaS are not open for negotiations, so all (or at least the most of) the users have the same, default condition to use the services. On the example of this selected Cloud service, we will demonstrate the impact of the aforementioned legal acts.

In the fourth and last chapter, introduces regulation of privacy in the European Union (further only EU), with General Data Protection Directive (further only GDPR), where it's being interesting discussion point, as the date of it being enforceable is already glooming over. This chapter will contain comparison of EU and US regulations mentioned in previous chapter, with focus on pointing out the biggest differences that can have potential impact on data possession. Also challenging the both EU and US regulations in contrast to GDPR.

1. CLOUD COMPUTING

Although Cloud Computing become very popular, we need to establish what it is first, in order to be address further talking points and advance in the discussion. Thanks to complexity, novelty and constant innovation in the filed of the ICT, Cloud Computing still remains sort of mystery for many users till this day. Many of the Cloud Computing users are not even aware of the fact that they are using Cloud Computing solutions, when being presented with the topic. For example, Gmail (and all other applications that are part of google account) by Google is Cloud based application and even Facebook can be defined as Cloud application.

1.1. Definition of the Cloud Computing

To better understand the changes Cloud Computing presents and what is and what is not part of the Cloud Computing, it would be good to make small detour into evolution of Cloud. Firt major discussion about Cloud Computing was brought by Nicholas Carr, in his book "The Big Switch: Rewiring the World, From Edison to Google", where he compares the effect Cloud Computing had on ICT, to effects comparable to impact electrification had during industrial revolution[11], as Cloud Computing similarly revolutionised the filed of the ICT. Before electrification, companies had to invest into own infrastructure to be able to produce electrical energy, however, after electrification it was sufficient just to plug into the grid and company was able to use electrical energy. Carr in his work argues that Cloud Computing had similar impact on the field ICT, where till introduction of Cloud, companies had to invest into and build own ICT infrastructure, to be able to use ICT, with introduction of Cloud Computing, no longer need to invest into own infrastructure, as they can plug into 'Cloud' trough internet and they can enjoy having all the necessary infrastructure available immediately, provided by Cloud Computing service provider.

This development could be illustrated by Figure 1, where we can see this development of Cloud Computing. In the beginning there was basic model, where internet service providers[12] (further only ISP) were offering basic connectivity to internet to individual users or companies, that is

[11] Carr, N. (2008). The Big Switch: Rewiring the World, From Edison to Google. 1st ed. New York: W. W. Norton & Company, Inc.

[12] For this discussion, that surrounds explanation of Figure 1, ISP should be understood in wider sense as it's commonly used (common understanding is that ISP is provider of internet connection), as author of the Figure 1 sees Cloud service provider as extension of ISP's

model of ISP 1.0 on the Figure 1. In later on service providers were trying to add new services as addition to just offering internet connection, in order to stay competitive they started to provide also e-mail hosting and limited server hosting, in the Figure 1 it is shown as ISP 2.0. Later, specialised centres for hosting of companies servers emerged, that allowed to easily connect those servers to another ICT solutions and service providers and all that for minimal price. This model, on the Figure 1 as ISP 3.0 is just minimal step away from providing Cloud services, that emerged as ISP 4.0 in the Figure 1, where service providers were offering software to the users through internet. Software was running on service provider's infrastructure and client had nothing to worry about, that's how SaaS emerged. Next step was offering clients the infrastructure itself, either in the form of platform that serves as base for clients actions or by providing infrastructure itself. This model ISP 5.0.

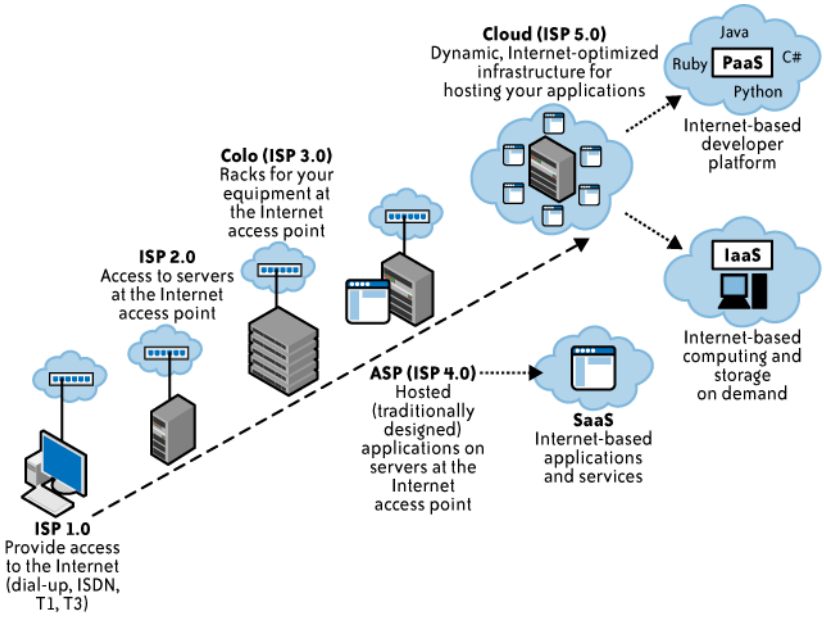

Figure 1. Evolution of Cloud Computing
Source: Maher, T. (2009) p 4

The flexibility of the solutions are as shown on the Figure 1 is the reasons why Cloud Computing become popular almost instantly. Current economy, constantly pushing to find ways how to lower expenses, drives most of the companies to search for ways how to optimise their business models. Cloud Computing presents solution, how to achieve minimisation of expenses, when it comes to ICT infrastructure, as it allows companies to outsource whole, or part of the ICT infrastructure. The cost reduction is based in the fact that the user pays only for using ICT infrastructure, without need to buy and maintain the infrastructure. Also the billing is only for extent to which the ICT

infrastructure is used. This way, Cloud Computing is causing changes of business models implemented by companies all around the world, no matter if it is small company, one man company, or multi billion companies, Cloud offers new, innovative ways of doing business and considerably dropping the costs, allowing more companies to enter new markets[13].

Responsibility for maintenance of the ICT infrastructure is shifted to Cloud service providers, who are responsible for keeping the infrastructure running and available to customers according to their needs. So there is no longer need for customer to take care of infrastructure maintenance and investments, also lowering the personal investments into IT support. Demands on Cloud Computing service providers are however quite big, as they not only have to provide the ICT infrastructure to the customers, they also have to provide effective, flexible and reliable services.

To the customers is appealing not only because of the costs saving, but also the ability to access and share the data at any moment, no matter where they are. The only thing needed is connection to the internet, trough which the Cloud service is accessed. Speed of such data transfer, when taken into account, is currently unmatched by any other technical means, especially given the speed how interned connection coverage is spreading around the world.

There were many attempts to define Cloud Computing, however sometimes we still see some differences between these definitions. But the definition provided by the NIST remains the most widely used one, as it achieves to be complex, yet understandable across various fields of expertise. NIST defines Cloud Computing as „model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [14]"

NIST also defines five essential attributes of Cloud Computing, that distinguishes Cloud services from another services provided through the internet. Those Characteristics are:

- **On-demand self service:**

  Customer is able to request service of the Cloud Computing according to imminent needs.

[13] Soghoian, C. (2009). Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. - *Journal on Telecommunications and High Technology Law*, vol. 8, p. 359 - 424. Available: https://ssrn.com/abstract=1421553, 19 March 2018. p 364

[14] National Institute of Standards and Technology. (2011). *Supra nota 9*

This operation can be done without the need of human interaction and may even be automated.

- **Broad network access:**

  The resources of Cloud Computing are available through the internet network and may be accessed by commonly used devices that are able to connect to the internet.

- **Resource pooling:**

  The Cloud infrastructure resources are interconnected and pooled together so they can serve all customers of the service provider. Multiple users can be using the same hardware from the infrastructure thanks to virtualisation, that is base for enabling this model of service provision, as it a "technology that abstracts away the details of physical hardware and provides virtualized resources for high-level applications[15]."

- **Rapid elasticity**

  The resources of the Cloud Computing can be appropriated and released rapidly according the need of the customer of the service. Thanks to its characteristics, it may appear to the customer that the resources are unlimited at certain moments.

- **Measured services**

  In order to be able to provide elastic services, the Cloud Computing service provider has to able to measure usage of the client in order to optimize its services. The services can be monitored and controlled in order to provide at least basic transparency to the Cloud Computing service provider and the Cloud Computing client.

Similar definition of the Cloud Computing is provided by Vaquero and collective, where they captured the essence of the NIST definition with similar description of the Cloud Computing as "a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay per-use model." [16] Publication Encyclopedia of Cloud Computing adds one more attribute to the essential attributes of Cloud Computing, which is Multi tenancy. That should be understood as use of the same resources by more than one user, that are in this case called tenants,[17] where this is allowed by virtualisation and resource pooling. It is worth to mention that

[15] Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. - *Journal of Internet Services and Applications*, Volume 1, Issue 1, p. 7–18. London: Springer London. p 8

[16] Vaquero, L. M, Rodino-Merino, L., Caceres, J., and Lindner, M. (2009) A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review*. Volume 39, Number 1, p. 50–55**.** p 51

[17] Encyclopedia of Cloud Computing. (2016). /Eds S. Murugesan,I. Bojanova, I. UK: John Wiley & Sons, Ltd. p5

this could be also noted that multi tenancy is implied in the NIST definition as well, its base is in the resource pooling.

As mentioned above, sometimes it is quite difficult to determine if the service provided to the client is Cloud based or not, so this characteristic provided by NIST is quite useful tool allowing to settle the discussion in the individual cases.

1.2. Service models

After we were able to determine whether is the service Cloud based or not, we can further qualify Cloud Computing services into more categories, according to services attributes and means offered to clients. Categorisation of Cloud Computing services also allows to elaborate the discussion about questions arising from differences between individual types of Cloud Computing services.

The most common division of Cloud Computing service models is again provided by the NI ST,[18] that brought up three basic models:

- Software as a Service (SaaS)
- Platform as a Service (IaaP)
- Infrastructure as a Service (IaaS)

SaaS requires the least involvement of the Cloud Computing service client, putting the most requirements on the Cloud service provider. On the other hand, IaaS is on the opposite side of the spectrum, where the Cloud service provider has least responsibility out of discussed models, as except physical maintenance and control, the client of the service is responsible for the actions, as the Cloud service provider offers the customer only hardware without any software or platform by this model. PaaS is in between booth of previous models, where the Cloud infrastructure is controlled by the Cloud service provider, however the client is allowed to run custom applications that can operate on the platform provided by the Cloud service providers.

1.2.1. SaaS

Traditionally when one acquires software, the client buys software for license fee and installs it [the software in question] on own hardware. The buyer has to consider compatibility with the

[18] National Institute of Standards and Technology. (2011). *Supra nota 9*

operation system he/she runs, needs to keep in mind updating the software and other niches. When using the SaaS, the user subscribes to service, and the rest is ensured by the Cloud Computing service provider. The subscription can be based on the time period or task based, where in some cases, service is even provided for free, but in such a case customer has to settle for some constrains from the service provider.

SaaS type Cloud services are complex solutions composed of Cloud service provider offering software, hardware and support to the user of the service, where the user access the software installed on the hardware of the Cloud service provider. The user of the service may access the SaaS service software from arbitrary device trough supported internet browser or dedicated application provided by the Cloud service provider.

The client has almost unlimited access to the software, but on the other hand he or she is not able to influence the ICT infrastructure used to run the software, as the customer is not owner nor tenant of that ICT infrastructure. In the case of the SaaS type Cloud services, the Cloud service provider controls distribution and usage of the ICT infrastructure resources, which also offers certain level of protection for intellectual property of the Cloud service provider, as clients does not have the copy of the software available to them. The model of subscription allows the Cloud service provider to allocate stable income that is generally paid up-front, that allows the Cloud service provider to invest this income from subscription into better quality service, better hardware and into implementation of security measures that could not be implemented by the individual users, thus making the Cloud service more secure for the individual user and small to medium companies.[19]

SaaS model of Cloud services lowers the costs of the software for the individual users of the Cloud service, as here is no need to invest into own hardware, subscription license is usually more affordable than buying individual software and because of the character of the Cloud Computing services, the users may access and share data between themselves in real time, that is also another step forward[20].

[19] Sun Y., *et al*. (2014). Data Security and Privacy in Cloud Computing. - *International Journal of Distributed Sensor Networks.* Volume: 10, Issue: 7. Thousand Oaks: SAGE Publications Ltd Accessible: https://doi.org/10.1155/2014/190903, 19 March 2018

[20] Shaqrah, A., Cloud CRM: State-of-the-Art and Security Challenges - International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, p. 39-43. Accessible: http://thesai.org/Downloads/Volume7No4/Paper_5-Cloud_CRM_State_of_the_Art_and_Security_Challenges.pdf, 19 March 2018. p 40

One of the most commonly knows SaaS type Cloud services are Google Apps, Gmail the most know email service is part of this bundle, Hotmail by Microsoft or now infamous service DropBox. These SaaS Cloud services are quite often run using another service models run by another Cloud service providers that provider of given SaaS Cloud service. This could lead to confusion or misinterpretation among the users of the SaaS Cloud services, that are often not even aware of the fact. The SaaS service of Drop Box could be used as example in this case, where the SaaS software is run on IaaS Cloud services provided by company Amazon.

1.2.2. IaaS

IaaS model of providing the Cloud Computing services represents the basis of the other Cloud service models, as they [the other models] just expand and provide added value on top of the infrastructure itself. The IaaS Cloud service model that offers its users opportunity to use computing power, storage space or different resources of hardware IC T infrastructure that is subject of service. The IaaS Cloud Computing service provider basically offers to the users access to the hardware ICT infrastructure, that is accessible through the Internet, in the extend required by the user at the given moment. The user has opportunity to implement and run own software and applications[21].

This model of the Cloud Computing service provision is more suitable for clients that wish to have enhanced control over own software, but on the other hand is [the client] not interested in buying or maintain necessary hardware.[22] Client has available hardware infrastructure that he or she may use at will and according to the needs, without having to withstand the higher requirements of such actions on the hardware in question. The best example of such Cloud service provider could be company Amazon, with its Amazon Web Service. Amazon is for long time market leader in the market of providing the Cloud Computing, even though being known mainly as internet shop.

[21] Marchini, R. (2010). *Cloud Computing: A Practical Introduction to the Legal Issues*. London: British Standards Institution. p 50

[22] Aldossary, S., Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. - *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, p. 485-498. Accessible: http://thesai.org/Downloads/Volume7No4/Paper_64-data_Security_Privacy_Availability_and_Integrity.pdf ,19 march 2018. p 486

1.2.3. PaaS

By the PaaS model of Cloud Service, is the Cloud service provider offer its clients hardware and / or software IC T infrastructure, suitable for development and implementation of the new software. Also client is able to distribute and offer for retail such a software developed on the PaaS platform to his [clients] own users. The Cloud PaaS service provider is usually paid for supplying client's with environment for development and implementation of their own software and for supplying them also with distribution platform. This model offer clients with lower cost for development of new software, faster and better propagation of their software if they are using well established Cloud Computing service provider, thanks to already created and functioning retail platform. Development and retail tools are available to the clients trough web browser or dedicated application. Thanks to this, client's developers have the necessary software and resources needed for development at their disposal without the need to install anything, thus making the process of developing, testing and implementing of client's software much easier[23]. Thanks to this even small teams and start-ups have opportunity to offer their software to the world market without the need to own expensive hardware and to some extent even software, thanks to this simplified process. Google AppEngine or Microsoft Azure are the quite good examples of the PaaS Cloud service providers, that may be known.

In order to fully offer such flexibility as desired by Cloud Computing users, the Cloud Computing service providers cannot stay only with above-mentioned service models of SaaS, IaaS and PaaS, that are basic for every discussion about Cloud Computing. But they also try to provide us with the cutting edge, trying to find new services for situations like privacy and security management, access management or ect. Examples of such cloud support services are data storage as a service (DSaaS), analytics as service (AaaS), desktop as a service (DaaS), security as a service (SecaaS), identity and access management as a service (IAMaaS), and monitoring as a service (MaaS)[24]. But these services are too specific and too supportive to make talking point of them, so we just make quick note of them.

[23] MAHER, T., KUMARASWAMY, S., LATIF, S. (2009). Cloud Security and Privacy. 1st ed. Sebastopol: O'Reilly Media, Inc. p 19.
[24] Encyclopedia of Cloud Computing. (2016). /Eds S. Murugesan,I. Bojanova, I. UK: John Wiley & Sons, Ltd. p 7

1.3. Deployment Models

Deployment models of the Cloud Computing services does not divide Cloud Computing services into according to service offered, like it was in previous subchapter about service models of Cloud Computing service, but rather distinguishes between Cloud Computing services on the basis who is the actor that owns and manages the I CT infrastructure running the service and who are the actors using the Cloud Computing service. There are four commonly used and agreed types of deployment models[25]:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Clouds

All of the Cloud Computing service models may be deployed on any of the abovementioned types of deployment models. The most commonly used type of deployment model are public Clouds, as they are available to the masses of the users, for very reasonable prices, sometimes even for free that only supports the popularity. However the public Cloud is the least flexible option, where sometimes the Cloud service providers have to compromise on security measures in order to be able to approach more users. The private clouds on the other hand are build or modified according to the specific requirements of the client, who will be the only one using the ICT infrastructure. This also requires much more engagement between Cloud Computing service provider and clients, as the communication is the key in such situation. Community Clouds and Hybrid Clouds are combination of previous deployment models, where there are either more deployment models used, or the number of the users is specified according to some kind of formula.

1.3.1. Public Cloud

Public Clouds are owned, maintained and managed by the Cloud Computing service provider and trough the means of the internet is the service offered to the clients, is open to anyone[26]. Clients of

[25] Botta, A., *et al*. (2016). Integration of Cloud computing and Internet of Things: A survey. - *Future Generation Computer Systems*, Volume 56, p 684–700. Accessible: https://www.sciencedirect.com/science/article/pii/S0167739X15003015, 19 March 2018. p 687

[26] Hon, W. K., Hörle, J., Millard, Ch. (2012). Data Protection Jurisdiction and Cloud Computing: When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3. - *International Review of Law, Computers & Technology*, Vol. 26, No. 2-3, p. 129-164. Abingdon: Taylor & Francis (Routledge). Accessible: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240,18 March 2018. p 130

public Cloud does not have to bear the costs of buying the ICT infrastructure or maintain such infrastructure. The only thing the user has to do, is to to get internet connection and web browser or dedicated application on some devices. Management of the security measures and maintenance of the public Cloud is affair of the public Cloud service provider, thus client loses control and overview of taken security measures, although some public Cloud providers tend to inform the users about taken measures and precautions in at least limited extent. However it looks like, from the fact that this type of the Cloud Computing services deployment model is the most popular one, that clients are willing to sacrifice potential danger and limited control for affordability of such solutions. Example of such approach to providing of public Cloud Computing services is Google with its G mail or Google Apps, or Drop Box.

Public Cloud services are build to be accessible to wide masses, that's why the are offered on the basis of the general Service Level Agreements (further only SLA). SLA of the public Cloud services are usually very general and vague, ins some cases they does not even cover all the specific relationships that emerge between the public Cloud service provider and the client of the public Cloud services. The company Google could be again used as one example, in the year 2012 company merged all the SLA's for their Google Apps Cloud services, into one SLA. This step was heavily criticized at the time by data protection authorities in many EU member states, mainly in Germany and France, where the company was facing high monetary fines[27]. The more specific discussion about SLA of the selected Cloud Computing services providers will follow in the last chapter of this paper.

1.3.2. Private Cloud

In the case of the private Cloud services, the ICT infrastructure is build, provided and controlled by individual client. In some cases infrastructure is not owned by the client, but it is owned by the Cloud service provider, but then the private Cloud service is provided under case specific SLA, custom made to fit the clients requirements and specifics, where the client has enhanced role when it comes to the control of the data and in the implementation of the security and data management. The main difference between the other types of the Cloud Computing implementation is that the

[27] Commission nationale de l'informatique et des libertés. (2012). *Google's new privacy policy: incomplete informationand uncontrolled combination of data across services*. Paris: Commission nationale de l'informatique et des libertés, Accessible: http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/ ,15 March 2018

client is the only one degerming who has access to the private Cloud, giving the client full control over data on the private Cloud.

1.3.3. Community Cloud

As mentioned here before, community Cloud has bits from both previous deployment models, and combines them in specific way. IC T infrastructure of the Cloud Computing service deployed as community Cloud is accessible and available to certain, closed, community of users. The basic distinction of the community is that the community of the users have common goal or interest, where as example could be used government's or university's community Cloud. Community Cloud is separate category of the deployment model because it is not an public Cloud deployment model, where everyone could access, as the access to the community Cloud is determined by the client, where usually the client is some community of users. On the other hand, the private Cloud deployment model is much more closed and controlled, as the range of the users is more specific than in the case of the community Cloud.

1.3.4. Hybrid Cloud

Hybrid Cloud deployment model presents a combination of previous Cloud Computing service deployment methods, consisting of two or more types of service deployment methods, but where each deployment method represents a separate entity in the interconnected network. For example imagine private or community Cloud implemented on the structure of the public Cloud, which gives the client of the Cloud service advantages of community Cloud employment model, so the access to client's Cloud is managed, yet still being part of the easy to access and use public Cloud.

1.4. SELECTED ASPECTS OF DATA CONTROL IN THE CLOUD COMPUTING

As can be seen from the definition of the Cloud Computing itself, the services that are provided trough the Cloud Computing are meant to be available to multiple users at once, from anywhere, at any time. Virtualization, scalability, resource sharing, the basic features of cloud computing services that were introduced in the first chapter of the work are the source of a number of complications when trying to maintain security and data management standards. Cloud computing critics point to data security as a problem that can cause leakage of sensitive data, and in some cases even contractual damage liability adjusted in the SLA does not fully compensate for the

potential damage that may arise. Data security for cloud computing is the most important issue for many users, which often discourages them from using these services, up to 50% of surveyed executives have concerns about cloud computing security[28]. These concerns are often also supported by cloud companies themselves such as Apple's iCloud data leak in 2014, the leak was due to flaws in security of service when it allowed infinite attempts to enter a password[29]. Just the very essence of the Cloud Computing, which is sharing the same ICT infrastructure with multiple users poses a risk. The risk is arise from the fact that the users do not know who they share the ICT infrastructure with, or what other users' goals and interests are. Insufficient security or lack of security at all of one user, could potentially lead to compromising the security of the other users that are using the same shared ICT infrastructure. Also successfully attack on the data of a single user, the data of the remaining users may be compromised.

On the other hand, there is also a large number of views supporting cloud computing as a safer alternative to individual data management. For example, Lothair Determann in his Data Privacy in the Cloud article: Dozen Myths and Facts[30], presents 12 common security and privacy-related myths in cloud computing. Determann considers the Cloud Computing as an equally secure way to transfer data to other IT services, as all the other services are operated over the Internet.

In the Cloud Computing service, client is basically transferring responsibility for security from himself to the Cloud service provider, the main responsibility of user is to choose the right Cloud Computing service provider. Given the concerns of users about data security, it is also very important for the Cloud Computing service providers themselves, to provide users with added value in higher level of data security and better terms and conditions, without enormous cost increases for the user. However, this is a rather big challenge, constituting in preventing a large number of risks. We will discuss the individual risks and their impact, as well as the solutions, in more detail in the following subchapters of the thesis.

1.4.1. Physical security and ICT infrastructure maintenance

ICT infrastructure must physically be located somewhere and must be connected to the Internet or at least to an internal network for someone to use it. Whether it is a classic model where there is

[28] Huges, J.T., Saverice-Rohan, A. (2017). IAPP-EY Annual Privacy Governance Report 2017. IAPP-EY. p 129
[29] Apple Inc. (2014). *Apple Media Advisory: Update to Celebrity Photo Investigation*. Cupertino, CA: Apple Inc. Accessible: http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html, 18 March 2018
[30] Determann, L. (2013). Data Privacy in the Cloud – myths and facts - *Privacy Laws & Business Internationl Report*, Issue 121, p 17-21. Middlesex: Privacy Laws & Business

no use of external services or the Cloud Computing model, physical destruction or physical theft of the data is also one of the potential threats to the ICT infrastructure security. This is the least likely threat to ICT infrastructure, but the Cloud Computing service providers has to invest in to the physical protection of the ICT infrastructure, that is provided to the users. In classical models of ICT[31], it is not customary for IT infrastructure to be physically protected. Similarly, this also applies to ICT infrastructure maintenance and care. The Cloud Computing service provider, however must have professionally trained staff available at all times to be able to ensure the continued availability of the services provided. In classical models, companies often neglect to care for their IT infrastructure.

1.4.2. Data control

One of the biggest risks of the Cloud Computing is the loss of user control of the service over its own data. The user often has no to very limited idea or information about the ICT infrastructure of the Cloud Computing service provider. As a result, the provider can provide more flexible, responsive services, but the user loses track of where his data is or who uses the same infrastructure as he is, and in most cases, user has no ability to influence these circumstances.

Another related problem in this area is responsibility. The customer might mistakenly believe that deploying the system into the Cloud environment automatically transfers data and service responsibility to the Cloud Computing service provider. But reality is different. Many leading providers do not take responsibility for the data and applications placed in their infrastructure, which are also enshrined in service contracts. It means that they do not accept the transfer of risks to their side, so it remains the client's responsibility to deal with them. The IaaS, PaaS, and SaaS models differ in the level of control over individual components, data, and applications in relation to customers and providers.

[31] By the classical model of ICT it is meant that the ICT infrastructure is owned and managed locally by the user, who owns and runs the ICT infrastructure

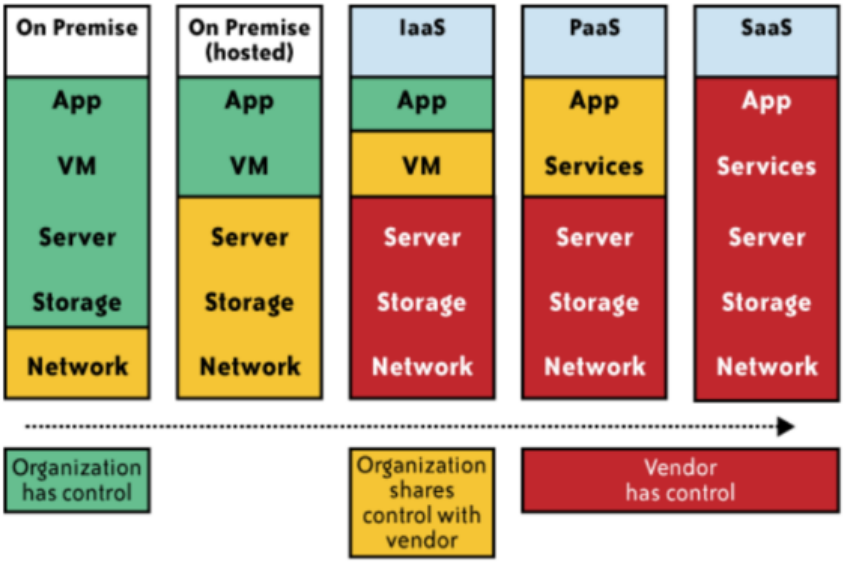

Figure 2 – Level of control across different Cloud Computing service models
Source: Maher, T. (2009) p 60

In the Cloud, unfortunately, the control over data available to the use varies in different service models. Figure 2 shows the limited amount of control that customers have in different layers for the three service models – IaaS, PaaS, and SaaS, compared to the more classical approach of hosting and on premises ICT infrastructure. In IaaS, users have more control than SaaS or PaaS. The lower level of control has made it almost impossible, where in SaaS and PaaS models it is more challenging than in IaaS. This fully show the importance SLA's have in Cloud Computing, as with lower control, they become the only tool for customer to understand basic concepts used by the Cloud service provider.

Customer may have troubles even locate the own data, as especially big Cloud service providers have many servers across the globe and generally it is unknow what formulas are used to determine where the data will be stored.

1.4.3. Abuse of the role of privilege user role

Privileged users are the employees of the Cloud Computing service provider, who have partial or full access to service's users data[32]. Companies must have at least partial access to user data and data in order to be able to respond and resolve potential issues. Most of the Cloud Computing

[32] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. (2012). Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency. Access: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security, 19 March 2018. p 31

service providers have a narrow circle of dedicated employees who have full access to data for auditing or legal requirements. Selection of employees with access to user data is significant issue as those employees are the source of potential risk.

The protection from abuse of the privilege user role may be achieved by limiting access to the ICT infrastructure only to the authorized personnel. This could be potentially achieved by implementing heavy access control, segregation of responsibilities and setting segments, where each employee has access only to own, assigned sector, where all of this measures should be supported by adding strong management level, to make sure said measures are upheld[33]. Ideally, the employees of the Cloud service provider should undergo security audits, helping to prevent and detect suspicious behaviour. Also implement contracts should contain clauses requiring employees to upheld the security requirements. Implementing encryption is also good way how to prevent malicious activities.

1.4.4. Data security and segregation

Users of cloud computing can send or store data containing a variety of information and some information can be sensitive, such as personal information or trade secrets. Digitized data must therefore be protected from being disclosed to a third party. This situation is not only a possibility, but unfortunately a fact, that each year we are seeing more and more data breaches, so data security is becoming necessity, for the Cloud Computing service providers, that has to be implemented properly and at the highest possible standard[34]. Also it could become part of the market, that the Cloud Computing service providers will see it as the cutting edge between themselves, that could give them advantage, as with better security come also better privacy, which is something Cloud Computing service providers may try to use in the competition market[35]. Data can be protected by multiple technical measures such as the use of antivirus protection, firewall, encryption, and so on. Encryption is used to conceal data content that is encrypted so that only those who have the correct encryption key can read it. Encryption is a standard security measure used by some companies to

[33] Kazim, M., Zhu S.Y. (2015). A survey on top security threats in cloud computing - International Journal of Advanced Computer Science and Applications, Vol. 6, No. 3, p 109 - 113. Accessible: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.6079&rep=rep1&type=pdf ,19 Mar 2018.

[34] Romanosky, S., Hoffman, D. A., Acquisti, A. (2013). Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, Volume 11, Issue 1, 74 – 104. Available: https://ssrn.com/abstract=1986461, 19 March 2018. p 2

[35] Kerber, W. (2017). Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int)*, 7/2016, Munich: C.H.BECK, p. 639-647, ISSN 0435-8600. Available: https://ssrn.com/abstract=2770479, 19 March 2018. p 4

protect some sensitive data, but it is still an exception. Data can be encrypted at different levels of IT structure:

- Encryption on user's device
- encrypting communication between the user and the service
- Encrypt transmission between the user's device and the service
- encrypting data stored by the provider

It depends on the will of the user or encrypts the data before the transfer to the service. But encryption of communications and data transmission is already the responsibility and role of the service provider. Encrypting communications and transmissions prevents data capture from 3rd party. If the communication was not encrypted, it would be very easy to obtain the user's login data only by monitoring the data flow. Similarly, the data sent could be captured. However, encryption prevents the data from being read, even if it is captured. Encrypting data stored with the Cloud Computing service provider prevents unauthorized access to that data.

There are 2 basic encryption models, a symmetric and asymmetric cryptographic model[36]. For symmetric models, the same encryption key as decryption key is used. Asymmetric models use 2 public and private encryption keys. Symmetric encryption is used in large volumes of data where asymmetric encryption has not been effective, many times or impossible, for its complexity.

But even implementing encryption does not automatically means that everything is safe. For example Google support encryption of the data stored and transmitted to the Cloud service they provide, however they also manage the encryption keys, which means that the users do not have control over who can access their data[37]. In a such situations, it is advised to add extra layer of encryption that happens before data are transmitted and stored on the Cloud service.

Data segregation of individual service users is also a very important element of data protection and control for users of the Cloud service. Segregation means not only the separation of data itself so that they do not interfere with each other, but also to prevent access by other users using the very same ICT infrastructure on which the data is located[38]. If there were no segregation of

[36] Maher, T. (2009) *supra nota 20.* p 67
[37] Encyclopedia of Cloud Computing. (2016). *supra nota 21*. p 245
[38] Bisong A., Rahman S. M. (2011). An overview of the security concerns in enterprise cloud computing - *International Journal of Network Security & Its Applications*, Vol.3, No.1, p 30 - 45. Chennai: AIRCC Publishing Corporation. p 41

individual users' data, the data would be compromised by technical errors, deliberate actions by other users or by third parties. Data encryption is one of the possible and used measures to prevent other users from accessing data stored on a shared IT infrastructure.

1.4.5. Data integrity, data localisation and data transfer

In addition to data security, data integrity must also be taken into account. Although the data will be encrypted, it may become unclear, basically making it impossible to provide the service[39]. The Cloud service providers often move data between different ICT infrastructures to ensure the flexibility of the provided services[40].

As explained here before, one of the most important attribute of the Cloud Computing is the scalability, which allows the Cloud Computing service providers to flexibly it's ICT infrastructure to process data or offer computing power according to customers needs, where this could potentially happen using ICT infrastructure from all around the globe. This produces technical risk, that the data may become corrupted or otherwise violated[41] and also it imposes legal risk for the customer. The basic legal problem is that data may be stored and processed in different places and jurisdictions, which causes questions and doubts for the clients of the Cloud service. Some Cloud Computing service providers have created zones in which they provide their services, so they can provide own customers with at least this limited safeguard.

But with possible application of different jurisdictions, customers have to tackle many other questions, such as compliance with the local laws, where for example data protection regimes in the EU are different to the one in the US, and clients and Cloud service providers alike, are trying to keep the data about European data subjects within the EU. Except the question of the data protection, there also the question about which country's authorities have potential jurisdiction over the data. When using the ICT infrastructure in more than one country it is possible that

[39] Liu, H. *et al*. (2017). Identity-based provable data possession revisited: Security analysis and generic construction. – *Journal of Computer Standards & Interfaces*, volume 54, p 10 – 19. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916301015, 18 Mar 2018. p 10

[40] Parekh, D. H., Daen, R. S. (2013). An Analysis of Security Challenges in Cloud Computing - *International Journal of Advanced Computer Science and Applications*, Vol. 4, No.1, p. 38 - 43. **Bradford:** The Science and Information (SAI) Organization Accessible: https://thesai.org/Downloads/Volume4No1/Paper_6-An_Analysis_of_Security_Challenges_in_Cloud_Computing.pdf, 19 March 2018. p 41

[41] Xue, L. *et al*. (2017). Provable data transfer from provable data possession and deletion in cloud storage. - Computer Standards & Interfaces, Volume 54, p 46 – 54. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916300630, 19 March 2018. p 48

authorities of more than one country could have jurisdiction, which is quite troubling for most of the clients.

1.4.6. Data availability

If user data is segregated, it is necessary to ensure that the data is available to the user at any time. There are three basic risks to data availability, not the risks that would arise directly with cloud computing, but cloud computing services are of increasing importance.

The first risk is network attacks where third party activity causes service unavailability. The second risk is the availability of the service provider's IT infrastructure itself. Companies guarantee a certain degree of availability of their services, but as shown in the table below (Figure 3), 99% availability during the year means service unavailability for more than 3 days of the year.

	Total downtime (HH:MM:SS)		
Availability	**Per day**	**Per month**	**Per year**
99.999%	00:00:00.4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

Figure 3 - Cloud Computing service availability explained
Source: Maher, T. (2009) p 70

For cloud computing companies, however, a small outage means the risk of losing clients and reputation. For example, in 2009, Google's Gmail recorded a 90-minute downtime due to a technical problem[42]. However, customers have responded with a lot of concern to the downtime, and the company rather offered compensation for suffered damaged to the users[43].

[42] Tchernykha, A., Schwiegelsohnb, U., Talbic, E., Babenko, M. (2016). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. - *Journal of Computational Science*, In press, Accessible: http://www.sciencedirect.com/science/article/pii/S1877750316303878, 19 March 2018. p 2
[43] GOOGLE Inc. (2009). *Google Apps - Gmail: Incident Report February 24, 2009*. Google Inc. Accessible: http://static.googleusercontent.com/media/www.google.com/sk//appsstatus/ir/1nsexcr2jnrj1d6.pdf (19 March 2018)

Another risk arising is backup and subsequent data recovery. Many Cloud Computing service providers do not back up their users' data, or back up their data as a service at an additional cost. By backing up, it is possible to avoid loss of data that is transferred within the provider's IT infrastructure, or loss of data due to technical failure or other unforeseen circumstances.

2. NEW LEGISLATION REGARDING ELECTRONIC EVIDENCE

Law enforcement authorities around the world are seeking ways how to access data about and content of electronic communications, like instant messages, emails and social media posts, stored on servers and in data centres located outside of the country[44]. The new technologies and trends created architecture that allows companies to store data at the geographic location most convenient for given process. As a result, electronic data connected to crime, or seek by the authorities, may be stored in completely different country as the said criminal activity happened. This has caused problems for governments all around the globe, including the United States and EU, where they have to seek data stored outside their territorial jurisdictions in the course of criminal investigations. Both US and EU have reacted to his by introducing new regulations that will tackle the topic, we will discuss it in detail below.

2.1. CLOUD ACT

Clarifying Lawful Overseas Use of Data Act (further only CLOUD Act) was introduced in the US on March 23, 2018 as amendment to Stored Communications Act. Although the draft was introduced and discussed to some extent, the act itself was signed into the law in not the most usual way, as CLOUD Act was signed as part of the cumulative spending bill. And there you have to be strong enough to get to page 2201 the US spending bill to find the CLOUD Act. First, we discuss the Supreme Court case between Microsoft and the US Department of Justice, regarding access to emails stored abroad and how CLOUD Act resolves this case. Then we have brief explanation of the new executive agreements system included in the Act, before short discussion about how these executive agreements will work in real life. Each of these agreements is subject to legal requirements, as explained below.

2.1.1. Microsoft v US Department of Justice

This, still ongoing, dispute between Microsoft Ireland and the United States Department of Justice regarding the reach of the Stored Communications Act, is currently pending at the US Supreme

[44] Woods, A.K. (2016). Against Data Exceptionalism. - *Stanford Law Review*, Volume 68, p 728-788. Stanford :School of Law, Stanford University

Court. The beginning of the case dates back to the year 2013 and deals with production of evidence by Microsoft, in this case e-mail data stored on it's Ireland based server. The US argued that warrant issued by US government has authority to compel US based companies to produce evidence required, no matter where the data is located. Microsoft on the other hand argued that authority of US government issued warrant extends only to data located within the territory of the US. In Microsoft's point of view, as was argued before the US Supreme Court, in this particular case, US are required to request the data from foreign country authorities (Ireland's authorities in this case) and wait for foreign authorities to access the data and hand them back to US government. When Microsoft won the dispute in the US Court of Appeals for the Second Circuit, even Microsoft itself admitted that this situation is not the ideal one and suggested to Congress updating Stored Communications Act so it reflects the needs of the new, modern digital age, when it comes to warrant authority.

The CLOUD Act provides such solution that has been urged by Microsoft and may others, tech giants as Google, already mentioned Microsoft, or Apple and US government alike. The CLOUD ACT changes the authority of Warrant issued by US government under Stored Communications Act, so it compels companies to disclose data in it's [company's] control and/or custody regardless of data location.

The CLOUD Act also includes solution to the cases when the interest of other countries call to the question. In the CLOUD Act includes also provisions about comity, where term "comity[45]" represents legal test that will be used by courts when considering interest of foreign countries. Statutory provision about institute comity applies in limited cases, where US government issues warrant for data located outside of the US and this request creates conflict between the request of the warrant and the law of a qualifying foreign government (term "qualifying foreign government" applies to countries that have executive agreement with US under CLOUD Act, this matter will discussed below) and on the basis of comity grounds, person who warrant is issued to, may start motion for quash of the warrant. When the newly introduced comity grounds are not available, the CLOUD Act explicitly preserves the common law comity claims available for such occasions.

[45] As defined in the case U.S. Supreme Court, 159 U.S. 113 (1895), *Hilton v. Guyot*: "Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and goodwill, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons was are under the protection of its laws."

2.1.2. The origins of the CLOUD Act

The new legal regime governing the executive agreements between the US and another foreign countries, is regulated by Section 105 of the CLOUD Act. The best way to explain this newly introduced system is understand the background that led to creation of this piece of legislation. As we illustrated in previous paragraph, using the case of Microsoft v US Department of Justice, law enforcement all over the world face the same problem – the globalisation of the criminal data. During the course of the criminal investigation, authorities have obtain data or communication that are often kept in the Cloud service, that has server in completely different country. Today in this multimedia driven age, our email, social network content and other data, are shattered all over the planet, as it is incredibly easy to send the over the country by one simple click. Nowadays most of the tech companies are based in the US, where the option of the direct cooperation between companies (based in the US) and the foreign (non-US in this case) countries limited by the provisions of the Electronic Communications Privacy Act, even in case when country's authorities were seeking data connected with own citizens. Foreign countries authorities have to made request for the data to the US government, using the Mutual Legal Assistance Treaty option, that usually proven to be time consuming and with uncertain result.

Governments and tech companies have long searched for ideal way how to address the possible changes. Not only the Mutual Legal Assistance Treaties proven to be difficult and time consuming, companies are often caught in middle of contradicting duties, to hand over data to authorities of one country, while the data are protected under the laws of another where the data are located (or the company is located). Sometimes it went even that far that authorities started to threaten to impose sanctions, either monetary or criminal, where in such cases it ended up in long lasting court proceedings exhausting authorities and companies.

Facing this new, complex challenges, extensive discussions have been held in recent years about creating a new system of cross-border data access. Many voices were arguing for keeping the system of the Mutual Legal Assistance Treaties, arguing it would guarantee that the transfer us overview by countries authorities, guarantying the upkeep of the standards of criminal proceedings, human right, privacy rules and such. On the contrary, countries are also trying to place measures that prevent data transfer to other countries at all.

US government decided to choose this way of dealing with the topic, as broad, international consensus achieved through the international treaty proven to be very difficult. At the same time as the CLOUD Act was being drafted, US and UK governments were working on mechanism allowing mutual cooperation in case of evidence production of electronical data in criminal case involving cross-border cooperation. However, in the end, these aspirations could not be implemented into the law, as they were opposed mainly by the US Electronic Communications Privacy Act.

Also, the Microsoft v US Department of Justice case pointed fingers to this problem, which helped to speed up the discussions and find solution that would suite the US government and tech companies alike. The CLOUD Act includes changes that allow for authorisation of similar agreements as the one with UK, mentioned in previous paragraph, by implementing privacy safeguards.

2.1.3. The new system of executive agreements

The executive agreements are regulated by the Section 105 of the CLOUD Act, that provides the mechanism under which the US may enter into executive agreement with foreign country, under the condition that foreign country meets the requirements set by the CLOUD Act. First step is that Attorney General, in cooperation with the Secretary of the State, in writing certifies that legal regime of the foreign country in question "affords robust substantive and procedural protections for privacy and civil liberties[46]", when dealing with data in question. Foreign country applying for executive agreement have to have appropriate minimisation measures for US citizens, data access, retention and deletion. All executive agreements entered into force according to CLOUD Act, are subject to review and may be invalidated by the US Congress.

Every single request for data, made under the executive agreement must also comply with a list of requirements, including the following:

A. It is prohibited to target US citizen and resident data. For such data, foreign countries' governments still need to go through the Mutual Legal Assistance Treaties procedure. This important provision reflects the train of thought of the legislators, that the US has much

[46] CLOUD Act section 5 / 18 USC 2523 (b)(1)

less justification to insist on US standards when a foreign authority is seeking data of its own citizen, based on the executive order, just because the data is stored on the US soil or is held by a US based company.

B. It is prohibited to target data of US citizen indirectly and it is prohibited for foreign government to share data of US citizens back with the United States, unless it is related to potential significant harm or threat of such harm to the United States or United States persons.

C. The request by foreign country authority must be specific, i.e. must be targeting a specific person, address, device, account or hast another specific identifier.

D. The request must be based on "articulable and credible facts".

E. The request must be subject to review or oversight by a court, judge or other independent authority.

F. The live intercept orders must be for a fixed, limited duration and may not last any longer than is reasonably necessary to accomplish the approved purposes and must be issued only if the same information could not reasonably be obtained by another less intrusive measures. These requirements similar to key requirements set out in the US Wiretap Act.

G. The data gathered trough request may not be used to infringe human rights and countries have to have implemented measures that ensure human rights standard.

H. Foreign country entering into executive agreement have to agree to be subject of compliance review, where US government shall be enabled to track how data was used by foreign authorities, thus preventing abuse.

The CLOUD Act tackles a complex and important area of law and is able to provide us with US vision on what rules should apply when one government seeks criminal evidence, but privacy and sovereignty interests of another country are also involved.

The most immediate effect of the Act is to the Microsoft v US court case, as the case itself was dismissed[47] on 17th April of the 2018, as the CLOUD Act grants authority to US issued warrant.

[47] SUPREME COURT OF THE UNITED STATES, 584 U. S. ____ (2018), 17.4.2018. *United States v. Microsoft Inc.*

This case could potentially be the reason why the CLOUD Act was signed in such a hurry. The new provisions regulating executive agreements will become important tool for US and big talking point in the future. Likely, there will be negotiations held with the UK and EU. These talks and negotiations of executive agreements will offer many thoughts and concerns about the CLOUD Act's privacy and human rights implications that could be there.

2.2. New proposal for EU E-evidence legislations

On April 17 of the 2018, the European Commission published draft of the new piece of legislation, regulating electronic evidence in criminal matters that deals with the handling cross-border requests for electronic evidence in the criminal matter within the members of the EU. The European Commission proposed two separate pieces of legislation:

a) Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (further only E-evidence Regulation) that enables law enforcement authorities of the EU Member States to issue order for production of the evidence, addressed to the communication and cloud providers based in other Member States of the EU or based outside of the EU, regardless of where the data is located

b) Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (further only Representatives Directive) that would require providers offering services in the EU Member State to establish legal representative one Member State of the EU for the receipt of cross-border demands.

If implemented as proposed now, both the E-evidence Regulation and Representatives Directive will together allow, in criminal proceeding, authorities of all EU Member State access to the data of internet users, all over the globe.

This is caused by the fact, that under some conditions, EU Member state authorities may compel providers to disclose data regardless of their [data] location and regardless the citizenship of the user the data are about. This presents risk for human rights and privacy and surely discussion will follow.

2.2.1. Representatives Directive

The reasoning and preamble of the Representatives Directive points out the inconsistent and different practices of the EU Member States when dealing with electronic evidence. Some EU Member States, like Germany, already have legislation that requires providers of selected services to appoint local representatives that would deal with Authorities and handle cooperation requests, other Member States use the methods of the international cooperation. Also Member States also applies different criteria to determine jurisdiction over the data and service provider, where some Member States base jurisdiction on the location of the service providers main office, some determine the jurisdiction based on location of the data in question, some use other criterion[48]. Member States also have different rules about enforcing the cooperation with service providers.

That's why this Directive proposes to unification, in the way that certain service providers will be required to appoint representative in EU Member State, that would cooperate with the law enforcement authorities in the EU, this representative will also serve for the requirements of the E-evidence Regulation, as discussed below.

The broadest factor determining whether the service provider has to establish such representative is that service provider offers service in Member State. Recital 13 of the Representatives Directive however states that the mere fact that the service is accessible in the Member State is not enough to establish this duty, there also must be significant number of users in at least one Member State, or the service is targeted on one or more Member States or the service is advertised in in at least one Member State. This could prove to be difficulty especially for small but rapid grooving services, as nowadays it's not difficult to surpass these requirements. For such cases there is remark in the notes that, these services may be provided by third parties, similarly as for the GDPR.

The entities that duties arising from this Directive applies to, are described broadly:

- providers of electronic communications services, that store data for it's users
- providers of information society services that store data for users
- providers of internet names and number services

[48] Further discussion about jurisdiction will follow

Providers of information society services for whom the data storage is not the defining component not required to have representative, in this case as example was used provision of legal or architectural services online. Domain names registers, proxy or VPN[49] service providers are however required to appoint representative.

The service provider may choose the Members State where the representative will be appointed, given the condition that the provider offers service in that particular Member State, or has office there. One representative may serve whole EU and service providers may not be obligated to establish representatives in specific Member State. The proposal for new legislature, proposed by the EU, misses the requirement to establish central register (or point of contact) of requests either in EU or each Members State, that would add more clarity and transparency to the process[50].

2.2.2. E-evidence Regulation

The main points that the E-evidence Regulation proposal brings are European Production Order and European Preservation Order. Where the European Production Order would authorise Member State authorities to compel service provider (or representative as mentioned in previous part) in another Member State, or outside of EU, to disclose transaction records or stored content of communication in criminal investigation. European Production Orders for subscriber information and access data does not require judicial approval, which means it could be issued also by the prosecutor or another competent authority as defined by the issuing Member State. "Access data" is new category of data, defined in the Article 2 (8) of the E-evidence Regulation proposal, as data "related to the commencement and termination of a user access session to a service". The other instrument introduced in this proposal is European Preservation Order, authorizing authorities of Members State to compel service provider to preserve content data, transaction records, access information or subscriber information, until European Production Order or another warrant is issued. European Production Order does not need court authorisation. Similarly to the Representatives Directive, the E-evidence Regulation includes rather wide description of providers on whom such orders can be issued to, where the entities re the same is as covered by the proposal of the Representatives Directive. When dealing with entity that is outside of the scope of the E-evidence Regulation, but the entity is using hosting or other infrastructure service, where the

[49] Virtual private network
[50] EuroISPA. (2017). E-Evidence Proposal: EuroISPA Criticises the Privatisation of Law Enforcement. Brussels: EuroISPA. Accessible: http://www.euroispa.org/e-evidence-proposal-euroispa-criticises-privatisation-law-enforcement/, 18 April 2018

provider falls within the scope, the request should be addressed to the entity and not the provider.

European Production Order for access data and subscriber information may be issued without authorisation by the judge and it may also be issued in case of all criminal offences. European Production Order for content and transaction data can only be issued during criminal investigation of crime with maximum penalty of at least three years of custody, explicitly are listed proceeding in the case of counterfeiting of non-cash payment methods, crimes of sexual abuse and exploitation and terrorism. This could meant that the authors of the proposal are expecting objections against to broad options where the European Production Order could be issued, so the explicit proceeding are the list of the most important cases where this procedure should apply and the rest of the cases could be free for negotiations.

Article 12 of the proposal discusses reimbursement, where compelling company may claim reimbursement for costs, but only when the issuing Member State has this situation regulated in domestic law. This could lead to different approaches of Member States, where uniform regulation could potentially limit the number of requests, as countries would consider filling request much more.

When it comes to the execution of the European Production Order or European Preservation Order, the addressee[51] is presented with European Production or Preservation Order Certificate. The biggest issue here is that the provider does not see, in the Production or Preservation Order, information that explains or shows the grounds upon which the order was determined to be necessary and proportionate. Instead, the Certificate provides only information necessary to identify the account from which data are sought, all in a standardised format of the Certificate. Articles 9 and 15 of the Proposal imply that the addressee may challenge a Production Order, if complying with it would violate the rights of the concerned individual and may be brought in the jurisdiction where the Order is served. However, the Regulation Proposal and it's Annex 1 make it clear that the provider will generally not receive the information that would be necessary to determine if the Order can be challenged or not.

In addition, the Regulation proposal does not require the alleged criminal activity to be a crime in both the issuing Member State and the Member State in where sits the addressee or it's representative, or the Member State request subject resides or is a national of. This is higlz

[51] Addressee is the service provider, as defined Article 2(3) of the E-evidence Regulation, that has to fulfil the order

suspicious solution that shows a high confidence in in all Member States because all Member States legislation and criminal procedures, as all Member States can issue Production Orders.

The Regulation Proposal also imposes short deadlines for addressee response - 10 days in normal circumstances and six hours in an emergency situation, when there is an imminent threat to life or physical integrity of a person or critical infrastructure.

Annex 1 of the Proposal also permits issuing authority to specify other deadlines in the case of the non-emergency situations, but it does not specify any parameters for the duration of those deadlines. This is highly risky situation, where the pressure is put on the addressee, that has to protect the interests of the request subject, but has very limited time to do so. This situation calls for a risk that addressee will comply with requests that are against request subject's interest and lack other requirements, just because the compliance deadline is approaching. According to the Article 11 of the Regulation Proposal, issuing authority may decide not to provide request subject of notice about Production Order when it would obstruct the criminal proceedings.

3. ANALYSIS OF SLECTECTED PROVIDERS OF THE CLOUD SERVICES

The smartphone today is far from being used only for calling other people. Most owners also use it as an alarm clock, for taking pictures, browsing the Internet, reading emails, watching online videos, and various activities that are offered by countless applications. One of the most popular activities is instant messaging over the internet, where Facebook Messenger and WhatsApp are the two most popular options.

SMS messages have been with us for over 25 years. Once, massively popular way of communication, is nowadays not what it used to be. Fast adoption of smartphones, vastly available mobile internet access and smart apps.

People send about 20 billion SMS messages per day, which is almost nothing compared to how many messages are sent using either Facebook Messenger and WhatsApp. Both services are currently part of the Mark Zuckerberg's Facebook and are daily handling about 100 billion messages. That's five times more than what operators are doing. Both WhatsApp and Facebook Messenger are growing at fast pace. Only two years ago they processed 40 billion messages a day less.

WhatsApp is currently the most used messaging app worldwide, while Facebook Messenger is closing on in second, with competition far behind, just check the Figure 4 below. Third app, Viber, is combined first or second in only ten countries around the globe. This illustrate how big imperium has Facebook gained in the world of instant messaging.

Facebook has bought WhatsApp for $19 billion in 2016 and now its proving to be the right decision done by the company. Since the Facebook done lot of work to move WhatsApp on the Facebook infrastructure, so they can offer better and faster services. Both Facebook Messenger and WhatsApp have their very own pros and cons. The users tend to rely on Facebook Messenger or WhatsApp for different reasons. To better understand the differences between both applications, we will compare them in the next subchapter.

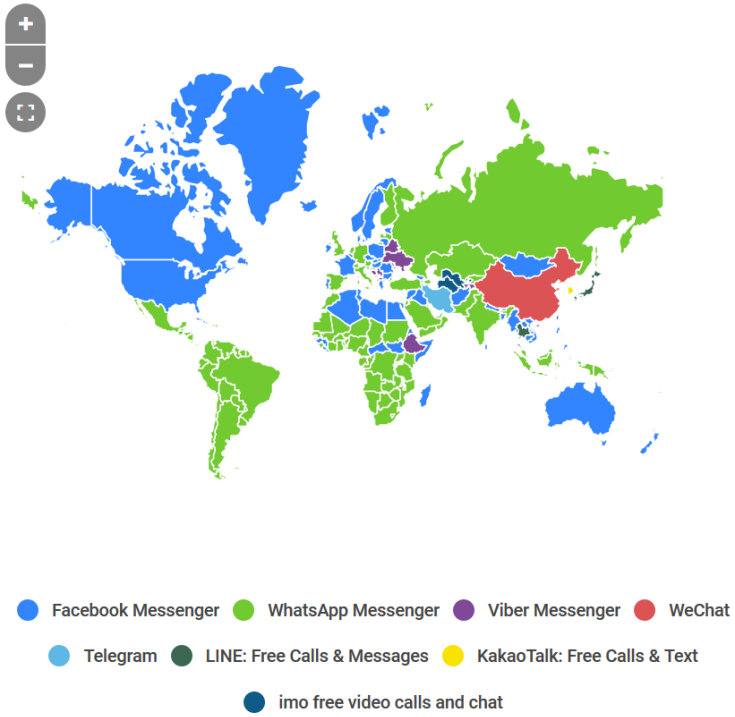

Figure 4: Mobile Messaging App Map – February 2018
Source: https://www.similarweb.com/blog/mobile-messaging-app-map-2018, 10 April 2018

3.1. Head to head comparison

While both Messenger and WhatsApp perform almost the same functions such as free VoIP calling and group messaging through the internet, the two apps are distinct from each other in some key factors.

A) Registration

In order to use the WhatsApp, you have to create account just for the service and verify the account. Then you can use the service. Facebook Messenger on the other hand is tied to the Facebook account and you cannot use the app without having account on this social network.

B) End-to-end encryption

All that you send on WhatsApp is end-to-end encrypted, which isn't the same for Facebook Messenger. This implies messages sent on WhatsApp are just visible to the sender and receiver,

using the app and to everyone else the message is just scramble of random strings, even the WhatsApp can't read them.

Facebook Messenger on the other hand does not encrypt messages by default, as the service being part of Facebook account. This way you see messages sent and received trough Facebook Messenger in your Facebook chat or inbox, making them easy to access. However, the Facebook Messenger has option to enable end-to-end encryption, making the messages visible only using the Messenger app, however this is not vastly popular option among the users, as they loose the option to read the messages on their Facebook account.

C) Sharing photos and other documents using the app

Both apps, Facebook Messenger and WhatsApp, allow it's users to send photos and other documents. Both also allow you to use footage from your device camera, device storage or some other apps. Both apps allow you to save the received documents on device storage, but users must take the added step of doing it manually inside the messaging app.

Unlike Facebook Messenger, WhatsApp has a limit of 10 files per single message. Both Apps limit the size of the file sent, but none limits the type of the file. Facebook Messenger's other (dis)advantage over WhatsApp for is its natural integration with Facebook, where you can use the files sent trough the Facebook Messenger even using Facebook account, unless the message is end-to-end encrypted as mentioned before.

D) VoIP

Both Facebook Messenger and WhatsApp also offer VoIP calling through the app.
One of the reason why WhatsApp has become so popular is its ability to perform using wide range of devices and signal strengths. WhatsApp's popularity is so big thanks to its ability to perform stably using all kind of networks like 3G, Wi-Fi, and even 2G. Facebook Messenger on the other hand uses it's integration with Facebook to it's advantage, allowing you better integration, with possibility to make a group calls for up to 50 people.

When talking about calls, Facebook Messenger allows you to contact wider range of contacts than WhatsApp on all counts. While WhatsApp only lets you to contact other WhatsApp users, who re

in your device contacts, Facebook Messenger, depending on users privacy settings, allows you to contact anyone, who is using the app downloaded.

WhatsApp also allows users to back-up the messages and data on popular Cloud storages such, iCloud or Google Drive, however this ruins the whole point of the end-to-end encryption, as the messages will be stored on 3rd party service, however it's up to the users to enable this service.

3.2. Facebook Messenger

As mentioned above, Facebook Messenger is app available to the users that have Facebook account and such has the same Term & Conditions as Facebook itself, as they are part of the same document[52]. As Facebook is primarily build as social network, the Terms & Conditions reflect that fact.

As such, Facebook is build around sharing feeling, your life and pictures with others, that's why Facebook asks for quite extensive permission to use the data and content you upload in the point 3.3. of the Terms and Conditions. This is to ensure Facebook is able to share your data and content with your Facebook friends,[53] as they may be situated all over the globe. In order to achieve this, Facebook also has to be able to transfer data outside the country user uploaded them. Facebook delivers this information in last paragraph of the chapter 1 of the Terms & Conditions. With having servers in US and EU only, the has information for EU users that their data will be transferred outside of the EU, doing so using the standard contract clauses approved by the European Commission, as explained in another document called Data Policy[54], in paragraph "How our global services operate."

To reflect this and also legal requirements, Facebook has created it's European branch, Facebook Ireland. Using this solution, Facebook stipulates Irish jurisdiction over the EU consumers. The rest of the world has the Terms and Conditions governed by US laws. In this it would mean that EU Members State authorities could in criminal matters use the new E-evidence rules, without need

[52] Facebook Ireland Limited. (2018). *Terms of Service*. California: Facebook Inc. Accessible: https://www.facebook.com/legal/terms/update, 14 April 2018

[53] Facebook users you have contact with

[54] Facebook Ireland Limited. (2018). *Data Policy*. California: Facebook Inc. Accessible: https://www.facebook.com/about/privacy/other , 14 April 2018

to apply the international cooperation proceedings. However there is still chance that some of parts of the data could be residing exclusively on the servers of the company that are located in the US, which would require international cooperation.

Facebook also uses the Privacy Shield framework for two of its services[55], Ads and Workplace Premium, as messenger is integrated with Facebook and advertisement, so Privacy Shield framework applies to it as well. Facebook also have guidelines[56] for law enforcements authorities and requests system that allows easy communication with authorities.

3.3. WhatsApp

WhatsApp is to some extent using the same infrastructure as Facebook, Terms & Conditions[57] are very similar with minor changes. Similarly as Facebook Messenger, WhatsApp has needs users to agree to give license to WhatsApp in order for the app to be able to send the messages and content to intended receivers. Like Facebook Messenger, WhatsApp needs to transfer the data all over the world, in order to deliver the message and content to intended receivers. As mentioned before, WhatsApp is using Facebook's infrastructure to do so, however, the messages and data encrypted during the transfer and are deleted from the serves latest 30 days after sending the message, even if it was not received or delivered properly, as state in the Your License to WhatsApp part of the terms and conditions.

However, WhatsApp Terms and Conditions include provision that WhatsApp "works and shares information with the other Facebook Companies" , but on the other hand stating that "[n]othing you share on WhatsApp, including your messages, photos, and account information, will be shared onto Facebook or any of our other family of apps for others to see, and nothing you post on those apps will be shared on WhatsApp for others to see, unless you choose to do so." This could prove to be tricky part of this Terms.

[55] Facebook Inc. (2018). *FACEBOOK INC. AND THE EU-U.S. and SWISS-U.S. PRIVACY SHIELD*. California: Facebook Inc. Accessible: https://www.facebook.com/about/privacyshield, 14 April 2018
[56] Facebook Inc. (2018). *Information for Law Enforcement Authorities*. California: Facebook Inc. Accessible: https://www.facebook.com/safety/groups/law/guidelines/, 14 April 2018
[57] WhatsApp Inc. (2018). *WhatsApp Legal Info*. California: WhatsApp Inc. Accessible: https://www.whatsapp.com/legal?eea=0#terms-of-service, 14 April 2018

The biggest difference however is in the governing law, where WhatsApp has in the Terms& Conditions that they are governed by US law, more specifically by law of State California, not having different Terms & Conditions for different regions of the world.

3.4. Facebook Messenger and WhatsApp as over-the-top service providers

As we described both, the Facebook Messenger and WhatsApp we can now try to establish their position, according to legislation. However, before that, it's good to mention that we have not established them as Cloud services yet. Cloud services are defined in the chapter 1.1. of this work, as on demand, scalable and elastic services accessed through the internet. As we described both of the applications above, the applications are accessible through the internet, are on demand, as they work only when message are sent or received, or the calls are made. Both services are using the same pool of resources (infrastructure), they use to be able to provide the service, that scales according to the need of the user, you need different amount of resources when sending message, making a call or sending file. Thus, it's safe to establish both of them as Cloud services.

But now the more difficult part, how to define them legally? Although both of them offer options how to call and send messages over the internet, they are not regarded as being telecommunication service providers (further only TSP). Question here could be why, but the difference is quite obvious, WhatsApp and Facebook Messenger provide their services through internet, existing infrastructure, which is taken case by internet service providers, however TSP offer their services over their own network of fixed lines and antennas.

Especially in EU law, this difference made a lot, they are regarded to be Over-the-top (further only OTT) services. This description reflects that they are using existing infrastructure of internet service providers (further only ISP), where they are competing with traditional telecommunications services, changing the market. But regulators, especially in the EU have failed to reflect this change. Although nowadays the topic is being reviewed at European level, the position of the WhatsApp, Facebook Messenger and alike OTT is different to classical telecommunications services.

OTT services, like WhatsApp and Facebook Messenger, could in theory be regulated as Electronic communications service (further only ECS), as defined in the Framework Directive,[58] as this categorisation would make the biggest sense. ECS are defined in the Article 2 (c) of the Framework Directive as: "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services[59], as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

So we could break the definition of the ECS into three main points, where they:

A. are normally provided for remuneration
B. consist wholly or mainly in the conveyance of signals
C. exclude services providing, or exercising editorial control over content

A. **Normally provided for remuneration**:

This provision reflects Article 57 of the Treaty of the Functioning of the European Union and Union law, where services provision is normally subject to renumeration, as part of conducting business, where it reflects the economical nature of the relationship that is created by service provision. ECJ has interpreted renumeration in broad sense. In the case C-291/13, also regarding the position of the information society services, ECJ stated that the information society services, as defined in Article 1 of Directive 98/34/EC, has to be understood as the "service provider is remunerated not by the recipient, but by income generated by advertisements posted on a website[60]".

In this case at least Facebook Messenger would qualify for economic renumeration, as the company is generating income through the advertisement, with ads being presented even inside the app itself.

[58] Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services
[59] as Annex V of Directive 98/34/EC, as amended, explains in point 2, that (a) voice telephony services, (b) telefax/telex services, (c) services provided via voice telephony or fax are not information society services.
[60] Court decision, 11.9..2014, Papasavvas, C-291/13, ECLI:EU:C:2014:2209 Para. 26

B. consist wholly or mainly in the conveyance of signals

There is absence of any sort of guidance, how to interpret this characteristic. However, we could find some interpretation in the ECJ case C-475/12, where UPC was transmitting audio-visual package from Luxemburg to customer in Hungary via the satellite. ECJ found that it is irrelevant that UPC transmitted the package trough infrastructure owned by 3rd party, "all that matters in that regard is that UPC is responsible vis-à-vis the end-users for transmission of the signal which ensures that they are supplied with the service to which they have subscribed".[61]

When using this as analogy, WhatsApp nor Facebook Messenger are still not affected by this definition, as they are not responsible for transmission of the messages of call, at least not in full extent. The service they offer works when you have the access to the internet, but the access itself is not provided, or transmitted, or otherwise facilitated by none of them. The access to the internet is sole responsibility of the client, who still need to rely on his or her internet service provider or telecommunication provider.

C. exclude services providing, or exercising editorial control over content

Nor WhatsApp nor Facebook Messenger provides own content or edits the messages or call that happen while using their app. So this excluding point does not applies to them.

In the US, situation is much clearer, as the OTT services like WhatsApp and Facebook Messenger's are defined as "Electronic communication services" under 18 U.S. Code § 2510 (15), where they are defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications[62]". Thanks to this the CLOUD Act could build up on these definitions, unlike the new E-evidence legislation, that had to reflects status of the OTT regulation in the EU in own text, explicitly mentioning them in the recital 1.3. There is was admitted that the OTT are not currently part of the EU regulation, but are meant to be regulated under new European Electronic Communications Code (so far only proposal), that should reflect this lack. That's why

[61] Court decision, 30.4.2014, Google Spain, C-475/12, ECLI:EU:C:2014:285, para. 43

[62] Electronic communications are defined in the 18 U.S. Code § 2510 (12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds

the new E-privacy Regulation decided to use the definitions provided by European Electronic Communications Code, as both are only proposal during the period this work was written. Under the definitions provided in the European Electronic Communications Code proposal, OTT services as WhatsApp and Facebook Messenger would fall under the definition of interpersonal communications services, defined in the Article 2 (5) of the European Electronic Communications Code proposal as "service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s)".

However as mentioned above, this could prove to be tricky definition, as especially thanks to the part "provided for renumeration", it could exclude WhatsApp, as this service is provided free of charge. However, as mentioned in the analysis of WhatsApp's Terms & Conditions, the service is part of Facebook company, is using the same infrastructure and is sharing some information with Facebook. Using analogy, we could say that by sharing this information with Facebook, WhatsApp is helping Facebook to make money on advertisement, thus WhatsApp services are offered for renumeration.

However this is only assumption about proposed legislation, in the future it would be good if the EU includes the clear definition of the OTT services and includes them in the legal regulation, also it's worth noting that maybe it would be advisable, in the future to look up to US as inspiration in clarity of the definitions, which could lead to far less questions.

4. IMPACT OF THE NEW E-EVIDENCE LEGISLTURE

As shown in previous chapter, the approaches taken by the US and EU are bit different, but both of them raise many questions, especially in connection to other branches of law. However there are two main talking points, where both of the solutions started discussions.

4.1. Privacy impact

One of the biggest questions that have arisen from the CLOUD Act is privacy impact and compliance with the new GDPR in the EU. To better understand these concerns, we will discuss the main points of the new EU privacy framework, that are connect to the topic.

4.1.1. GDPR

The main goal of the GDPR is to protect all EU citizens privacy from data breaches in an increasingly data-driven world, which is different to the times in which Data Protection Directive was established. The main, key principles of data privacy, established there still apply, there have been many changes introduced by the GDPR.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This represents the maximum fine which may be imposed for the most serious infringements e.g. violation of the core privacy principles. It is important to note that these rules apply to both controllers and processors - meaning Cloud services, and OTT alike, will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been changed, so companies can no longer use long terms and conditions as base for the consent. Now the consent must be given in an easy to understand form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in and readable and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to Access

Part of the extended rights of data subjects implemented by the GDPR is the right for data subjects to obtain confirmation if his/her personal data are being processed, where and for what purpose. Further, the controller is obliged, un request, provide a copy of the personal data, free of charge, in an electronic format.

Right to be Forgotten

The right to be forgotten entitles the data subject to request data controller to delete his/her personal data, stop further procession of the data, and have third parties stop processing the data as well. The conditions for erasure, as given by the Article 17, also include data that are no longer being relevant to original purposes for processing, or a data for which the subjects withdrawn consent.

Data Portability

This is new right introduced by the GDPR - the right for a data subject to receive the personal data concerning him/her, which have been gathered, in “commonly use and machine readable format” and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Under GDPR it will not be necessary to submit notifications or registrations to each Member State local data protection authority about data processing activities, nor will it be a required to obtain approval for data transfers based on the Model Contract Clauses. Instead, processors and controller will be required to keep internal record and appoint Data Protection office, however only for those controllers and processors whose core activities consist of processing operations which require

regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

4.1.1.1. Transfer of personal information outside of EU

The GDPR allows transfer of the personal data to a third country or international organization, but only under certain set conditions, including conditions for onward transfer. Similar to the framework set forth in the Directive, the GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection. In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states only under certain circumstances.

In addition to facilitating international data transfers through new mechanisms, the GDPR also makes clear that it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country. It also imposes hefty monetary fines for transfers in violation of the Regulation.

However, US is not deemed to be country with adequate protection of the personal data, so the transfer has to be facilitated according other provisions of the GDPR. There are 5 possible solutions:

- Legally binding and enforceable instrument between public authorities or bodies
- Derogations for specific situation, according to the Article 49 of the GDPR. Include likes of explicit consent for the transfer, transfers on the basis of performance of a contract, necessary for important reasons of public interest etc.
- Binding corporate rules in accordance with Article 47 of the GPDR
- Standard data protection contractual clauses adopted in accordance with the examination procedure referred to in Article 93(2)
- An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards according to the Article 46.
- An approved certification mechanism pursuant to Article 42
- Privacy Shield

4.1.1.2. Extraterritorial application of the GDPR

Probably the biggest change, that is brought by the GDPR, to the subject matter of data privacy comes is the extended jurisdiction of the GDPR, as will apply to all companies that are processing the personal data of data subjects residing in the Union, regardless of the company's location. Till now, there was territorial jurisdiction of the Data Protection Directive[63] referred to data processing 'in context of an establishment'. This led into number of court cases. GDPR makes it very clear - it will apply to the processing of personal data of the EU citizens and residents, regardless of the location where the processing takes place. The means that the GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, if the activities relate to: offering goods or services to EU citizens and the monitoring of behaviour of EU citizens, that takes place within the EU. Entities processing the data of EU citizens will also have to appoint a representative in the EU. Let's discuss these requirements, to determine when GDPR applies.

A. offering goods or services

The biggest question determining whether the company offers services or goods in the EU is not the availability itself, as nowadays wit the internet this would mean that by simply having offer on the internet you would fulfil this requirement. However, the intention and anticipated outcome is the important thing. There are two important ECJ cases that explain offering of goods or services in more detail and what determines it. First is case Google Spain case,[64] where Google had only marketing subsidiary in Spain and argued that Spanish data protection laws does not apply to this subsidiary, thus not applying to Google at all (at that time company did not have EU subsidiary). But the ECJ found that Google offered advertising directed at Spain, in Spanish, next to the search results, which made the activities of Google Spain and Google US inextricably linked. The argument for Google's data processing activities being subject to Spanish data protection laws, was that Google orientates its activity towards the inhabitants of Spain.

[63] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On the protection of individuals with regard to the processing of personal data and on the free movement of such data
[64] Court decision, 13.5.2014, Google Spain, C-131/12, ECLI:EU:C:2014:317

Second case is Weltimmo case,[65] where Slovakian company offered it's service in Hungary. The company was not only operating in Hungary, it also offered it's service there and had website offering it's services in Hungarian language. The ECJ found that if a company operates a service in the native language of a country (applies of course only when the languages are different) it could be held accountable to that country's data protection laws.

To wrap this up, the availability of a business's website to EU data subjects is not sufficient to establish an intention to offer service or goods in the EU. However, if the website is in an EU language which is different to business, the offer for goods or services is in an EU currency or, it is explicitly targeting EU citizens, this could be the proof that business has the intent to offer service or goods in the EU.

B. monitoring of behaviour

Companies that use tracking cookies and/or apps to track usage and behaviour of clients, will fall under the scope of the GDPR, when the information they collect may be used and combined in that way it could render the customer identifiable. In this case, session cookies, only used to keep service functioning would not fall under the regulation, however the persistent cookies that are used to track and remember actions of specific user would fall under.

When applying this logic to our case, with WhatsApp, we can clearly see that although the company is base in the US and in the Terms & Conditions it applies jurisdiction of US law, WhatsApp will have to oblige with the GDPR. Not only the service is available worldwide, there are translations of the app and website to most of the EU languages and the service clearly targets EU citizens. Even when talking about user behaviour, WhatsApp admits to collect and process data about user's "activity on […] Services, like service-related, diagnostic, and performance information. This includes information about your activity…" So we can establish that even the ground behaviour monitoring would apply. Facebook has EU subsidiary in Ireland and will be subject to the GDPR.

[65] Court decision, 1.10.2015, Weltimmo, C-230/14, ECLI:EU:C:2015:639

4.1.2. Privacy Shield

When it comes to transfer of personal data to the US, there is problem, as according to the adequacy decision adopted by the European Commission, that establishes what non-EU country ensures an adequate level of protection of personal data by the means of its domestic law and international commitments, US does not provide adequate protection for data transferred. Before Privacy Shield, Safe Harbour framework was in place, but it was rendered to be in conflict with EU data protection, as explained further in the work. So European Commission and the U.S. Department of Commerce reached on 2 February 2016 agreement on a new framework for transfer of personal data for commercial purposes: the EU-U.S. Privacy Shield.[66] The core of the Privacy Shield is Annex II to the above-mentioned Commission Decision. Annex II contains the full text of the Privacy Shield principles, which has to be abide by US processor of personal data that is registered in the Privacy Shield list. The Privacy Shield framework is built in essentially the same way that Safe Harbour system worked. However, in addition, the Privacy Shield also has a number of elements that should ensure real protection of personal data and the enforcement of data subjects rights. These include:

- the commitment of the US Department of Commerce to transparently administer a website with a list of organizations involved in the Privacy Shields. Carry out periodical checking that the organization meets its privacy compliance obligations, including the check of company's published privacy policy. That Privacy Shield certification will be renewed annually, and if company fails to do so, it will be removed from the list managed by the US Department of Commerce.
- An annual joint audit of the Privacy Shield, with the participation of the European Commission, the US Federal Department of Commerce and the US Federal Trade Commission.
- Explicit responsibility of the organization for the transfer of personal data to 3rd parties, while these 3rd parties must provide the same level of protection of personal data.
- The process of resolving complaints of data subjects in arbitration proceedings, with three arbitrators chosen from the Arbitration Panel (appendix 1 of Annex II).
- Independent Ombudsperson mechanism, for handling complaints of EU data subjects, about the processing done by US intelligence services (Annex III).

[66] the EU-U.S. Privacy Shield (IP/16/216)

- Safeguards and transparency obligations of U.S. government, limiting access to data of EU citizens.

4.1.3. Schrems cases

Safe Harbor framework was in place before Privacy Shield and had the same job, to facilitate the data transfer to the US. However, it did not survive the court case[67]. Maximillian Schrems, Austrian citizen, filed a complaint by Irish Data Protection Commissioner (further only Commissioner), asking the Commissioner to prohibit transfer of his personal data to the US. Schrems claimed that, Snowden's revelations demonstrated that the US did not offer adequate protection to personal data, mainly not protecting them from NSA surveillance activities. The Commissioner refused to investigate the complaint, as the Safe Harbor indicated that the US provided adequate privacy protection. Schrems continued and challenged the decision by Ireland's High Court, which noted that several US federal agencies carried out widespread in a manner probably with contrary to Irish privacy laws, and recognized that Schrems was challenging the legality of the Safe Harbor framework. ECJ was asked to determine whether the Commissioner could investigate a claim that a US's data protection laws were inadequate when presented with evidence supporting that theory, even if there already was a Safe Harbor framework. ECJ noted that the Safe Harbor could be held invalid only by ECJ, which pursued to investigate the framework further. ECJ found out that Safe Harbor framework did not adequately protect personal data from the US government interference, "founded on national security and public interest requirements." ECJ further stated that the EU data protection law only permits access to personal data only when strictly necessary, while US law allows for access to personal data on a more generalized basis, the ECJ in the end found that Safe Harbor failed to comply with the Directive's requirements and therefore was invalid. The main grounds for this ruling by ECJ was that US legislation was permitting US authorities to have generalized access to electronic communications, which constitutes violation of the Charter of Fundamental Freedoms of the European Union and also the fact that US failed provide judicially enforced rights of access to personal data, does not respect the right for effective judicial protection of data subject's rights.

After this decision, the case returned to Ireland's High Court, where Schrems updated his petition and on the April 12th 2018, High Court again referred to ECJ with new set of questions, where

[67] Court decision, 6.10.2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

Privacy Shield framework is being questioned, under similar grounds as Safe Harbor was questioned, it will be interesting to see the outcome.

4.1.4. CLOUD Act and GDPR

As we have introduced the framework of the privacy in the EU, now it's time to tackle individual questions that need to be answered prior to CLOUD Act being able to work under EU privacy legislations.

A. CLOUD Act request and data transfer

This is one of the biggest questions arising from the CLOUD Act, how to transfer the data to US and being compliant with the GDPR? The position of the WhatsApp and Facebook Messenger, here is the same, they both are data processors for their users, who are data controllers as they decide what to do, apps only carry out the commands. In this case, as both WhatsApp and Facebook Messenger are owned by Facebook, we can talk about Facebook only. With this new rules, company is set to be in the middle of two different legal obligations. Let's say the company stores messages of a person A, who is US citizen, on Irish servers. US issues warrant to get the data and Facebook has obligation to provide data, now with the CLOUD Act in place. However, the GDPR does not allow to transfer data to US under this conditions, as the only solutions we could apply only first two, as the rest of the options is suitable for corporate environment, but could not be applied to the US as receiving party. However there are no binding instruments between US and EU yet, as the Executive Agreement is not place now, there seems to be no other solution thatn the classical way through the Mutual Legal Assistance Treaty.

This stance is also supported by the Article 48 of the GDPR, that instructs that "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State".

So here we can see that Facebook in this case, has no viable option under the GDPR to transfer the data. Prior to the GDPR, companies would choose the way of cooperation with authorities issuing the warrant, as it would be less dangerous. However with GDPR and new rules for the

penalties, this would be dangerous step to take, as it could lead to fine up to 4% of annual turnover, where in case of Facebook we are talking about billions of Euros. So companies would be deliberate to take any action, probably leading to quashing all warrants, resulting into long lasting legal fight at the courts.

Another thing here worth mentioning is that if the Facebook would overstep the line and decide to transfer data to US authorities and this step would be later found to be against EU legislation, it would also change the position of Facebook from data processor to data controller. This was first decided during Society for Worldwide Interbank Financial Telecommunication (further only SWIFT) case.

Company SWIFT provides financial services with goal to facilitate international money transfer. The company kept data about the transfers on own servers, were they have been mirroring data on the server in both the EU and the US. Following the attacks in September 2001, the US Treasury Department issued a regulation requiring SWIFT to allow the Treasury Department access to reports and information stored on servers in the US. SWIFT has granted the US Treasury Department the access, however, SWIFT is a Belgian-based company subject to Belgian and European law. Working Party 29 concluded in its opinion, that the company's decision to grant access to data to the US Treasury Department did not only breach it's [SWIFT's] obligations under Directive 95/46/EC, but by cooperating with the US Treasury Department, SWIFT has made autonomous decision, without prior consultation with the banking institutions for which it processed the data, thus the company became data controller[68].

As illustrated on this example, there are still many question that yet has to be answered. The notion of the CLOUD Act implies that the intent is to answer similar question trough the Executive Agreements, where it would involve safeguards and framework specifically addressing this concerns, as it would allow to reflect the stance of the EU and Article 48 of the GDPR. So even the CLOUD Act applies, the Mutual Legal Assistance Treaty still seems to be the only viable option.

[68] Article 29 Data protection Working Party. (2010). *Opinion 1/2010 on the concepts of "controller" and "processor"*. Article 29 Data protection Working Party. Accessible: http://www.pdpjournals.com/docs/88016.pdf, 19 March 2018. p 9

B. Lack of privacy safe guards of the CLOUD Act

In Section 3(a)(1) the CLOUD Act amends the Stored Communications Act, so it will require the service providers to "preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States." Providers could move to quash the proceeding, in the case that the target is not a US person and compliance would be in conflict with the law of the country where the data is being stored. If the proceeding are move to quash, court would have to conduct a comity analysis and, consider the accessing the data via other means (like Mutual Legal Assistance Treaty), the interest of the US government in the data, and the interests of the foreign government and it's legislation.

The CLOUD Act would also permit access to records stored in the U.S. that pertain to foreign citizens, including foreign citizens here in the U.S. illegally, to foreign governments on the ground of the Executive Agreements. It would also allow foreign governments to obtain wiretap, trap and trace, and pen register orders in the same manner as U.S. law enforcement, some of the data could be even obtained without the warrant requirements. All Executive Agreements with qualifying foreign governments would be effective 90 days after notice to Congress if no joint resolution of disapproval is enacted and would have to be renewed every five years.

However foreign government orders would be limited to "obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism," must have "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation," and must be subject to judicial review. As seen, this brings even more questions, with some institutes and procedures that are not common or even to be seen in the EU criminal procedure.

The CLOUD Act, compared to new E-evidence Regulation proposal, does not limit to only citizens of the US, which could be seen discriminatory application to foreign citizens living in the US, especially given that the points from the Schrems case are still valid. When it comes to accessing the content of any stored emails, texts or online chats, US government is by law not required to obtain warrant if the data is older than 180 days old, as the as is currently written in the Stored

Communications Act[69]. However after the Warshak[70] court case, in which the 6th Circuit held that this course of action was unconstitutional to the extent, that it allowed production of any communication content, regardless of the storage time, so as reaction the Justice Department adopted a policy to always use warrants when seeking the content of communications[71]. The CLOUD Act is no further providing any safeguards in regard to this situation, to some extent it is even worsening the situation, as under the Executive Agreements, the foreign governments are brought in.

Even thought US still have volatile procedures that offer less safeguards in criminal procedure, which is one of the reasons why Schrems case is still on, as the main argument there was that US legal system lack guarantees without offering sufficient controls.

The CLOUD Act in the Section 4 amends US State Code § 2702, so it allows foreign governments, with valid Executive Agreement, to request service provider to disclose content of communication and customer record, without any need for warrant. The US State Code was amended by the CLOUD Act that § 2702 (b) (9) states that "A provider […] may divulge the contents of a communication […] to a foreign government pursuant to order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523" and that § 2702 (c) (7) so "A provider […] may divulge a record or other information pertaining to a subscriber to or customer of such service […] to a foreign government pursuant to order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523."

This presents serious impact for rights of EU citizens, as not only the CLOUD Act allows US government to data and content of communication of EU citizens, it allows the same to be done by EU authorities, using Executive Agreements, where this proceeding under CLOUD Act lack basic requirements of criminal procedure set in EU, it constitutes huge and shocking question mark, that would hopefully be addressed by the EU.

[69] 18 U.S.C. § 2703(a)
[70] UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT, Nos. 08-3997/4085/4087/4212/4429; 09-3176, *United States v. Warshak, et al*
[71] H. Rept. 114-528 - EMAIL PRIVACY ACT

Applied this on the example of Facebook Messenger, it could easily happen that the data and communication of EU citizens would be accessed by both US and their own government, without them having a say, where their own government could even obtain the communication without warrant. The situation with the WhatsApp is bit different however, as the service is end-to-end encrypted, the company can not provide any government with communication content, as it has no access to it, even thought there have been discussions that company would make backdoor allowing access to government upon request, the company has not implemented this solution.

However, as it is, the CLOUD Act has given the power to protect the interest of subject into the hands of companies, as they are the one eligible for the motion to quash, as described therebefore. To some extent it is understandable that the subjects themselves are not brought in, as it may be against the interest of the criminal procedure, however the lack of safeguards provided by the legislation is shocking, given the fact that it opens the door for another countries to scope on own citizens.

4.2. Jurisdiction implication

The default mechanism for sharing evidence between countries is a bilateral Treaty on Mutual Legal Assistance, as previously explained. However this process become too slow in current world where new technologies allow to store data and communication in completely different countries. As technologies become part of every day life, they also become part of crime. As result governments around the globe started to seek the ways how to effectively access data stored outside their territorial jurisdictions in the course of law enforcement investigations[72].

This desire is nothing new and countries in the EU has found way how to work around territorial jurisdictions to some extent. Many countries have established universal jurisdiction over content of Facebook messages, or other similar services. For example Denmark has established universal jurisdiction over reading Facebook and Facebok Messenger's profiles in the case,[73] where the police was in possession of the username and password. Although noted that "In the case at hand,

[72] Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests Before the Committee on the Judiciary U.S. House of Representatives, statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916300630 19 April 2018

[73] Højesteret (Supreme Court), U 2012.2614 H

the ‘computer’, meaning the content of the Facebook and Messenger profiles, were undoubtedly physically located on a server in California, USA. Under normal circumstances this would mean that the Danish police should ask for the assistance from the American police authorities to carry out a search of the content. But in this case, the Danish police were able to carry out the search from their own office in Denmark since they were in possession of the necessary username and password and because the content of the computer in question was linked to the internet, which meant it was accessible from the entire world”. Similar approach is for example taken by Estonia[74].

Both CLOUD Act and E-evidence Regulation has built on this and establishing it into the legislation. CLOUD Act taking step further by extending the jurisdiction even on non-residents, where under section 3 says that “[provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.”

The E-evidence Regulation has not taken such steep action, where in Article 3(1) it says that the Regulation applies to the “provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required, the use of such services and the protection of information related to the terminal equipment of end-users located in the Union.”

Both legislations reflect the need to have in place motion to resolve possible conflict with law, as addressees of the order in EU and request or warrant in the US have options how to review the proceedings and potentially turn then or judicial review. However unless the Executive order under CLOUC Act is in place, there are available only common law comity principles, that offer less options to protect the interests.

Not only the CLOUD Act expressly expands the ability of the US government to access data stored outside the United States, it [CLOUD Act] also addresses a reciprocal issue: limitations on foreign governments’ ability to obtain data in the US. As internet based communications have become par of our daily life, evidence in criminal proceedings is frequently located on servers located outside

[74] E. Laurits. (2016). Criminal procedure and digital evidence in Estonia. - *Digital Evidence and Electronic Signature Law Review*, volume 13, p. 113-120.

the territorial jurisdiction of the nation where the crime was committed[75]. Because technology companies headquartered are mainly located in the California, US the majority of the world's electronic communications is stored on servers located in the US, which results in foreign governments frequently seeking data held by US companies. At the same time, US legislation was prohibiting service providers from directly disclosing the data directly, unless there was a statutory exception or a warrant from a federal court. With ECPA acting as a "blocking statute" that prevents foreign governments from directly acquiring certain third-party data stored by private entities in the United States, foreign nations have sought the U.S. government's assistance in obtaining warrants that authorize disclosure. Prior to the CLOUD Act, there were two common international legal processes for obtaining a warrant in the United States: letters rogatory requests and Mutual Legal Assistance Treaties.

Letter Rogatory are requests from courts in one country to the courts of another country requesting the performance of an act[76]. They are seen as the least efficient way of dealing with things. Mutual Legal Assistance Treaties, as described here before are bi-, or multi- lateral treaties providing regulation for processes of cross-border evidence sharing between governments in criminal cases[77].

The process however become subject of criticism in recent years due to the length of response time under such agreements, also the fact that US does not have any Mutual Legal Assistance Treaty with more than half the nations in the world does not help the cause. That's why the CLOUD Act creates a system of international data sharing arrangements: the possibility of international agreements that remove legal restrictions of US law and allow companies to respond directly to certain foreign nations to orders issued by foreign nations.

However this solution is suspicible to all problems discussed in previous parts of this work. The notion of the CLOUD Act makes the feeling that the goal is to overcome all possible obstacle and objections countries may have using the framework of Executive Agreements, that could,

[75] Daskal, J. (2015). The Un-territoriality of Data. – *Yale Law Journal*, Volume 125, Number 2, p.326-398. New Haven: The Yale Law Journal.
[76] Jones, H. (1953). International Judicial Assistance: Procedural Chaos and a Program for reform. The Yale Law Journal, Volume 62, Number4, p. 515-562. p 519
[77] Moskowitz, Y.L. (2016). MLATS and the Trusted Nation Club: The Proper Cost of Membership. - *Yale Journal of International Law*, Vol. 41: 2. Accessible: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2016/09/moskowitz-macro-finished-1-1s9vmcy.pdf, 10 April 2018, p. 1

hopefully regulate certain topic in more detail, so we could overstep the clear differences between EU and US legislations.

SUMMARY

Technologies are integral part of our lives now, where Cloud Computing played crucial part in this change, as it presents technological solution allowing companies to offer scalable, flexible services to the customers thought the internet. The only thing you need to experience it is device with connection to the internet and you can enjoy, the rest happens on the infrastructure of the service provider, somewhere there over in the "Clouds". This allows you to enjoy many different types of the service or always have access to your data, no matter where you are, only if you have internet connection.

Even thought the term Cloud Computing is in mind of the most people connected to the company Google and it's Gmail or Google Drive service, or Amazon and Microsoft, thanks to their marketing, most of the services now are offered trough the means of the Cloud Computing. This happened also in the field of communication, where we have seen the emergence of instant messaging and calls over the internet. These services are specific category of over-the-top telecommunications, as contrary to classical telecommunication companies, they offer services over the existing infrastructure (internet in this case), build an maintained by their competition mostly. Although the Skype could be named as the pioneer of this field of over-the-top service, now the segment is ruled by Facebook with WhatsApp and Facebook Messenger, which are used to conduct the vast majority of the instant messages and calls. Even thought both services are owned by Facebook, the difference between them is quite big. WhatsApp offers end-to-end encrypted messages and calls, that are almost impossible to access but by recipients and senders. Facebook Messenger on the other hand offers messages that are not encrypted, but on the other hand are accessible on all devices of the users, but at cost of security. Both of these services are great example for analysis of the new legislature both in the US and EU, as they not only process and store data about the user, they also store the communications of the user, so we can use them as example for the full extend of new legislature.

This new technologies and trends lead into creation of the computing architecture that allows companies to store data at the geographic location most convenient for given process ie. Nerest possible to the user and so. As a result of Cloud Computing becoming part of everyday activities,

also crimes and the electronic data connected to crime, begin to be more often stored in completely different country as the criminal activity carried out. In the face of these changes caused by mass expansion of the Cloud Computing, the governments and law enforcement authorities all around the world started to search for new ways how to access data about and content of electronic communications, like instant messages, emails and social media posts, that are thanks to the Cloud Computing stored on servers located outside of the country's jurisdiction. This has caused problems for governments all around the globe, including the USand EU, where they have to seek data stored outside their territorial jurisdictions in the course of criminal investigations.

Despite this anxieties over surveillance, countries are also facing the problems in the field of national security and crime prevention, as with these global services provided by Cloud, they are losing the control over the data and it's proving to be difficult, sometimes even impossible, to effectively use data stored on Cloud outside of country as part of criminal proceedings. That is why US and EU come up with new legislative solutions that will allow respective countries to access data outside of their borders and could lead to international discussions about further regulation of said process.

EU has presented new proposal E-evidence framework, consisting of E-evidence Regulation and Directive. The good thing is that the framework clears the vacuum surrounding the regulation of the OTT services like WhatsApp of Facebook Messenger, clearly involving them in the definitions. Framework also creates European Production Order that will allow a judicial authority in Member State to obtain electronic evidence, like instant messages or emails, or users data like phone number and other identifiers, directly from a service provider. Also it creates European Preservation Order, that enables authority of one Member State to request that a service provider in another Member State, to preserves specific data as part of further request to produce this data through European Production Order or by mutual legal assistance.

However the service provider, is during the process, presented only with notice, that does not shows the grounds for the decision to issue the order, thus limiting his power to protect interests of it's clients. This framework also provides quite strict and short respond times for service providers, who will be obliged to respond within 10 days, and within 6 hours in cases of emergency, making them even less fit to protect interests of it's users, as such response times could cause them to be overwhelmed quite easily.

In the US, the changes I done thought CLOUD Act, which will apply to all companies based in the US, with no difference done between US citizens and aliens. The CLOUD Act acts as amendment of the Stored Communications Act, widening the applicability of it's instruments "overseas", outside of the US. Not only this is highly subspecies, as US legislation is deemed to be lacking some safeguards and review options according to ECJ, as mentioned in the Schrems decision[78], the CLOUD Act also allows governments of other countries to use these institutes. One of the biggest concerns is that CLOUD Act amended the Stored Communications Act in the way that companies may voluntarily disclose user data and content of communication to the foreign governments, in the case they have Executive Agreement with the US government. The fact that there is a chance that your government could access your data in the US without warrant, just by request is highly suspicious and calls for intranational concern, at least. Appling this to OTT service providers, WhatsApp comes over bit better, thanks to end-to-end encryption it is not possible for the company to surrender users' communication. However, Facebook Messenger is hit by these provisions in the open.

Of course, the CLOUD Act offers remedies, but again they will be carried out by the companies, however the mechanism gives them more power than the EU framework. Under the CLOUD Act A provider may quash the request or warrant if reasonably believes that the customer is not a US person and does not reside in the US, if the disclosure would create a material risk that the provider would violate the laws of the foreign government, or the challenge would serve the interests of justice. Starting the move for quash would lead to judicial review of the request.

While the CLOUD Act is so far likely to only define US criminal procedure rules, its broader impact on the international crime procedure regime is less certain. As the internet continues to be more globalized, governments worldwide will continue to seek access to data stored on servers outside their territorial jurisdictions. Even though the major technology companies handling the biggest share of world's data are located in the US, the US citizens presents only around 10% of the estimated 3 billion internet users around the globe. This demographics potentially could lead many nations starting negotiations about Executive Agreements, potentially enabling the biggest thread of the CLOUD Act. It is true that it would provide faster access to data held by providers based in the US, but the lack of safeguards and the possibility of the governments accessing data

[78] Court decision, 6.10.2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

without warrant is scary. The good think is this is not possible unless the Executive Agreements are made, so for now, we have to wait and hope that EU will be able to negotiate Executive Agreement that would provide safeguards and regime that the CLOUD Act is now missing.

LIST OF REFFERENCES

A. Scientific books:

1. Carr, N. (2008). The Big Switch: Rewiring the World, From Edison to Google. 1st ed. New York: W. W. Norton & Company, Inc.
2. Encyclopedia of Cloud Computing. (2016). /Eds S. Murugesan,I. Bojanova, I. UK: John Wiley & Sons, Ltd.
3. Maher, T., Kumaraswamy, S., Latif, S. (2009). Cloud Security and Privacy. 1st ed. Sebastopol: O'Reilly Media, Inc.

B. Scientific articles

1. Aldossary, S., Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. - *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, p. 485-498. Bradford**:** The Science and Information (SAI) Organization. Accessible: http://thesai.org/Downloads/Volume7No4/Paper_64-data_Security_Privacy_Availability_and_Integrity.pdf, 19 march 2018
2. Bisong A., Rahman S. M. (2011). An overview of the security concerns in enterprise cloud computing - *International Journal of Network Security & Its Applications*, Vol.3, No.1, p 30-45. Chennai: AIRCC Publishing Corporation.
3. Botta, A., *et al*. (2016). Integration of Cloud computing and Internet of Things: A survey. - *Future Generation Computer Systems*, Volume 56, p 684–700. Amsterdam: Elsevier Ltd. Accessible:https://www.sciencedirect.com/science/article/pii/S0167739X15003015, 19 March 2018.
4. Chander, A., Uyen P. Le. (2014). Breaking the Web: Data Localization vs. the Global Internet. *Emory Law Journal*, Forthcoming; UC Davis Legal Studies Research Paper No. 378. Available at SSRN: https://ssrn.com/abstract=2407858, 11 March 2018.
5. Daskal, J. (2015). The Un-territoriality of Data. – *Yale Law Journal*, Volume 125, Number 2, p.326-398. New Haven: The Yale Law Journal.
6. Determann, L. (2013). Data Privacy in the Cloud – myths and facts - *Privacy Laws & Business Internationl Report*, Issue 121, p 17-21. Middlesex: Privacy Laws & Business
7. E. Laurits. (2016). Criminal procedure and digital evidence in Estonia. - *Digital Evidence and Electronic Signature Law Review*, volume 13, p. 113-120.
8. Hashem, I. A. T., Yaqoob I., Anuar, N.B., Mokhtar S., Gani, A., Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. - *Information Systems*, Vol. 47, p. 98-115. John Wiley & Sons. Accessible: http://www.sciencedirect.com/science/article/pii/S0306437914001288, 10 March 2018.
9. Hon, W. K., Hörle, J., Millard, Ch. (2012). Data Protection Jurisdiction and Cloud Computing: When are Cloud Users and Providers Subject to EU Data Protection

Law? The Cloud of Unknowing, Part 3. - *International Review of Law, Computers & Technology*, Vol. 26, No. 2-3, p. 129-164. Abingdon: Taylor & Francis (Routledge). Accessible: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240,18 March 2018

10. Hon, W.K., Millard Ch., Walden I. (2012). Negotiating Cloud contracts: Looking at Clouds from both sides now – *Stanford technology law review*, Vol.16, Number 1, p 81 – 131. Stanford: Stanford University. Accessible: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374, 18 March 2018
11. Jones, H. (1953). International Judicial Assistance: Procedural Chaos and a Program for reform. The Yale Law Journal, Volume 62, Number4, p. 515-562. p 519
12. Kazim, M., Zhu S.Y. (2015). A survey on top security threats in cloud computing - *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 3, p 109-113. Accessible: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.6079&rep=rep1&type=pdf, 19 Mar 2018
13. Kerber, W. (2017). Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int)*, 7/2016, Munich: C.H.BECK, p. 639 - 647, ISSN 0435-8600. Available: https://ssrn.com/abstract=2770479, 19 March 2018.
14. Khan, M. A. (2016). A survey of security issues for cloud computing. - *Journal of Network and Computer Applications*, Vol. 71, p. 11-29. West Yorkshire: The Science and Information (SAI) Organization. Accessible: http://www.sciencedirect.com/science/article/pii/S1084804516301060?via%3Dihub, 10 March 2018
15. Liu, H. *et al*. (2017). Identity-based provable data possession revisited: Security analysis and generic construction. – *Journal of Computer Standards & Interfaces*, volume 54, p 10 – 19. Amsterdam: Elsevier Ltd. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916301015, 18 Mar 2018.
16. Moskowitz, Y.L. (2016). MLATS and the Trusted Nation Club: The Proper Cost of Membership. - *Yale Journal of International Law*, Vol. 41: 2. Accessible: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2016/09/moskowitz-macro-finished-1-1s9vmcy.pdf, 10 April 2018
17. Parekh, D. H., Daen, R. S. (2013). An Analysis of Security Challenges in Cloud Computing - *International Journal of Advanced Computer Science and Applications*, Vol. 4, No.1, p. 38-43. Bradford**:** The Science and Information (SAI) Organization. Accessible: https://thesai.org/Downloads/Volume4No1/Paper_6-An_Analysis_of_Security_Challenges_in_Cloud_Computing.pdf, 19 March 2018
18. Romanosky, S., Hoffman, D. A., Acquisti, A. (2013). Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, Volume 11, Issue 1, p 74 – 104. UK: John Wiley & Sons, Ltd. Available: https://ssrn.com/abstract=1986461, 19 March 2018.
19. Samarati, P., Capitani di Vimercati, S. (2016). Cloud Security. - *Encyclopedia of Cloud Computing* (eds.) Murugesan, S., Bojanova, I. Chichester, UK: John Wiley & Sons, Ltd, 205 - 219. Accessible: http://spdp.di.unimi.it/papers/sd-cloud_security.pdf, 10 March 2018.

20. Shaqrah, A., Cloud CRM: State-of-the-Art and Security Challenges - *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 4, p. 39-43. Bradford**:** The Science and Information (SAI) Organization. Accessible: http://thesai.org/Downloads/Volume7No4/Paper_5-Cloud_CRM_State_of_the_Art_and_Security_Challenges.pdf, 19 March 2018.
21. Soghoian, C. (2009). Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. - *Journal on Telecommunications and High Technology Law*, vol. 8, p. 359 - 424. Colorado: University of Colorado. Available: https://ssrn.com/abstract=1421553, 19 March 2018.
22. Sun Y., *et al*. (2014). Data Security and Privacy in Cloud Computing. - *International Journal of Distributed Sensor Networks*. Volume: 10, Issue: 7. Thousand Oaks: SAGE Publications Ltd Accessible: https://doi.org/10.1155/2014/190903, 19 March 2018.
23. Tchernykha, A., Schwiegelsohnb, U., Talbic, E., Babenko, M. (2016). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. - *Journal of Computational Science*, In press. Amsterdam: Elsevier Ltd. Accessible: http://www.sciencedirect.com/science/article/pii/S1877750316303878, 19 March 2018
24. Vaquero, L. M, Rodino-Merino, L., Caceres, J., and Lindner, M. (2009) A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review*. Volume 39, Number 1, p. 50–55. New York: ACM
25. Woods, A.K. (2016). Against Data Exceptionalism. - *Stanford Law Review*, Volume 68, p 728-788. Stanford :School of Law, Stanford University
26. Xue, L. *et al*. (2017). Provable data transfer from provable data possession and deletion in cloud storage. - *Computer Standards & Interfaces*, Volume 54, p 46 – 54. Amsterdam: Elsevier Ltd. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916300630, 19 March 2018.
27. Zhang, Q., Cheng, L. & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. - *Journal of Internet Services and Applications*, Volume 1, Issue 1, p. 7–18. London: Springer London
28. Zhang, Y, *et al*. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. - *Information Sciences*, Volume 379, Pages 42-61. Elsevier. Accessible: http://www.sciencedirect.com/science/article/pii/S002002551630250X, 19 March 2018

C. EU legislation:

1. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, L 77/20
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On the protection of individuals with regard to the processing of personal data and on the free movement of such data
3. Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services
4. Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177/6

5. Regulatio (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
6. the EU-U.S. Privacy Shield (IP/16/216)

D. Other countries legislation:

1. United States Code (U.S.C.)
2. CLOUD Act - H.R.4943
3. Stored Communications Act (18 U.S.C. Chapter 121 §§ 2701–2712)
4. H. Rept. 114-528 - EMAIL PRIVACY ACT

E. Court decisions:

1. Court decision, 30.4.2014, Google Spain, C-475/12, ECLI:EU:C:2014:285, para. 43
2. Court decision, 6.10.2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650
3. Court decision, 13.5.2014, Google Spain, C-131/12, ECLI:EU:C:2014:317
4. Court decision, 1.10.2015, Weltimmo, C-230/14, ECLI:EU:C:2015:639
5. Højesteret (Supreme Court), U 2012.2614 H
6. SUPREME COURT OF THE UNITED STATES, 584 U. S. ____ (2018), 17.4.2018. *United States v. Microsoft Inc.*
7. UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT, Nos. 08-3997/4085/4087/4212/4429; 09-3176, *United States v. Warshak, et al*

F. Other resources:

1. Apple Inc. (2014). *Apple Media Advisory: Update to Celebrity Photo Investigation*. Cupertino, CA: Apple Inc. Accessible: http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html, 18 March 2018
2. Article 29 Data protection Working Party. (2010). *Opinion 1/2010 on the concepts of "controller" and "processor".* Article 29 Data protection Working Party. Accessible: http://www.pdpjournals.com/docs/88016.pdf, 19 March 2018
3. *Cloud Predictions 2017*. (2017). Oracle. Available: http://www.oracle.com/us/solutions/cloud/top-10-predictions-cloud-3436083.pdf , 11 March 2018.
4. Commission nationale de l'informatique et des libertés. (2012). Google's new privacy policy: incomplete informationand uncontrolled combination of data across services. Paris: Commission nationale de l'informatique et des libertés, Accessible: http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/, 15 March 2018
5. Curran, K. (2012). *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments.* US: IGI Global.
6. European Union Agency For Network And Information Security. (2017). *Security aspects of virtualization* .Accessible: https://www.enisa.europa.eu/publications/security-aspects-of-virtualization, 11 March 2018
7. European Union Agency For Network And Information Security. (2017). *Security aspects of virtualization.* Accessible:

https://www.enisa.europa.eu/publications/security-aspects-of-virtualization, 11 March 2018.

8. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. (2012). Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency. Access: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security, 19 March 2018
9. Facebook Ireland Limited. (2018). Terms of Service. California: Facebook Inc. Accessible: https://www.facebook.com/legal/terms/update, 14 April 2018 Facebook Ireland Limited. (2018). Data Policy. California: Facebook Inc. Accessible: https://www.facebook.com/about/privacy/other, 14 April 2018
10. Facebook Inc. (2018). FACEBOOK INC. AND THE EU-U.S. and SWISS-U.S. PRIVACY SHIELD. California: Facebook Inc. Accessible: https://www.facebook.com/about/privacyshield, 14 April 2018
11. Facebook Inc. (2018). Information for Law Enforcement Authorities. California: Facebook Inc. Accessible: https://www.facebook.com/safety/groups/law/guidelines/, 14 April 2018
12. WhatsApp Inc. (2018). WhatsApp Legal Info. California: WhatsApp Inc. Accessible: https://www.whatsapp.com/legal?eea=0#terms-of-service, 14 April 2018
13. GOOGLE Inc. (2009). *Google Apps - Gmail: Incident Report February 24, 2009*. Google Inc. Accessible: http://static.googleusercontent.com/media/www.google.com/sk//appsstatus/ir/1nsexcr2jnrj1d6.pdf, 19 March 2018
14. Marchini, R. (2010). *Cloud Computing: A Practical Introduction to the Legal Issues*. London: British Standards Institution
15. National Institute of Standards and Technology. (2011). *The NIST Definition of Cloud Computing*. Special publication 800-145. Accessible: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 11 March 2018.
16. Huges, J.T., Saverice-Rohan, A. (2017). IAPP-EY Annual Privacy Governance Report 2017. IAPP-EY.
17. Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests Before the Committee on the Judiciary U.S. House of Representatives, statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp. Accessible: https://www.sciencedirect.com/science/article/pii/S0920548916300630 19 April 2018
18. EuroISPA. (2017). E-Evidence Proposal: EuroISPA Criticises the Privatisation of Law Enforcement. Brussels: EuroISPA. Accessible: http://www.euroispa.org/e-evidence-proposal-euroispa-criticises-privatisation-law-enforcement/, 18 April 2018