US GOVERNMENTAL ACCESS TO DATA IN THE CLOUDS THROUGH THE USA PATRIOT ACT

Law and Technology, Master Thesis

Teresa del Rocío Espinosa Vega

ANR 125095

Supervised by Prof. dr. Ronald Leenes

Tilburg, the Netherlands

July, 2012

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CC	Cloud Computing
ECPA	Electronic Communications Privacy Act
EU	European Union
FBI	Federal Bureau of Investigations
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
IaaS	Infrastructure as a Service
ISP	Internet Service Provider
IT	Information Technology
MLA	Mutual Legal Agreements
NIST	National Institute of Standards and Technology
NSL	National Security Letters
OGC	Office of General Counsel
PaaS	Platform as a Service
RGPA	Right to Financial Privacy Act
SaaS	Software as a Service
SLA	Service Level Agreement

US / USA	United States of America
USA PATRIOT Act / PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
WP 29	Working Party 29

Introduction

Years have passed since the attacks of September 9th were perpetuated on US soil but, nonetheless, it is an irrefutable fact that their effects continue to have a great impact around the world, and one that not only can be seen at the airports but that with due analysis it is apparent even on issues that, at first glance, would seem impossible to think of them as related, as it is the case with Cloud Computing.

The USA PATRIOT Act was enacted as a result of the mentioned attacks and it contains amendments to several statutes; some of which grant authorities more powers for their investigations, in order for them to prevent terrorism and other threats to national security.

Among some of the most relevant changes this Act brought, are the possibility of issuing documents with requests for disclosure of data under control of providers of different services (electronic communications, remote computing systems, telephony, etc.). The focus of this dissertation will be, precisely, on issues related to this type of disclosures of data.

Cloud computing is a phenomenon that has transformed information technology services and that will gain importance in the coming years. Subject to be explained in greater detail in the following pages, it should be noted now that cloud computing "refers to a technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers."[1]

Despite its multiple benefits, cloud computing also comes with several risks, some concerning privacy and data protection; issues that need to be taken

[1] Dan Svantesson, Roger. *"Privacy and consumer risks in cloud computing".* The computer law and security report vol. 26 (2010) nr. 4, pp.391-397. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364910000828> February 7, 2012.

into account seriously because of the amount of users' personal data that can be found in the clouds.

The combination of the legal instruments implemented in the PATRIOT Act and the amount of data that is under control of Cloud providers, is what has resulted in the problem to be studied throughout this paper.

Even though there are Privacy and Data Protection Regulations in some countries, and especially in the European Union, when it comes to enforcement of the USA Patriot Act, cloud providers disregard anything else and seem to focus on compliance with US laws; violating the privacy expectations of consumers.

This problem has acquired more relevancy for two reasons; one, that the US is the country that has under its jurisdiction the most important cloud providers (Google, Microsoft, Rackspace, Amazon…), which happen to have a significant presence around the globe and the biggest databases[2]; and two, the fact that the American government is actually making use of all the instruments for governmental access, to obtain data from the worldwide population.

Even when the right of privacy is reason enough for consumers to want their data shielded off from US governmental access; when the only connection a consumer has with the US is the cloud provider, this fact is yet more important because they are not subject to the laws of said country and have no interests there. States may also want to avoid access to data of their citizens by other governments for sovereignty reasons, and because information of their nationals could provide the US with knowledge of internal matters.

For all of the above, this dissertation will address the issue of governmental access to data stored and transmitted in the clouds, in order to analyze if it is

[2] Bort, Julie. *"The ten most important companies in cloud computing."* Business Insider, 2012. Available at: < http://www.businessinsider.com/the-10-most-important-companies-in-cloud-computing-2012-4?op=1> Consulted on May 24, 2012.

possible for providers to avoid compliance with the PATRIOT Act, and if so, how could this be achieved.

Therefore, the research question to be answered is the following:

To what extent can Cloud Computing Providers guarantee data protection from US Governmental Access through the USA PATIOT Act?

In order to find the answer, the methodology followed through this dissertation was “literature study”. The text is divided into five chapters. In the first one, the basic concepts of cloud computing are explained, to provide a general idea of its functioning and other implications.

The second chapter deals with the USA PATRIOT Act; with its background and its more controversial provisions. Later, on chapter three, European regulation concerning privacy and data protection are explained to compare how the laws of the US and the European Union are in conflict and place providers into a difficult situation when they have to comply with both regulatory systems.

In the fourth chapter the issue of jurisdiction is explained and particularly regarding jurisdiction in the clouds. Here, six possible scenarios are studied to clarify in which situations the PATRIOT Act would apply and in which ones it would not.

Finally, after analyzing all of the above, in the last chapter some possible solutions to the problem or recommendations are presented, for consumers who would find problematic the idea of a foreign government accessing their data without their consent, and for American cloud providers that are aware of the impact this situation could have on their business outside of the US, in order for them to ameliorate the situation and to reinforce their clients’ trust towards the cloud.

Chapter 1

Basics of Cloud Computing

1.1 Introduction

Cloud computing (CC) is a phenomenon that is changing information technology as such, because even though the ideas from which Cloud computing originates have being developed throughout the years, the way in which they are combined is somehow novel.

A lot of research is taking place regarding the topic and not only in the computational and software engineering areas, but also from a legal perspective, since due to its inherent characteristics it is very difficult to frame and regulate.

It is not clear if the said phenomenon is here to stay or how long it is likely to last, but what it is certain is that from its existence and forward, Information Technology, or technology to deal with information, will never be the same.

1.2 Definition

At some point we all have probably heard the term “cloud computing” and construed an idea of such an abstract concept based on its literacy. And this is the very core of the concept but, as cloud computing did not emerge spontaneously, nor did the word cloud, which actually came from the image that had been used in “network diagrams to depict the Internet’s underlying networking infrastructure” and it is used as a metaphor. [3]

As a consequence of all the uncertainty surrounding CC, there have been several attempts to define what it is and no real consensus on the matter. Therefore, two of the definitions I consider to be the most complete since they mention all relevant elements of CC, are presented herein.

[3] Kamal, Dahbur, et al. *“A Survey of Risks, Threats and Vulnerabilities in Cloud Computing”*. New York Institute of Technology. Mendeley. Available at:< http://www.mendeley.com/research/survey-risks-threats-vulnerabilities-cloud-computing/> Consulted on February 20, 2012.

The National Institute of Standards and Technology (NIST) of the United States published a special report destined to provide a definition that could be used for the public, in general, to understand the phenomenon discussed herein, and this definition has been well accepted in the IT community.

> "Cloud Computing is a 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. This cloud model promotes availability and is composed of five essential characteristics, three service models and four deployment models."[4]

The essential characteristics, services and models will be explained later on in this chapter.

In order to clarify the concept, another definition that seems to contain all the relevant characteristics and that is written in simpler vocabulary may be helpful.

> "It is an information technology service model where computing services (both, hardware and software) are delivered on- demand to customers over the network in a self- service fashion, independent of device and location. The resources required to provide the requisite quality- of service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction."[5]

1.3 Essential Characteristics

From the definitions provided before, the main characteristics can be deduced as follows:

- **On demand- Self Service.** Also known as pay- per- use. It means that the consumer can use different services automatically, without having to

[4] Mell, Peter; Grance, Timothy. *The NIST Definition of Cloud Computing*. January 2011. Available at: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> Consulted on February 01, 2012.
[5] Marston, Sean; et al. *Cloud Computing: The business perspective*. April 2011, Elsevier Journal, Decision Support Systems, Volume 51, Issue 1, 176- 189 pp. Available at: <http://www.sciencedirect.com/science/article/pii/S0167923610002393> Consulted on February 16, 2012.

sign a contract for each kind of service (one contract for multiple services). Besides, he will only pay for the services he uses and for the amount of each of them.[6] This is very convenient for customers that have different necessities during the year; months of a lot of movement and some others very calm.

- **Broad network access.** It has to do with the accessibility of the capacities of the network. It may be accessed always and from all kind of appropriate devices.[7]
- **Resource Pooling or Multi- tenancy.** The resources and applications of the network are shared by several customers. This is possible through a Web service, which is "a software system designed to support interoperable machine- to- machine interaction over a network".[8] Some examples of resources are: storage, processing, memory, network bandwidth and virtual machines. [9]
- **Elasticity**. "Ability to locate and release resources rapidly". Consumers can decide what resource to use, where and for how long.
- **Measured service.** The usage of resources is monitored, controlled, measured and reported.[10] This is why is possible for the consumer to pay only for what is being used.

For all of these particularities, Cloud Computing is often known as well as "utility computing" since the costumer can take advantage of all the resources or only some of them, whenever they are needed and paying only for the services that were used.

A very important thing to be noted here is that all these features are possible due to the nature of the cloud; specifically, the mobility of data and resources and lack of territorial restrictions.

[6] Cfr. Mell, Peter; Grance, Timothy. Op. cit. p. 2
[7] Ibid.
[8] Marston, Sean; et al. Op.cit. p. 178
[9] Mell, Peter; Grance, Timothy. Op. cit. p.2.
[10] Ibid. P. 2.

Going back to the part that explains the origin of the term cloud, in the diagrams where the internet is represented with a cloud because of the abstractness of the idea, we can make an analogy and see that in coining the new term “Cloud Computing”, such abstraction was intended to be passed on.

Cloud providers have servers anywhere and everywhere, normally gathered in enormous amounts in data centers; which make possible the transmission of data, resources and all kind of information between the servers, hence data centers owned by the same supplier.

At the same time, these characteristics do not only make the cloud workable, but they are also the direct cause of some of the advantages this system offers to its users, such as access to data from anywhere, low cost because of massive data storage possibilities, and use of up to date software.

1.4 Service Models

Although some authors argue that due to the dynamics of the cloud, that allow the construction of services, these should not be categorized into well- defined groups, they are normally classified into three categories or delivery models; but we should take into consideration that a combination of services can take place, and that there are other categories still to be defined.

- **Software as a Service (SaaS).** In this model the software is found on the cloud at disposal of the user who can rent the software in exchange of a subscription fee. Users avoid buying and installing the software on their systems. The application runs in the network and the rent normally includes the usage of hardware and some support. An advantage of this model is that users can have access to more and updated software. [11]

[11] Babbar, Muhammad; Chauhan, Muhammad. “*A tale of Migration to Cloud Computing for Sharing Experiences and Observations”*. ACM Press, 2011, 50-56 pp. Available at: <http://www.ics.uci.edu/~shengwl/resources/courses/inf211/Readings/07_A%20Tale%20of%20Migration%20to%20Cloud%20Computing%20for%20Sharing%20Experiences%20and%20Observations.pdf> Consulted on March 03, 2012.

- **Infrastructure as a Service (IaaS).** Consumers can access and use the infrastructure through the network. It is the capability to provision processing, storage, networks and other resources where the consumer is able to deploy and run software and operating systems.[12]

- **Platform as a Service (PaaS).** Consumers can use a development environment in which applications are executed. They may utilize all the tools provided by the cloud to create and run their own applications.[13]

Some examples of services offered by different cloud providers are shown in Figure 1.

1.5 Deployment Models

To bring to a close the explanation of the definition of Cloud Computing, here are the models in which it can be exploited.

Private Cloud. "Is a collection of computing resources, storage resources and cloud technologies owned by an organization for its private use."[14] This model is very advantageous for organizations that need to be in control of the infrastructure.

Public Cloud. The infrastructure is owned by the cloud provider but is available to third parties through the Internet. It is very useful for small or medium businesses, as well as for the public at large.

Community Cloud. In this model "the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns. It may be managed by the organizations or a third party." [15]

Hybrid Cloud. Is a combination of two or more clouds that are bound together by technology that enables data and application portability.[16]

[12] Cfr. Mell, Peter; Grance, Timothy. Op. cit. p. 3.
[13] Cfr. Ibid. P.2.
[14] Babbar, Muhammad; Chauhan, Muhammad. Op. cit. p. 51
[15] Mell, Peter; Grance, Timothy. Op. cit. p. 3

All of these models have advantages and disadvantages for consumers depending on the use they want to give them and their needs.

The following drawing illustrates in a clear manner all the services and deployment models of clouds.

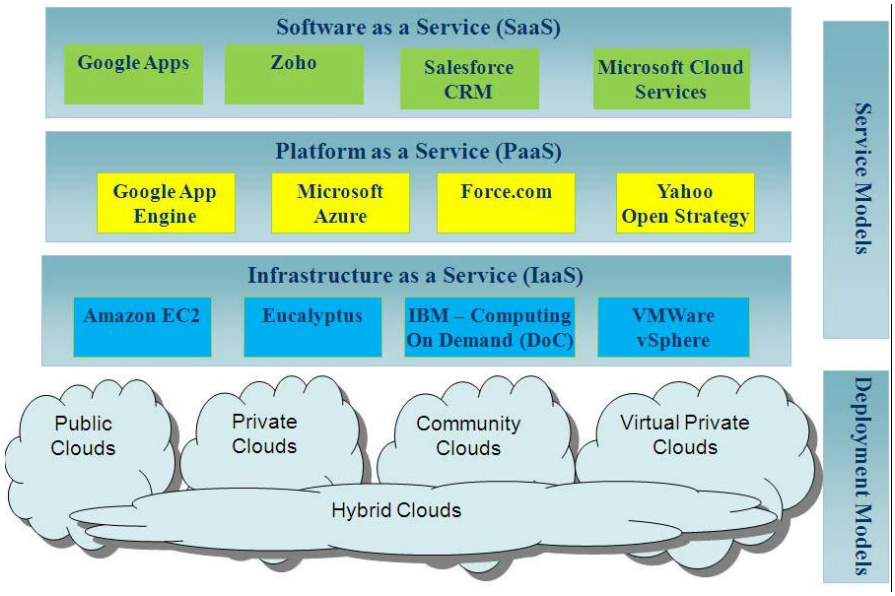

Fig. 1 Most common known service and deployment models of cloud computing[17]

1.6 Stakeholders

In order to understand better the functioning of cloud computing it is necessary to have in mind who the main stakeholders at play are; particularly since they have complex and varied roles. The three relevant stakeholders for this paper are described hereafter.

The first actors or stakeholders are **cloud consumers**. They are the ones that pay for the service (either PaaS, IaaS, SaaS or a combination), come to an understanding with the cloud provider regarding the terms of service and their

[16] Ibid. P.3.
[17] Babbar, Muhammad; Chauhan, Muhammad. Op. cit.

legal relation, and also the ones that test and manage the service. Consumers can be both, individuals or businesses and also other kind of organizations.[18][19]

For purposes of this dissertation, consumers shall be understood to be either individuals, businesses, Ministries, governmental agencies or others. This, because concerning disclosure of information to the US government by providers, there is no or very little difference between them (all consumers), since they all can be subject to application of the PATRIOT Act under particular circumstances. Nevertheless, if a difference needs to be clear, then it will be specified to what kind of consumer something applies.

Secondly, there are **cloud providers** who are the counterparty of the consumer concerning the contractual relation and the one that is responsible for the quality of the service. They operate the cloud, process and store the data; maintain and upgrade the infrastructure, software, etc, and are also in charge of security in the cloud and privacy issues. Normally cloud providers are companies but this does not exclude individuals from the possibility of being providers as well.[20]

Cloud carriers are intermediaries between cloud consumers and providers that give "connectivity and transport of cloud services… through network, telecommunication, and other access devices."[21] This, because "the distribution of cloud services is normally provided by network and telecommunications carriers or a transport agents, where a transport agent refers to a business organization that provides physical transport of storage media such as high- capacity hard drives".[22]

[18] Marston, Sean. Op. Cit. p. 183.
[19] Throughout this paper they will be called consumers, customers, users or clients indistinctively.
[20] Hogan, Michael; et. al. *"NSIT Cloud Computing Standards Roadmap"*. USA, 2011, p. 24. Available at: <http://www.navigatingthroughthecloud.com/wp-content/uploads/2012/03/NIST-Cloud-Computing-Standard-Roadmap-2011.pdf?9d7bd4> Consulted on February 4th, 2012.
[21] Ibid. p. 24.
[22] Ibid. p. 25.

Moreover, providers need to sign service level agreements (SLA's) with cloud carriers[23], in order to be able to provide the services they offered consumers; therefore, SLA's on the one hand, are signed between providers and carriers, and need to be consistent with SLA's signed, on the other hand, by providers and consumers.[24]

Contractual relationships between providers, carriers and consumers can be more complicated (there may also be an agreement between carriers and consumers)[25] but for this dissertation is only necessary to understand the explained above.

1.7 Data Protection and Privacy Issues

Taking as starting point the nature of clouds, that among other things consists on massive storage of information, multiple transfers of data, and possibility of use of a variety of computing services; it is easy to think of several issues that could be of concern for consumers.

Even when not all of such problems or disadvantages are related to data protection or privacy, the purpose of this chapter, and of the whole text, is precisely to discuss only issues associated to the said matter.

Accordingly, it seems appropriate to begin by establishing what it should be understood by right to privacy and the right to data protection.

The Charter of Fundamental Rights of the European Union defines them in the following terms:

[23] Internet Service Providers (ISP's) can be considered as cloud carriers; nevertheless, there are ISP's also providing cloud computing services; which makes it difficult to enclose ISP's specifically as providers or carriers. See: Sluijs, Jasper; et.al. "*Cloud Computing in the EU Policy Sphere"*. TILEC Discussion Paper, 2011. Available at < http://ssrn.com/abstract=1909877> Consulted on February 10, 2012, p. 10.

[24] Hogan, Michael. Op.cit. p.25.

[25] Sluijs, Jasper; et. al. Op. Cit. P. 10.

"Article 7. Respect for private and family life.[26] Everyone has the right to respect for his or her private and family life, home and communications."[27]

"*Article 8. Protection of personal data*.

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law…"[28]

In the US, the first mention of the right to privacy dates back to 1890, when Warren and Louis Brandeis talked about "the right to be left alone". Hitherto, the right to privacy is not explicitly contained in the American Bill of Rights but the Supreme Court has ruled in several cases in favor of some privacy interests in relation to the first, third, fourth, fifth, ninth and fourteenth Amendments to the Constitution.[29]

As to the right of protection of personal data, "there is no single law in the United States that provides a comprehensive treatment of the right to data protection…" [30] There are only a number of laws that deal with certain kind of data protection but are limited to specific issues, such as prohibition to disclose medical and educational records. [31]

So far I have been referring to data in general, now is time to narrow the concept. To avoid going into a deep analysis of different types of data and definitions in various legislations, for purposes of this essay, in which the focus is on American and European laws, and since there is no clarity on the

[26] The right to privacy is also contained in Article 11 of the American Convention on Human Rights.
[27] Charter of Fundamental Rights of the European Union. Article 7.
[28] Ibid. Art. 8.
[29] Slemmons, Jean; Stratford, Juri. "*Data Protection and Privacy in the United States and Europe".* IASSIST Quarterly. P. 17. Available at: < http://www.iassistdata.org/downloads/iqvol223stratford.pdf> Consulted on June 13, 2012.
[30] Ibid.
[31] Ibid.

concept of data protection and privacy in the US[32], I will focus on the definition of personal data contained in the EU Privacy and Data Protection Directive. Furthermore, by utilizing this definition, it will be easier to notice the existing conflict between regulations of the US and the EU.

> *"Art. 2. (a) 'Personal data'* shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity…"[33]

In accordance to Working Party 29 (WP29), that analyses the above definition in parts, "any information" is all personal data regarding a person; either personal or private information, or in relation to his daily activities. Besides, such information does not have to be true nor proved in order to be protected.[34]

To this respect, something also important to notice is that it does not matter where data are kept or how data are presented (with numbers, images, words, graphics, electronically, in codes or any other way) for it to be considered as personal data.[35]

As to "relating to", WP29 clarifies that for information to be related to a person is not necessary the existence of an obvious or direct relation between data and the subject, in view of the fact that information can also be related if it

[32] In the USA PATRIOT Act, data is divided in content data and no- content data. This distinction will be explained in the following chapter.
[33] 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 the free movement of such data. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:html> Consulted on February 5, 2012.
[34] See Article 29 Data Protection Working Party. "Opinion 4/2007 on the concept of personal data." Europe, 2007, p. 6. Available at: <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm>
[35] Ibid. p.6.

concerns objects, processes or events, which belong to someone, or there is another sort of connection between them and an individual. [36]

Someone is “identified or identifiable” when is possible to distinguish him from a group. Data that can lead to the identification of someone can be direct, by name, or indirect by any information that by itself or in combination can lead to identify someone individually.[37]

Finally, a “natural person” shall be understood to be any human being with no restrictions of nationality or place of residence, because everyone has the right of protection of their personal data. This is also in accordance with the Universal Declaration of Human Rights where “natural person” was first defined. [38]

Furthermore, even when the concept of natural person does not directly include legal persons, information about them “may also be considered as ‘relating to natural persons’ on their own merits”.[39] This means that if the information allows identifying a specific subject or worker within the entity; as it could be by the use of an e- mail account, or by carrying out specific duties, then data can be considered as personal.

Now, due to the fact that the advantages of Cloud Computing are obtained from the handling of data in a dynamic way and all over the world, the risks and disadvantages posed by said handling, in relation to privacy and data protection, are directly connected to the system’s intrinsic characteristics.

Having in mind the latter definition and understanding the variety and importance of the wide range of data that can be found in a cloud, it is important to take into consideration potential risks of this system towards its clients’ data; risks that can be associated with issues such as:

[36] Ibid. p. 9.
[37] Ibid. p. 12.
[38] Ibid. p.22.
[39] Ibid. p.23.

- Whether the collection of data is carried out in an appropriate and secure manner;
- Whether the data are used in the way the customer intends it;
- Whether the data are disclosed to third parties without consent of the user;
- Whether the data is stored and transmitted safely;
- Whether or not copies of the data are being made every time it changes location;
- Whether or not the consumer can access and correct the data at his convenience;
- How long the data will be retained for;
- If in case of termination of the contract all data and its copies would be deleted, and,
- If the user is sufficiently informed of all this matters.[40]

Even when the situations mentioned are somehow linked to each other, in this paper attention will mainly be focused on the second and third issues: data utilized as consumer intended to, and disclosure to third parties without data subject's consent. This, because said issues are directly connected to privacy and data protection on disclosures to governments[41].

Since some of the most important cloud providers worldwide (Google, Microsoft, Amazon…) are governed by laws of the USA and have their bases on the land of said country, I will approach the matter specifically in relation to disclosure of data to the US government under provisions of the USA PATRIOT Act.

[40] Svantesson, Dan; Clarke, Roger. "*Privacy and Consumer Risks in Cloud Computing*." Elsevier, Computer and Security Law Review, 26, 2010, p.392. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364910000828> Consulted February 9, 2012.

[41] When talking about disclosures of data to the US government, I am referring to disclosures that are authorized by the laws of this country but that may be forbidden by other countries, or the EU. Furthermore, in all cases, without consumer's consent.

Attention will be paid on storage of data and trans-border data flow (from one country to another); how this results in conflict of jurisdiction and how can the USA PATRIOT Act be enforceable upon foreigner's data.

Before any further analysis, it is important not to forget that in order for Cloud Computing to be effective, providers not only need to be able to transfer data to their different data centers that can be located all over the globe, but it is likely that they will also replicate the data within the cloud (regardless of the location of the centers) to keep it available for use, for the cloud to perform as expected and also as back-up. Such replications or copies are sometimes temporary but can also be permanent.[42]

Besides this, providers use techniques such as "sharding" and "partitioning" that consist on fragments of data being stored in different servers that are linked in such a way as to allow consumers to have the data on demand and to improve the performance of huge databases.[43]This is especially true for SaaS.

Having this in mind, it is easy to understand that if data cannot travel freely through the servers the provider has, then most of the benefits of the cloud are lost. Providers, when calculating the investment needed to properly provide the services they offer, they take into consideration the capacity that will be required, an approximate amount of possible consumers, and the number of servers they would need to operate in a competitive manner.

The latter plays an important role especially when talking about transborder providers because the demand servers have varies in accordance to the time, place and even activities of consumers. So, if in one place more capacity is needed, then servers located in another place with less demand can provide the service for such location but, if data could not leave a specific region then

[42] Walden, Ian. "*Accessing data in the Cloud: The long arm of the Law Enforcement Agent*." Queen Mary School of Law Legal Studies Research Paper No. 74/2011, United Kingdom, 2011, p. 3. Available at: <http://ssrn.com/abstract=1781067> Consulted on April 3, 2012.
[43] Ibid.

providers would need to have servers in every country or region in which they wish to offer their services; making the investment required a lot higher and somehow even useless.

1.8 Scenarios

To give structure to this dissertation and to present the information and the results in an organized way, six scenarios will be analyzed separately in order to see in which ones the USA PATRIOT Act is applicable, or how can its enforcement be avoided by changing stakeholders or location.

The scenarios take into consideration the location of providers, if they have subsidiaries and their location, the place where their data centers are, and the nationality of the consumer.

Scenario	Provider	Subsidiary	Data center	Customer
First	American	None	America	European
Second	American	European	Europe	European
Third	European	None	Europe	European
Fourth	European	None	Europe	American
Fifth	European	American	America	Both
Sixth	European	American	Europe	Both

1.9 Conclusions

- Cloud computing is an information technology service model where computing services are delivered on-demand to customers over the network independent of device and location.[44]

- It can be delivered, in different forms, including as Software as a Service, Infrastructure as a Service, Platform as a Service or a combination of them.

[44] See Marstoon, Sean; et.al. Op.cit.

- The main stakeholders are: Cloud Provider, Cloud Consumer and Cloud carrier.

- Data, for purposes of this paper shall be understood as “Personal Data” as defined in the European Directive 95/46/EC.

- When handling data in the clouds, there are some risks that need to be considered. This dissertation focuses on disclosure of data in relation to the USA PATRIOT Act.

- For Cloud Computing to remain effective, providers need to be able to transfer data to their data centers, that can be located anywhere in the world.

- Six possible scenarios that take into consideration, providers, different locations and consumers, are presented to keep them in mind when analyzing applicability of the USA PATRIOT Act in the forth chapter.

Chapter 2

USA PATRIOT ACT

2.1 Introduction

In this chapter the USA PATRIOT Act, a controversial piece of legislation will be analyzed as a whole and some of its sections in particular.

To be able to understand correctly its functioning, it is necessary to go back to the situations that originated it; to later continue with the analysis of some of its sections, in order to be able to distinguish the different instruments available for the government to request providers access to data of consumers, and finally, to see how these instruments are being used and challenged in Court.

2.2 Background

USA PATRIOT Act is the acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"[45].

It is well known that there are many critics[46] of this piece of legislation, not only within the United States nationals but also internationally. Nevertheless, there are also defenders of it that argue that no civil liberties are being violated and that it fits right with security aims[47].

In order to understand both arguments and to create one's own criteria, it is indispensable to go back to the very particular circumstances that gave rise to it; as well as the wording of the text and its form.

The USA PATRIOT Act dates from October 26th, 2001, just a little more than a month after the occurrence of the infamous terrorist attacks perpetrated on American territory, when two passenger planes were crashed on two of the

[45] USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), available at: http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf>

[46] Two of the most representative ones are Judge Napolitano and ex Senator Ron Paul.

[47] See: Dinh, Viet. *"USA PATRIOT Act".* German Law Journal, Vol. 5, Number 5, USA, 2004. Available at: < http://www.germanlawjournal.com/pdfs/Vol05No05/PDF_Vol_05_No_05_461-467_special_issue_Dinh.pdf> Consulted on January 25, 2012.

most representative buildings in the city of New York and of the country, the twin towers of the World Trade Center; as well as more attacks in other cities; such as Washington D.C. and Pennsylvania.

Thus, while American society was shocked by the attacks that had just occurred, and there was great uncertainty as to possible new and imminent attacks, the Act was drafted under the idea of preventing them by giving authorities wider faculties to investigate individuals that could be involved in terrorist activities or organizations.

Some people claim that the idea of giving more power to authorities in charge of security in detriment of Americans' civil rights was not new but something that had already been planned and so, the attacks were the perfect pretext to send the initiative to the Congress, who in light of the situation earlier described was inclined to approve the Act.[48]

Nonetheless, the official version of the creation and approval of the Act is that it was drafted in approximately six weeks[49], by, at the time, Attorney General Ashcroft. Once the initiative reached the Congress, the legislative procedure was duly followed. In hastiness but it was discussed in both, the House of Representatives and in the Senate and after limited debate and experts opinions, it was approved in both chambers.[50]

Even when excuses for the behavior of the Congress could be found if taking into consideration the series of events that had just taken place; it should be noted, before going into a deeper analysis of the Act and staying with only the

[48] Van Bergen, Jennifer. *"The USA PATRIOT ACT was planned before 9/11"* Truthout, 2002. Available at: < http://www.globalissues.org/article/342/the-usa-patriot-act-was-planned-before-911 >

[49] Dinh, Viet. Op.cit. p. 463.

[50] On the one hand, on October 23rd it was introduced in the House of Representatives; the following day was passed by 357 votes in favor, 66 against and 9 abstentions; and on the other hand, the initiative was introduced to the Senate on October 25th and it was approved, almost unanimously, by 98 votes in favor, one against and one abstention. The next day, October 26th, President George Bush, signed the Act and it was enacted. See Standler, Roland. *"Brief History of the USA PATRIOT Act of 2011".* 2008, p.3. Available at: <http://www.rbs0.com/patriot.pdf>

legal formalities, that legislators approved the most controversial sections of the Act only for a period of five years, renewable.

The reason why these provisions, unlike the rest of the Act, had a limited period of validity was because of concerns that they could be used to violate civil liberties of Americans; particularly the ones contained in the first and fourth Amendments of the Bill of Rights. This leads to the suspicion that members of Congress knew beforehand that such provisions were unconstitutional and still, they decided to pass them.[51]

Such provisions, known as "Sunset provisions", were discussed again in 2006, now without the hastiness and immediate motive that could have led Congressmen to act irresponsibly, and yet, the sixteen provisions were again passed; most of them were made permanent provisions with few minor changes and three were left as "sunset provisions".[52]

In February 2010, when the "sunset provisions" were set to expire, President Obama signed into law an extension of one year because at this point, Congress had not had enough time to discuss and reach an agreement.[53]

Once again, just before the expiration date of the provisions, in 2011, Congress voted for a three months extension for discussion of the provisions.[54] After this period, they decided in favor of maintaining the three "sunset provisions" for four more years.[55]

---

[51] Standler, Roland. Op. Cit. p.7.

[52] This was approved in the House of Representatives by 280 votes in favor, 138 against and 14 abstentions, whereas in the Senate were approved by 89 votes in favor, 10 against and one abstention. The President, still George Bush, also signed the approval for renewal of the provisions, this time for a period of four years. CNN Politics. *"House approves PATRIOT Act renewal"* CNN online, USA, 2006. Available at: < http://articles.cnn.com/2006-03-07/politics/patriot.act_1_patriot-act-renewal-controversial-provisions?_s=PM:POLITICS>

[53] Abrams, Jim. "*Patriot Act Extension signed by Obama*". Huff Post Politics, USA, February 2011. Available at: < http://www.huffingtonpost.com/2011/05/27/patriot-act-extension-signed-obama-autopen_n_867851.html>

[54] Associated Press. *"Patriot Act Extended for three months*" New York Times, USA, 2011. Available at: < http://www.nytimes.com/2011/02/18/us/politics/18brfs-PATRIOTACTEX_BRF.html>

[55] In the House of Representatives there were 250 votes in favor, 153 against and 29 abstentions; in the Senate, 72 in favor, 23 against and 5 abstentions. CNN Politics. "*Congress approves extension of*

Among the provisions that were set to expire are those that have caused more problems in the field of privacy, data protection and technology.

The temporary provisions at first were the following:

> "Sections 201 (wiretapping in terrorism cases), 202 (wiretapping in computer fraud and abuse felony cases), 203 (b) (sharing wiretap information), 203 (d) (sharing foreign intelligence information), 204 (Foreign Intelligence Surveillance Act (FISA) pen register/trap & trace exceptions), 206 (roving FISA wiretaps), 207 (duration of FISA surveillance of non- United States persons who are agents of a foreign power), 209 (seizure of voice- mail messages pursuant to warrants), 212 (emergency disclosure of electronic surveillance), 214 (FISA pen register/trap and trace authority), 215 (FISA access to tangible items), 217 (interception of computer trespasser communications), 218 (purpose for FISA orders), 220 (nationwide service of search warrants for electronic evidence), 223 (civil liability and discipline for privacy violations), and 225 (provider immunity for FISA wiretap assistance)."[56]

The three provisions that were renewed in 2011 are: Section 206, also known as "roving wire", 214, called "lone wolf" and Section 215 or "business records".[57]

2.3 Content

As stated in the first part of the text of the USA PATRIOT Act, its purpose is "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes".[58]

---

expiring Patriot Act provisions". CNN online, USA, 2011. Available at: < http://articles.cnn.com/2011-05-26/politics/congress.patriot.act_1_lone-wolf-provision-patriot-act-provisions-wiretap?_s=PM:POLITICS>

[56] Doyle, Charles; et.al. "*USA PATRIOT Act Sunset: Provisions that expire on December 31st, 2005*." CRS Report for Congress, The library of Congress, USA, 2004, p.1. Available at: < http://www.fas.org/irp/crs/RL32186.pdf>

[57] Left and right news. "*Patriot Act faces renewal in 2011*". Left and right news, USA, 2011. Available at: < http://www.leftandrightnews.com/2011/01/17/patriot-act-faces-renewal-in-2011/>

[58] USA PATRIOT Act.

It is divided into ten Titles and each Title, in turn, is composed by a different number of sections that altogether result in a total of 158, translated into almost 350 pages.

When reading it, it is easy to notice that is not written as a normal statute or piece of legislation since it contains only amendments to other Acts, compiled in the United States Code; among which are: the Foreign Intelligence Surveillance Act (FISA), the Victims of Crime Act of 1984, the Electronic Communications Privacy Act (ECP), Computer Fraud and Abuse Act, Stored Communications Act, Money Laundering Control Act, Bank Secrecy Act, Immigration and Nationality Act, Right to Financial Privacy Act and Telemarketing and Consumer Fraud and Abuse Prevention Act.

Given that this dissertation does not focus on the PATRIOT Act as such, but on its international effects in relation to cloud computing, I will not expand on the issues addressed in each title of the Act, but I will limit the analysis to the sections really relevant for the topic at hand.

Before going there, and as it will be relevant later on, because of all the controversy that has caused for the violation of some of the basic rights of Americans[59], herein, though not the only ones, are two of the most affected Amendments of the American Bill of Rights and should be kept in mind when reading through the Sections of the Act and the case analysis of this chapter.

> **First Amendment**. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or a abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition to the Government for a redress of grievances."[60]
>
> **Fourth Amendment**. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause,

[59] See Doe v. Gonzales, Doe v. Ashcroft, et.al.
[60] Bill of Rights. USA. Available at: < http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html>

supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[61]

As we can see, the First Amendment is not about privacy but rather about freedom of speech, however is relevant for this chapter because through these two amendments Courts have found the requests for disclosure to be unconstitutional. The Fourth Amendment does contain the right to privacy and protects against unreasonable searches.

2.4 Analysis of relevant Sections

Because a thorough analysis of all the sections that might relate to the subject in comment would be very long and to some extent repetitive, I selected the sections that, in my opinion, help answer the research question and make clear that there are different types of legal instruments that can be used to request data from cloud service providers. Therefore, two sections in which is necessary to obtain court orders, two regarding the FISA Act and the one encompassing National Security Letters will be studied.

What the Act has really changed in comparison to the legislation as it was before, is that now, authorities can ask for more information to providers, they can issue orders under the Foreign Intelligence Surveillance Act and National Security Letters in a relatively easier way, the prohibition to disclose the existence of such orders, and has also enabled more authorities to emit said documents.

With the analysis of specific sections we will see the above in more detail.

Regarding the second Title of the PATRIOT Act, "Enhanced surveillance procedures", it contains the most problematic and relevant sections for the topic being discussed.

Section 210 of the Act addresses the subject of "Scope of subpoenas for records of electronic communications"[62] and what it modifies is that increases

[61] Ibid.

the categories of information governmental entities[63] can request when issuing subpoenas for electronic communications providers.

Such information consists of name, address, telephone connection records, time and duration of session, length of service and type of service utilized, telephone or instrument number or identity, assigned network address, source of payment, including credit card or bank account numbers of a subscriber. [64]

Data mentioned in the preceding paragraph may be requested by 1) a warrant issued by a Court under the Federal Rules of Criminal Procedure; 2) a Court order obtained by fulfilling the requirements that are mentioned below, 3) with consent of the customer, or 4) by a formal request for a law enforcement investigation regarding telemarketing fraud.[65]

In this case, as Court orders are the method to follow to acquire data through this section of the Act, herein are the requirements orders need to contain. This is useful as well because it allows us to distinguish between these documents and the ones that will be explained later on.

> "A court order[66] for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation… A court issuing an order pursuant

[62] ""Electronic communication" means 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, photo electronic or photo optical 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." 18 U.S.C. § 2510 (12)

[63] "Governmental entity means a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711 (4)

[64] 18 U.S.C. § 2703 (C) (2)

[65] 18 U.S.C. § 2703 (C)

[66] These types of Court orders are also known as "warrants".

> to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."[67]

Furthermore, there is an immunity clause for providers that disclose information due to a Court order; which means that no legal action can be started against them, their employees, agents or other people involved.

This section relates to cloud computing because cloud providers, since they handle electronic communications, can be subpoenaed to release "stored wire and electronic communications and transactional records."

Section 212, "Emergency disclosure of electronic communications to protect life and limb" modifies the US Code, Title XVIII, under topic "Stored wire and electronic communications and transactional records access", sections 2702 and 2703.

The referred section 2702 is an exception to the rule of the ECPA that prohibits voluntary disclosures, and it provides that in case service providers "reasonably believe" there is imminent danger that could cause death or serious physical injuries to someone, then they are allowed to disclose data that could help prevent such things from happening.

Concerning Section 2703, part "B", the PATRIOT Act did not change significant things related to privacy; it only changed the heading of the section, that now reads: "Required disclosure of costumer communications or records"; and the first paragraph of the citation that follows; even so, the inclusion of this stipulation in the analysis is important because it shows that the US government can ask for content of communications taking place in the clouds.

[67] 18 USC § 2703 (D)

"(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service[68] to disclose the **contents**[69] of any wire[70] or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection.

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service…a) on behalf of a subscriber; and b) solely for the purpose of providing storage or computer processing services…"[71]

[68] "Remote Computing Service means the provision to the public of computing storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711

[69] ""Contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510 (8)

[70] "Wire communication means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce". 18 U.S.C. § 2510 (1) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception. 18 U.S.C. § 2510 (18)

[71] 18 USC § 2703

Under this article is stated as well that a governmental entity can also ask to disclose records of a subscriber (not including content) and to preserve evidence, when so requested, for 90 extendable days.

Regarding the requirements for issuing a Court order, these are the same that the ones explained for section 210.
The immunity clause for providers that disclose information also applies.

This type of court orders are directly related to Cloud Computing because they refer to requests for data in "Remote Computing Systems", that are the "provision of computing storage and processing services"; and as established on chapter I, such services fit into the definition of Cloud computing.

Section 215 amends the Foreign Intelligence Surveillance Act (FISA) that is about governmental agencies gathering foreign intelligence information for investigations.

There are several types of FISA orders, depending on the authorization given to federal officials, and they can be for electronic surveillance, physical searches, to use pen registers and trap and trace devices, to access business records and other tangible things or to target US persons believed to be abroad. [72]

All FISA orders need to be related somehow to foreign powers or intelligence, but their issuance by the FISC there are different standards:

For *electronic surveillance*, a "statement of the facts and circumstances relied upon"[73] to justify the governmental believe that an order of this kind is needed. It should also include "the identity, if known or a description of the target of the

[72] Henning, Anna. Op.cit. p.9.
[73] Ibid.

search".[74] When discussing the next section of the PATRIOT Act, an important change to this sort of orders will be duly noted (as well as for physical searches).

For *physical searches*, identity or target believed to be of a foreign power or intelligence and a statement of facts as explained above.

For the use of trap and trace devices, authorities need to certify that the "information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism and clandestine intelligence activities."[75]

As to orders for *access to business records and other tangible things*, these will be studied with more detail in the subsequent paragraphs. This citation was added by the PATRIOT Act.

> "Sec.501. Access to certain business records for foreign intelligence and international terrorism investigations.
> (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director may make an application for an order requiring the production of <u>any tangible things</u> (including books, records, papers, documents, and other items) for an investigation to obtain <u>foreign intelligence information</u>[76] <u>not concerning a United States person or to protect against international terrorism or clandestine intelligence activities</u>, provided that such investigation of a United States person

[74] Ibid.
[75] Ibid.
[76] "Foreign intelligence information", for purposes of section 2517(6) of this title, means—
(A) Information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(B) Information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—
(i) the national defense or the security of the United States; or
(ii) the conduct of the foreign affairs of the United States." 18 USC § 2510 (19)

> is not conducted solely upon the basis of activities protected by the first amendment to the Constitution …" [77]

Before the USA PATRIOT Act, it was specified what kind of documents could have been requested, then, with the "any tangible things" the scope became so broad that this part was a target for criticism because the range of information that could be requested.

As this section was one of the "sunset provisions", in 2005 legislators added a part to somehow restrain the scope of the concept, and it now reads that if the information sought is related to "library circulation records, library patron lists, book, sales and records, book customer lists, firearms sales records, tax return records, educational records or medical records",[78] the authorization for requesting the order has to come from one of the three Federal Bureau of Investigations (FBI) officers with a higher rank.

Despite the latest addition, "any tangible things" is still too broad, because it allows for the possibility of governmental authorities acquiring data, since, even when data as such is not tangible by definition, tangible things that contain data can be requested, among others, hard drives, medical, educational, business records or, in general, any tool in which data can be stored.[79]

As to the requirements for obtaining an order of this kind or "FISA order", these are different to the Warrants mentioned in the previous section. First, a warrant is issued by one of the District Courts in the country, and for FISA

[77] USA PATRIOT ACT, Title II, Section 215 and 50USC § 1861

[78] Liu, Edward. *"Amendments to the Foreign Intelligence Surveillance Act (FISA) extended until June 1, 2015"*. Congressional Research Service, USA, 2011, p.10. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf>

[79] American Civil Liberties Union. "*Reclaiming Patriotism: A call to reconsider the PATRIOT Act".* ACLU, USA, 2009, p.32. Available at: <http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf> Consulted on April 02, 2012.

orders there is a special Court for all issues related to the Act, the Foreign Intelligence Surveillance Court (FISC)[80].

Second, warrants are issued only when there are indicia of a criminal conduct and reasonable grounds to believe the information is relevant to the investigation, while to get a FISA order, with the modifications of the reauthorization of the Act, there has to be a statement of facts indicating the relevancy of data for the investigation, and a "enumeration of minimization procedures[81]… applicable to the retention and dissemination"[82] of tangible things by the FBI.

Moreover, people that receive this kind of orders cannot disclose to any other person and under no circumstances, neither that they received an order nor the information they were asked to provide. Orders that contain this non-disclosure requirement are also normally known as "gag orders".

As in the preceding section, people that reveal or help to obtain the required information, shall not be liable to any other person in relation to the production of such information. [83]

Finally, every six months, the Attorney General needs to present a report concerning all the requests issued under this section to the respective Committees on Intelligence of each of the Houses in Congress.

Since FISA orders allow for the obtainment of "any tangible things" for foreign intelligence investigations, data in the clouds can also be acquired if stored in tangible devices or if contained in tangible things. .

[80] This Court is comprised of eleven district judges, of "whom no fewer than three shall reside within 20 miles of the District of Columbia". US Department of Justice." *The Foreign Intelligence Surveillance Court*". Membership, 2007. Available at: <http://www.fas.org/irp/agency/doj/fisa/court2007.html> Consulted on May 12, 2012.

[81] "Minimization procedures"… are safeguards which limit the government's use of collected information" regarding retention, dissemination or disclosure of data. Henning, Anna, et.al. "Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization. Congressional Research Service, USA, 2010, p.9. Available at: < http://www.fas.org/sgp/crs/intel/R40980.pdf> Consulted on March 27, 2012.

[82] 50 USC § 1861 (2) (B)

[83] USA PATRIOT ACT. Section 215

Section 218, "Foreign Intelligence Information" modified two provisions of the US Code: 50 USC § 1804 and § 1823 in which instead of saying "the purpose", now it reads "a significant purpose. The former for electronic surveillance and the latter for physical searches.

The part that was changed refers to applications for court orders for electronic surveillance[84] and besides the standards that were mentioned in the analysis of section 215 of the PATRIOT Act, it is established that a certification by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security of defense…"[85] need to certify that the information they deem to obtain is foreign intelligence information; and "that a "significant purpose" of the surveillance is to obtain foreign intelligence information…"[86] Exactly the same applies but for physical searches.[87]

---

[84] Electronic surveillance" means—**(1)**the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; **(2)**the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;**(3)**the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or **(4)**the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. 50 USC § 1801 (f)(1)(2)(3)(4)

[85] 50 USC § 1804 (a)(6)(A)

[86] 50 USC § 1804 (a)(6)(B)

[87] "Physical search" means any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under

The importance of this modifications lays in the fact that by establishing that only a significant purpose is needed, the fourth Amendment to the Constitution is surpassed, since it is meant to protect against unreasonable searches and it states that "no warrants shall be issue, but upon probable cause".

This section can be related to cloud computing because American providers could receive an order of this type, but it is not relevant for the topic being discussed, which is, disclosure of data from cloud service providers.

Section 505, entitled "Miscellaneous National Security Authorities" is a particularly relevant section for this dissertation since is about National Security Letters, the instrument that in recent years is used the most by the United States government to collect data from people all over the world by following a relatively easy procedure.

The idea of giving the government the opportunity to hand out documents requesting data from users of different services goes back to the Right to Financial Privacy Act of 1978 (RGPA), which, as an exception to the privacy rules contained therein, allowed the possibility of issuing an informal document requesting financial information regarding users, in "the case of foreign intelligence, secret service protective functions and emergency situations"[88]. Nevertheless, such documents could not legally compel service providers to disclose information.

It was not until 1986 when the FBI started using the term National Security Letters for the type of documents they could use to request information; at this

circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include electronic surveillance…" 50 USC § 1801 (5)

[88] Nieland, Andrew. *"National Security Letters and the Amended Patriot Act"* Cornell Law Review, Vol. 92, USA, 2007, p. 1208.

time, for both, financial institutions and electronic and communication providers, since a similar provision was added to the Electronic Communications Privacy Act (ECPA) of the said year.[89]

During all this time, letters continued to be voluntary because their outcome was very successful. As there was one main communications provider at the time (AT&T), and was willing to cooperate with the government, no other measures needed to be taken; therefore, problems only began to arise with the emergence of new companies and the coming into force of privacy laws in several states of the country.[90]

In the following decade, Congress added a similar provision to a couple of Acts. To the National Security Act, regarding investigations of leaks of classified information by governmental employees, and to the Fair Credit Reporting Act, allowing the FBI to obtain access to credit agency records.[91]

Despite the above mentioned it was not until the enactment of the USA PATRIOT Act that the existence of NSL's became evident to more people, and hence, highly controversial due to the modifications that were made to the four Acts that contemplated the existence of said document.

The four Acts are: (a) The Electronic Communications Privacy Act (ECPA), for communication providers; (b) the Right to Financial Privacy Act (RFPA) addressed to financial institutions; (c) the National Security Act (NSA), for financial institutions and consumer credit agencies; and (d) the Fair Credit Reporting Act for consumer credit agencies as well.[92] Practically all of these Acts were modified by the Patriot Act in the same way.

---

[89] Cfr. Ibid. p. 1208

[90] Cfr. Ibid.

[91] Doyle, Charles. "National Security Letters in Foreign Intelligence Investigations: A Glimpse of the legal background and recent amendments."Congressional Research Service, USA, 2010, p.1. Available at: <www.crs.gob>

[92]See: Office of the Inspector General. *"A Review of the Federal Bureau of Investigation's use of National Security Letters*". US Department of Justice, USA, 2007. Available at: <http://www.justice.gov/oig/special/s0803b/final.pdf> Consulted on February 20, 2012.

Summing up, the history of NSL's expressed in the preceding paragraphs is relevant because back then, due to the circumstances in which provisions where drafted, legislators did not envision the impact they would have later on with the development of technologies and massive storage of data. However, such provisions were the basis for the reach they now have.

National Security Letters can be said to have five main characteristics that are useful to understand how they work and what the USA PATRIOT act really changed. The underlined parts in each of the quotations were added or modified by the Act.

1. – **Subject** or to whom a letter is addressed.

> "Duty to Provide.— *A wire or electronic communication service provider*[93] shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the

[93] "A electronic communications service provider means: a) A telecommunications carrier , as the term is defined in section 3 of the Communications Act of 1934 (47 USC 153); b) A provider of electronic communication service, as the term is defined in section 2510 of title 18 USC; c) A provider of a *remote computing service*, as the term is defined in section 2711 of Title 18 of the USC; d) Any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; e) A parent, subsidiary, affiliate, successor or assignee of an entity described in subparagraph A, B, C or D; or; f) An officer , employee or agent of an entity describe in A, B, C , D or E." See FISA Amendment Act. Available at: <http://www.govtrack.us/congress/bills/111/hr3846/text> Consulted on June 22, 2012.

Definition of remote computing service was already provided; therefore here is the term as defined in the Communications Act. –"Telecommunications service : The term "telecommunications service" means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." 47 USC § 153 (53).

> Director of the Federal Bureau of Investigation under subsection (b) of this section."[94]

This provision was not modified by the Act but, as pointed out earlier since circumstances changed with the development of technology, what first could have been understood as "wire and electronic communication service providers", now the same terminology includes not mainly telephone companies but more important providers; from Internet Service Providers (ISP's), Cloud Computing Providers, Telephone Companies and, according to the FBI "any business or organization that enables users to send messages through a web site.- Including universities, libraries, businesses, political organizations, and charities".[95]

Furthermore, if we take into consideration all the NSL Statutes, not only communications providers are subjects but also financial institutions, consumer credit agencies and travel agencies.

As previously stated, before the Patriot Act, compliance with NSL's was thought to be voluntary because there were no penalties in case of noncompliance; but, with the amendments some penalties (that will be discussed with the last characteristic) were added in order to clarify the mandatory nature of these letters.

2. - **Certification** or authority that issues the letter.

> "The Director of the Federal Bureau of Investigations or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director."[96]

[94] 18 U.S.C. § 2709.
[95] Nieland, Andrew, op.cit. p. 1214
[96] 18 U.S.C. § 2709

With such addition the range of people that can issue an NSL increased dramatically to the point that even field offices can issue them and do not require the supervision of a headquarter.

3. - **Nexus** or the relation between the information sought and the relevance of it for the investigation.

> " …Made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism and clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States;…"[97]

Before, the Director or entity issuing the document had to certify to the subject that the information sought "pertained to a foreign power or the agent of a foreign power"[98], and now that it only needs to be relevant and related to international terrorism, the nexus is broader, making easy the justification of the emission of letters and not only that, but also the emission of letters requesting data of anyone that might be related to the investigation regardless of their nationality and place of residence.

We will see later on, that a high percentage of NSL's are issued even when there is only a preliminary investigation.

4. - **Scope** of the letter. It refers to all the information requested.

As stated in the Patriot Act, in the paragraph cited herein in the first of the characteristics, information refers to "subscriber information and toll billing records information, or electronic communication transactional records".

[97] Ibid.
[98] Fine, Glenn. "A *Review of the Federal Bureau of Investigation's Use of National Security Letters*." US Department of Justice, USA, 2007.

Since there is no definition of what electronic communication transactional records mean, in accordance to the FBI, the term includes "every Web site a particular person has accessed, as well as the recipients addresses and subject line of every e-mail sent to the provider in question."[99]

5. - **Non- disclosure** requirement.

As in FISA orders, there is a permanent non- disclosure requirement, also known as "gag order". This was established under the idea of the repercussions it could have for the investigation in place or for the life of people involved in it.

Prohibition reads as follows:

> "…no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."[100]

The part in the parenthesis did not appear in the first version of the Act; it was added in the reauthorization as the outcome of the most significant case about NSL's, *Doe v. Ashcroft*. Before, the prohibition applied with regard to "any person" and it was believed to be restricting of the First and Fourth Amendments of the US Constitution.[101]

Moreover, with the Patriot Act, penalties were made clear for both cases, noncompliance with the gag order or confidentiality requirement, and if data

[99] Ibid.
[100] 18 U.S.C. § 2709.
[101] See: Crime and Federalism. *"Doe v. Gonzales: Disclosure under the Stored Communications Act".* 2006. Available at: <http://federalism.typepad.com/crime_federalism/2006/05/doe_v_gonzalez_.html> Consulted on February 22, 2012.

requested is not disclosed to the FBI. If a person "knowingly and with the intent to obstruct an investigation or judicial proceeding violates such prohibitions or requirements… such person shall be imprisoned for not more than five years, fined under this title, or both."[102]

Now, after the analysis of the main characteristics of NSL's, it is worth mentioning some particulars of the case that caused social awareness of the existence and reach of the letters and a couple of reforms that, due to the ruling, took place with the reauthorization of the Act.

The name of the case is *John Doe v. Ashcroft*. We currently know that John Doe stands for Nicholas Merrill, but at the beginning, due to the gag order, plaintiff was only known to be a small Internet Service Provider in New York City with not so many clients. [103]

In 2004, when he was served a letter requesting sixteen categories of electronic communications transactional records on one of his users, he rightly believed that if he disclosed such data, besides harming his client, his business would have suffered; hence, he was the first one in the whole country to challenge a NSL in Court.

In the claims plaintiff stated violation to the First Amendment of the Constitution that contains the right to freedom of expression and of the Fourth Amendment that bans unreasonable seizures and searches.

Obviating procedural stages, the outcome of the case were two rulings. The first one in 2004 from a District Court that found the NSL statute to be unconstitutional, because of the permanent non disclosure requirement that

[102] 18 U.S.C. § 1510 (e).

[103] Nakashima, Ellen. *"Plaintiff who challenged FBI's national security letters reveals concerns*." Washington Post, USA, 2010. Available at: < http://www.washingtonpost.com/wp-dyn/content/article/2010/08/09/AR2010080906252.html> Consulted on March 02, 2012.

goes against the first amendment, and the "compulsory, secret and unreviewable production of information required by the FBI's application".[104]

Such ruling led Congress to change the provision on non-disclosure by precisely adding the part that was underlined in the citation under the fifth characteristic. With that adjustment it is now clear that any person served with a letter can challenge it in Court or be advised as to its compliance.

The second decision, in 2008 from the Court of Appeals, held that the first Amendment was still being infringed because of the permanent nature of the gag order, and that in order to avoid that, it was necessary for the FBI to prove to a Court, in cases where the gag order was challenged, that disclosure would put in danger national security.[105]

From that day forward, it appears that the FBI adopted the ruling as policy and now, when a letter reaches Court, the Agency (FBI) drops the non disclosure requirement. In this case, the gag order was finally withdrawn in 2006.[106]

As we have seen, National Security Letters relate to Cloud Computing because the FBI can request data in the clouds through this method, to wire or electronic communication service providers.

Now that FISA orders and National Security Letters have been explained, it is important to realize what the differences between both instruments are, to understand why NSL's are issued in larger amounts than FISA orders.

First, FISA orders have to be approved by the FISC, while NSL's are issued directly by officers of Federal Agencies; which means that there is one more

[104] Marrero, Victor. "*Opinion Doe v. Ashcroft*". United States District Court, New York, 2004. Available at: < http://www.aclu.org/FilesPDFs/nsl_decision.pdf> Consulted on April 2, 2012.
[105] Ibid.
[106] Ibid.

procedural step with FISA orders and that authorities need to comply with the standards set for each different type of order, which might include presenting before the FISC their statement of facts.

Another important thing to consider is that while with a FISA order the type and quantity of information that can be obtained is considerable due to the scope set by "tangible things"; with a NSL it is not possible to acquire "content information".[107]

Content information "includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication"[108]. Hence, the whole content of an e-mail or a telephone call can be requested through a FISA order.

Data that can be obtained with a NSL varies due to the Act in which a letter is based, but among the sort of data that can be requested are financial and credit records, IP addresses, customer's names, addresses, length of service provided, billing records, current and former places of employment, identification of financial institutions in which a person has accounts, etc.[109]

Another difference between both documents is that NSL's have their legal basis in four Acts while FISA orders, as implicit in the name, are based on the FISA Act.

For all of the above, since the coming into force of the USA PATRIOT Act, the number of NSL's issued every year exceeds by far the number of FISA orders, and this mainly because it is not necessary to have a court approving the order.

---

[107] See: Liu, Edward. *"Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended until June 1st, 2015."*Congressional Research Service, USA, 2011, p.4. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf>

[108] 50 U.S.C. § 1861 (n).

[109] Henning, Anna, et.al. "*Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization.*" Congressional Research Center, USA, 2010, p. 11. Available at: <http://www.fas.org/sgp/crs/intel/R40980.pdf> Consulted on February 12, 2012.

In the next part we will come to show this with facts and figures in order to relate it to the threat and concerns NSL's are causing; particularly outside of the US.

2.5 Facts and Figures NSL's and FISA orders

As requested by Law, there is a FBI's National Security Letter Database, known as Office of General Counsel (OGC), in which information is gathered regarding the number of requests by year, the type of data and if such data concerns an American citizen or a foreigner. It shall be noticed that a request and an NSL is not the same since in one NSL there can be more than one request.

From analyzing a couple of reports of the US Department of Justice for the years 2003-2011, some facts and figures were abstracted and are herein presented. It is clear that the majority of data requested are telephone toll billing records and e-mail or electronic transactional records under ECPA.

Also, that from the total of NSL's, 43.7% were issued when there was only a preliminary investigation and 56.3% when there was a full investigation taking place. Regarding the cause of all the requests, 73% were issued for counterterrorism purposes, 26% for counterintelligence and 1% for computer intrusion.[110]

In the first Table, the number of requests per year is illustrated, as well as if requests were for data on American citizens or non American. In the second one, the number of FISA orders approved by the FISC is shown, as well as the number of orders that were denied. [111]

[110] Office of the Inspector General. "*A Review of the Federal Bureau of Investigation's Use of National Security Letters*". US Department of Justice, USA, 2007, p.21. Available at: <http://www.fas.org/irp/agency/doj/oig/natsec.pdf> Consulted on March 14, 2012.

[111] Electronic Privacy Information Center. "*Foreign Intelligence Surveillance Act Court Orders 1979-2011*". Available at: < http://epic.org/privacy/wiretap/stats/fisa_stats.html> Consulted on May 31, 2012.

NSL	2003	2004	2005	2006	2007	2008	2009	2010	2011
US	6,519	8,943	9,475	11,517	4,327	7,225	6,114	14,212	7,201
Other	10,232	8,494	8,536	8,605	12,477	17,519	8,674	10,075	9,310

FISA	2003	2004	2005	2006	2007	2008	2009	2010	2011
Approved	1727	1758	2074	2181	2371	2082	1329	1579	1745
Rejected	4	0	0	1	4	1	1	0	0

As we can see, the number of National Security Letters exceeds by far the number of FISA orders that are issued each year.

This is the reason why these documents are the ones best known in the world from all other available instruments for governmental access to data. This is also the base of concerns inside and outside of the US regarding the accessing of data of foreigners without their consent or acknowledgement and approval from other governments.

Moreover, this is happening on a great scale since are thousands of orders that are issued every year and a high percentage of them with only having a preliminary investigation.

2.6 FBI's dissemination of data to other entities

In accordance to Attorney's General Guidelines and other information- sharing agreements, the FBI's should share their intelligence with other agencies.[112]

[112] Op. Cit. P. 56

The FBI's Guidelines for National Security Investigations provide that "… the information should be shared as consistently and fully as possible among agencies with relevant responsibilities…the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security…"[113]

This sharing of information means that data obtained from NSL's is not only for FBI's enjoyment but also for any other agency requesting information gathered by the FBI, which can lead us to think that the latter is acting more as intermediary that acquires the data and then transfers it without any other legal precautions or requirements.

Hence, it can be said that NSL's provide easy access to data that can later be used in a wide range of ways and without further procedures.

Summarizing: Why should NSL's worry us?

- NSL's are issued without approval of a Court.
- Because of the large number of people that can request such letters and the consequent dissemination of data acquired through them.
- The easiness with which an NSL can be issued.
- The fact that due to the "gag order", users are intended to remain in the darkness, both during compliance with the letter and afterwards.
- Every year thousands of letters are issued regarding both, Americans and foreigners, even if there is not yet an ongoing investigation.
- Most Service providers seem willing to cooperate with the government, which can also lead to excessive and incorrect use of NSL's.

[113] Ibid.

- Even though "content information" cannot be requested in a NSL, the information that can be obtained may lead to know a lot of aspects of an individual.

2.7 Case Law

Once the challenging of NSL's became public and possible after the case previously mentioned, Doe v. Ashcroft, others followed plaintiff's example and started going to Court.[114]

Two cases are worth mentioning here because plaintiffs are service providers; one of them is well known and is also one of the most important cloud providers at the moment, Twitter. In the other one plaintiff still remains secret but, due to the characteristics of the case that are similar to the one of Twitter, it is believed that plaintiff is also a technology company; could be an Internet Service Provider (ISP), a cloud provider or something of the sort.[115]

In 2011, Wikileaks[116] released several US governmental classified documents that were leaked to them by Pfc. Bradly Manning[117]; causing great commotion around the globe and a strong reaction from several governments towards the USA and from the USA to different Service Providers, who, with the purpose of investigating the people responsible of this "attack" and to stop the functioning

[114] See *Doe v Gonzales*. Plaintiff, a Consortium of Libraries challenged the gag order claiming a violation to their first amendment rights. The case ended when the FBI decided to withdraw both, the gag order and the request itself.
Internet Archive v. Mukasey. Plaintiff was a digital Library. Parts reached an agreement and the FBI eliminated the gag order and the NSL.
ACLU. *"National Security Letters*". USA, 2011. Available at: < http://www.aclu.org/national-security-technology-and-liberty/national-security-letters> Consulted on February 18, 2012.
[115] Zetter, Kim. "Unknown Tech Company Defies FBI in Mystery Surveillance Case." Wired, Privacy, Crime and Security Online, 2012. Available at: < http://www.wired.com/threatlevel/2012/03/mystery-nsl/> Consulted on March 25, 2012.
[116] Wikileaks is " a not- for – profit media organisation" that has as main objective "to bring important news and information to the public" obtained through "sources that leak information to their reporters". Wikileaks. Available at:< http://wikileaks.org/About.html>
[117] Singel, Ryan. "*Twitter's response to Wikileaks Subpoena should be the Industry Standard*". Wired, 2011. Available at: < http://www.wired.com/threatlevel/2011/01/twitter/>

of the means used for communication and financing of the organization, were subpoenaed.

As a result of such measures, "Twitter" was served with an FBI subpoena[118] in which it was required to hand in information, such as subscribers' names, their contact information, session times, length of service[119], etc, regarding "a number of people connected to Wikileaks, including founder, Julian Assange, accused leaker Pfc. Bradley Manning…"[120] and other people allegedly, part of the organization (such as dutch activist Rob Gongrijp, and a member of the Icelandic Parliament Birgitta Jonsdottir).[121]

Twitter went to Court looking to suppress the gag order of the subpoena, in order to be able to make its users aware of the existence of the subpoena, so they could challenge it by themselves.

Surrounding what happened with Wikileaks, particularly at that time, it is easy and probably not incorrect to assume that Twitter was not the only provider that received a similar subpoena, but it certainly was the only one to challenge it.

Twitter has a "policy of notifying a user before responding to a subpoena, or a similar request of records. That gives the user a fair chance to go to Court and try and quash the subpoena."[122]

Concerning the second case, earlier this year a document was filed against an NSL. It is only known at the moment, and due to the gag order requirement,

[118] The subpoena was issued under provision of the US Code: 18 USC § 2703, "Required disclosure of customer communications or records".
[119] Wittacker, Zack. *"Wikileaks: Homeland Security invoques Patriot Act on Assange; seeks server data."* ZD Net, USA, 2011. Available at: < http://www.zdnet.com/blog/btl/wikileaks-homeland-security-invokes-patriot-act-on-assange-seeks-server-data/55950>
[120] Singel, Ryan. Op.cit.
[121] Kane, Muriesl. "*Judge rules that Twitter must hand over information on Wikileaks supporters*". The Raw Story, 2012. Available at: <http://www.rawstory.com/rs/2012/01/06/judge-rules-that-twitter-must-hand-over-information-on-wikileaks-supporters/> Consulted on February 20, 2012.
[122] Ibid.

that the company challenging the NSL is a provider of communication services in the US with employees in several countries around the world. [123]

The aim of this company is, again, to eliminate the gag order, to be able to notify its customers about the request of disclosure of their data, so they can proceed as they deem necessary.

So far, documents have been written in such a way as to maintain secret the name of the company, the information requested and people involved. [124]

If Cloud Service Providers are really interested in having customers that trust their services and even in attracting new users; they should follow the example set by the providers that initiated the cases explained herein.

By setting in their contract with users a guarantee that they will be notified of any order requesting disclosure of some of their data not containing a gag provision; and for those with a gag order, that at least they will challenge the secrecy part to try to eliminate it and be able to notify them; then security in that cloud would increase dramatically.

At the time being, this seems to be the most adequate solution for combating governmental orders, such as NSL's, that infringe people's basic rights and also that greatly affect the growing business of cloud computing.

2.8 Conclusions

- The USA PATRIOT Act, even if highly controversial, is a piece of legislation that is here to stay because even when the specific circumstances that originated it have disappeared, Congress, and in general the US government are pleased with the prerogatives contained in it that, among other things, allow them to gather information in several ways.

[123] Zetter, Kim. *"Unknown Tech Company Defies FBI in Mystery Surveillance Case".* Wired, 2012. Available at: < http://www.wired.com/threatlevel/2012/03/mystery-nsl/>
[124] Ibid.

- Sections analyzed in this chapter, are all applicable to cloud computing through requisition of data to cloud providers.

- Five sections that allow the use of three different instruments were analyzed.

Section 210. Regarding subpoenas for records of electronic communications (no content data), for which it is necessary to go to Court to have them issued. This means that there are some requirements to fulfill, such as to have reasonable grounds to believe that data seek is relevant for the investigation. Immunity is granted for providers that disclose information.

Section 212. Is about orders seeking to obtain content data from remote computing services. It is also necessary to go to Court and to comply with the same requirements as in the previous section. Immunity applies as well.

Section 215 and 218. FISA orders. These are issued by a specific Court, the FISC, and relevancy of data for the investigation regarding a foreign person also needs to be proved. Its purpose is to gather data (content data) for investigations in which is necessary to obtain foreign intelligence information. There is a non disclosure provision or gag order for recipient and immunity applies too.

Section 505. National Security Letters. There is no need to have the approval of a Court; the FBI can issue them at will but there has to be a connection between the investigation and the data sought to obtain. NSL's are addressed to wire and electronic communications providers. They cannot be used to acquire content data. NSL's have a permanent and strict gag order for recipients, and there is also immunity for compliant providers.

- Since NSL's infringe the First and Fourth Amendments of the Bill of Rights, that contain the freedom of speech and the right to be protected against unreasonable searches, in 2004 the first case against an NSL took place. Since that moment, some other complaints have been presented.

- Thousands of NSL's are issued every year; is the instrument used the most by US authorities.

- Data obtained by the FBI through the issuance of NSL's are further disseminated to other agencies, in accordance to Attorney's General Guidelines and information sharing agreements.

- At the moment, the best way to combat NSL's is to set an industry standard consisting on the challenge of the gag order of each of the letters by service providers; to be able to communicate their customers about the existence of the letter so they can act accordingly.

Chapter III

European Data Protection Legislation

3.1 Introduction

The purpose of this chapter is to provide a general overview of Data Protection Legislation in Europe, to be able to analyze how serious US governmental access to data can be, from a European perspective, which is also comparable to the vision other countries[125] have, due to their similarities in regulation and in the importance given to privacy issues and data protection.

This chapter is not intended to provide an exhaustive analysis of European law on the matter, but rather it is just a showing of the most relevant parts of legislation useful for the purpose of this dissertation, which is to assess if service providers can prevent disclosures of data to the government.

3.2 Privacy and Data Protection Directives

As a starting point of the examination of European Law, it is necessary to state that a Directive is a legal instrument of the European Union in which specific results to be accomplished by the Member States are set. It has priority over national law and is binding for national authorities, who need to implement Directives on their own terms and chosen way within a certain amount of time.[126]

In particular, this Directive is different to other Directives because it is a long-arm statute[127], in other words, its provisions have a long reach spectrum of applicability, even when it has to be implemented by the Member States first.

---

[125] Countries like Canada, Australia, Argentina, Sweden, etc. See: Greenleaf, Graham. *"76 Global Data Privacy Laws*". Privacy Laws and Business, 2011. Available at:<http://ssrn.com/abstract=1946700> Consulted on May 25, 2012.

[126] European Commission. *"What are EU Directives?"* European Commission, 2011. Available at: < http://ec.europa.eu/eu_law/introduction/what_directive_en.htm> Consulted on June 12, 2012.

[127] Long-arm statute. A statute providing for jurisdiction over a nonresident defendant who has had contacts with the territory where the statute is in effect. Garner, Bryan. Op. cit. p. 428.

At this time, regarding the matter of study, it is important to notice that Data Protection has been recognized as a human right in the European Convention for the Protection of Human Rights (ECHR). This fact shows the importance that is given to this matter in Europe.

In the first chapter the definition of "personal data" provided by this Directive was cited and explained; therefore, now we only have left to clarify other complementary but basic terminology used in the Data Protection Directive (DPD):

> "**Processing** of personal data ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction…"[128]

Moreover, processing needs to be fair and lawful, with legitimate purposes, adequate, relevant, not excessive, accurate, up to date and kept in a form in which data subjects can be identified just for the time needed for the purposes of the processing.[129]

> **"Controller** shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law…

[128] Article 2, Data Protection Directive 95/46/EC
[129] Ibid. Art.6

> **Processor** shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"… [130]

The importance of determining who the processor and the controller are derives from the obligations and liabilities appointed to them. Controllers are the ones in charge of the implementation of appropriate security measures to protect personal data;[131] processors may solely act under instructions of controller.

For this reason, controllers are forced to compensate for damages suffered as a result of an unlawful processing operation, and they can only be exempted from this liability if they manage to prove that the damage was not generated as a result of their actions.[132]

When talking about Cloud Computing, to make the distinction between controller and processor becomes difficult due to the multiple possibilities this system has to offer and the different types of clouds and services available. At times, it would seem that the data subject or consumer is the controller because is the one that "determines the purposes and means of the processing"; while cloud provider might as well be the processor.

Nonetheless, it is also the case that the role played in such relationship shifts when circumstances change, and so, for example, both, provider and costumer can be controllers because providers normally determine the means of the processing (hardware, software, data centers…) while consumers determine the means by choosing a particular cloud provider, its services and tools[133].

---

[130] Ibid. Article 2.
[131] Ibid. Article 17.
[132] Ibid. Article 23.
[133] Hon, Kuan et.al. *"Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part II".* Queen Mary University of London, Legal Studies Research Paper No.77/2011, 2012, p. 10. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130> Consulted on April 29, 2012.

Others argue that as in cloud computing provider's function can also just be to supply consumers with the functionality or infrastructure needed and they do not decide what to do with data nor process such data; in this scenario, cloud consumers are controllers and processors of their own data at the same time.[134]

To avoid reaching a controversial and sometimes acrimonious debate, we will just state that in the case of governmental access to data, fortunately roles can be defined. When providers are asked to disclose personal data of consumers, if they do not have data subject's consent, and comply and disclose data, they become controllers and processors at the same time with regard to said data. From now on, we will focus our attention in this scenario.

As we will see later on, the above means that Cloud computing providers, when disclosing data, are breaching the DPD and are liable for damages that result as a consequence of such infringement.

After the definitions, Directive further specifies the rules governing data transfers, both, within the EU and to third countries. For transfers outside of the EU, the third country has to ensure an adequate level of protection, which shall be assessed by the Member States, taking into consideration all circumstances surrounding the transfer and the laws of the country that will receive the data.

If the third country fails to ensure the required level of protection, then, the transfer can still take place, provided that Member States corroborate either that the data subject has given free consent for the transfer; that controller guarantees adequate safeguards for personal data; that the transfer is necessary for performance of a contract or its conclusion; that is required on important public interest grounds or to protect vital interests of data subject.[135]

[134] Ibid.

[135] Article 26. Data Protection Directive 95/46/EC.

The transfer would also be possible between a company in the EU and another one outside, if EU Standard Contractual Clauses are followed.[136]

When talking specifically about data transfers to the US, as this country does not have an adequate level of data protection, in accordance to the European Union, data transfers can be done if following the previously specified options for situations of this kind; or by two more possibilities.

The first one is for the entity that wants to receive the data, to comply with the Safe Harbor Principles. "The Safe Harbor Framework allows U.S. organizations to satisfy the Privacy Directive's requirements regarding, amongst other things, adequate protection. Until now, no U.S. Authority has adhered to the Safe Harbor Principles."[137]

The second way, similarly to the one explained, is with the use of EC Model Agreements, which are instruments previously approved by the European Commission and that work as a guide for drafting other agreements; in this kind of contracts, liability is shared between the parties. So, an EU company that wants to export data has to enter into an Agreement based on the EU Model with a US authority, but this normally requires as well, the permission of the Data Protection Agency of the Member State transferring the data.[138]

Albeit data transfers to third countries are possible, companies, and in our case of study, cloud computing providers, need to fulfill a series of requirements and security measures in order to assure that the data to be transferred will enjoy the same level of protection, or otherwise, such transfer cannot take place.

However, it is normally the case that US providers set in their agreements with consumers that in order for services to be adequately provided, transfers of

---

[136] Moerel, Lokke. *"Binding Corporate Rules: Corporate Self- regulation of Global Data Transfers*." Chapter 7, Oxford University Press, 2011, p.210.
[137] Moerel, Lokke, et. al. "*U.S. Subpoenas and European Data Protection Regulation*". Privacy and Data Security Law Journal, 2009, p. 654
[138] Ibid. p. 655.

data between all their servers would have to take place, independently of their location. In this situation, it can be argued that consumers consent to those transfers since providers inform them of this necessity, in a clear and correct manner. The same would apply when consumers hire EU providers with databases in the US and they know transfers to the latter country need to take place.[139]

Going back to the topic that concerns us, data disclosures to the US government, when trying to assess legitimacy of the processing of data, there are three criteria from the Directive that can be useful to determine whether or not compliance with US subpoenas[140] is possible under European regulations:

1.- "The individuals involved have provided their unambiguous consent;

2.- The data processing is necessary for compliance with a legal obligation that applies to the company; and

3.- The data processing is necessary for the legitimate interests of the company, unless the right of privacy of the individuals involved prevail."[141]

Regarding the first criteria, as I mentioned before, in order for consent to be valid, it needs to be given for specific purposes (in this case, compliance with subpoena) based on clear and complete information, and free. It is not likely for providers to obtain consumers' consent, especially if is the case that the subpoena has a "gag order" included that prohibits the revelation of the existence of such document.

In relation to compliance with a legal obligation, even when it would seem that the Directive allows disclosure of data with this purpose, in an opinion of

[139] In order for this to be true, it is desirable to determine whether or not consent can be considered to be given freely when talking about contracts of adherence.
[140] Here, by subpoena it should be understood a criminal or administrative subpoena with basis in different statutes, PATRIOT Act included.
[141] Moerel, Lokke. *"U.S. Subpoenas and European Data Protection Legislation"*. Op. cit. p. 652.

Working Party 29, it considered that this legal basis applies only if the processing serves to comply with European laws.[142]

As to the third criteria, compliance with subpoenas would not be possible unless data is anonymize and pseudonymized; this, because the right of privacy prevails. Proportionality and subsidiarity have to be taken into account as well.[143]

There are also obligations for providers that wish to meet the terms of an US subpoena. To start, they have to inform all people involved, prior to compliance, about the purposes of the processing of their data, and all other relevant information, including the level of protection their personal data would have. Besides the above, the provider company must take all measures within its capability to protect the data requested by a subpoena.[144]

For all of the above, up until now, it is not possible to comply with a U.S. subpoena without an immediate violation to European laws.[145]

Even though there are more Directives on the matter, with all of the explained in this chapter, we can see that European legislation regarding protection of data is strict and protective of the rights of European people.

Now, in case of breach of the content of Directives, sanctions may be in place but their determination is left for each Member State to decide. They normally would consist in economic fines and civil liability.

At this point, when comparing the content of this chapter and the previous one, the clash between legislation of the US and Europe becomes apparent. The US government is authorized to request for data disclosure through various ways, and they actually use their instruments to do it. Under this panorama,

[142] Ibid. p. 653.
[143] Ibid.
[144] Ibid. p. 656.
[145] See Ibid. p. 657.

cloud providers that for whatever reasons must comply with both legislations, find themselves into a disjunctive regarding the appropriate way to act.

Hence, by logical deduction, in the process of reaching a decision, they will consider the capabilities of enforcement, the sanctions they may be subjected to, but more importantly, the possibility of complying with US legislation, without European authorities realizing their breach of European laws.

This option is originated due to the characteristic that especially National Security Letters and FISA orders have regarding the "gag order" or non disclosure requirement; meaning that if they do not notify the data subject or European authorities, and do not challenge the order, their disclosure of data would remain secret indefinitely. Furthermore, even if European authorities come to realize the violation of the law, proving disclosure of data to which providers already have access to, would be an incredibly difficult thing to do.

Since this has been going on for years, in the proposal for a new Data Protection Regulation, drafters of the text, trying to directly forbid the continuance of this provider's behavior, included a provision where it was specified that "the transfer of personal data based on orders or requests from non-EU Courts, tribunals, administrative authorities, and other governmental entities, unless mutual legal assistance treaties or procedures under international agreements were followed, or unless the relevant DPA had approved the transfer…"[146] was forbidden.

At the end said provision was deleted but it is expected that the same restrictions on data transfers will be incorporated into a Recital of the final version of the text.[147]

[146] Kuner, Christopher. *"The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law."* Bloomberg BNA, Privacy and Security Law Report, 2012, p. 10. Available at: < http://www.huntonprivacyblog.com/wp-content/uploads/2012/02/Kuner-EU-regulation-article.pdf> Consulted on June 6, 2012.
[147] Ibid.

Furthermore, sanctions were specified and they would consist on administrative fines for data protection violations that could be for up to 2% (two per cent) of the worldwide annual income of a company.[148]

3.3 Conclusions

- European Legislation protects Data as a human right and provides for safeguards for the processing of data.

- Transfer of data to other countries is possible when following the requirements established to that effect in the European Data Protection Framework.

- In Cloud Computing is difficult to distinguish who controllers and processors are since it depends on the role played by each stakeholder in a given set of circumstances.

- For the time being, it is not possible to comply with a request for disclosure of data sent by an American authority (or from any other country) without violating European laws.

- Cloud providers may take advantage of the “gag order” contained in some governmental requests, to comply with US legislation without awareness of the data subject or European authorities.

- By setting more stringent sanctions in a proposal for a new regulation, Europe will try to face the problem of disclosure of data to foreign governments.

[148] Ibid. p.2.

Chapter IV

Jurisdiction and Governmental Access to Data in the Cloud

4.1 Introduction

As we saw in the second chapter, in the USA there are various mechanisms that can be used to acquire data from its citizens or from foreigners that have some connection with it. Although not always, in general, governmental agencies that want to use these mechanisms have to justify their use before a judicial authority, which is responsible for safeguarding the interests and rights of people.

Normally, all governments are able to collect data for security purposes but what can be different is that each State has a particular set of mechanisms and specific requirements for their use.

In order to understand all the implications that the use of such instruments have and why it is a subject of dispute these days, some concepts that need to be defined first are explained in the following pages.

4.2 Jurisdiction gets cloudy in the cloud

Nowadays, due to the development of new technologies, privacy and data protection are acquiring significant importance, probably more than ever, because of the threats these represent to individuals' rights.

As communications normally work through an open network, the internet, that has no borders and can be accessed from anywhere in the world, States are finding every time more difficult to protect their population's privacy, within its territory, and particularly in the international sphere. Hence in new legislation on the said matters we can see a tendency in which extraterritorial application

is sought as an attempt to address this problem.[149]Before explaining what this means, is important to bear in mind other concepts that are defined below.

Jurisdiction is a legal term that can be understood as "A government's general power to exercise authority over all persons and things within its territory"[150] or, it can also refer to the "entity's authority to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things…by legislation, by executive act or order, by administrative rule… or by determination of a court."[151]

Both definitions had their origin in the principles of territoriality and nationality that are the basis for a correct understanding of jurisdiction. We have then, concerning the territoriality principle, that this power is primarily exercised in a certain territory where the State has sovereign or exclusive jurisdiction over people that live there, companies established there or that carry out activities on that territory, as well as over individuals that at a given moment are physically located there; which means that all of them are subject to its authorities and applicable laws.

It should be noted thought that internationally speaking, "one state's exercise of sovereign power cannot infringe upon the sovereignty of another state or states" (equality of States doctrine).[152] For this reason, the idea of enacting long arm statutes[153] or laws with extraterritorial reach conflicts with international law, since more often than not, the State applying the long arm statute would interfere with the sovereignty of another one. In addition, enforcement is difficult to achieve because no State should enforce its laws

[149] Svantesson, Dan. *"Protecting Privacy on the Borderless Internet: Some thoughts on Extraterritoriality and Transborder Data Flow*". Bond Law Review, Vol.19, Iss.1, Article 7, 2007, p.3. Available at: <http://epublications.bond.edu.au/blr/vol19/iss1/7> Consulted on March 3rd, 2012.

[150] Garner, Bryan. *"Black's Law Dictionary*". Second edition, West Group, Minnesota, 2001, p. 383.

[151] Brenner, Susan; Koops, Bert- Jaap. *"Approaches to Cybercrime Jurisdiction".* Journal of High Technology Law, V. 4, N.1, 2004, p. 5.

[152] Scassa, Teresa; Currie, Robert. *"New First Principles? Assessing the Internet's Challenges to Jurisdiction".* Georgetown Journal of International Law, 2011. Available at: < http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF> Consulted on March 20, 2012, p. 1025.

[153] A Long arm statute is a statute providing for jurisdiction over a nonresident defendant who has had contracts with the territory where the statute is in effect. Garner, Bryan. Op. cit. p. 428

upon the territory of another State, unless there is clear legal authorization for it. This extends to investigations and jurisdiction over a person.[154]

To further clarify this concept, it can also be said that extraterritorial jurisdiction is "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under International Law."[155]

What is more, International Public Law "prohibits an act by one State in the territory of another State which only State officials (as opposed to private individuals) may perform."[156] This could be the case of acquiring data for purposes of investigations.

Regarding, the nationality principle, this one "allows the state to exercise jurisdiction irrespective of the territory where the act was committed because of the nationality of the actor (active nationality principle) or because of the nationality of the victim (passive nationality principle).[157]In other words, a State "may assert jurisdiction over the acts of their nationals, wherever the act might take place."[158]

Besides the two principles mentioned, there is yet another way to determine jurisdiction, and it is important for the matter at hand because is mostly used in the US since it derives from case law, and is based on the concept of "minimum contacts". To establish whether or not a business has minimum contacts with the US, there has to be a test or analysis of all the activities of the company, and if such company benefits somehow from US legislation, then the US would have jurisdiction over it. This connection cannot be based

[154] See Scassa, Teresa; Currie, Robert. Op.cit. p. 1028.
[155] Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet. Part 2.". International Journal of Law and Information Technology, Vol. 18, No. 3, Oxford, 2010, p. 1. Available at: < http://ijlit.oxfordjournals.org/content/18/3/227.full.pdf> Consulted on March 28, 2012.
[156] Ibid. P.8.
[157] Timofeeva, Yulia. "Worldwide Prescriptive Jurisdiction in Internet content controversies: A comparative analysis." Connecticut Journal of International Law, Vol. 20, USA, 2004, p.4.
[158] Scassa, Teresa. Op.cit. p. 1027.

on a company selling products on US soil and profiting from it, there has to be a more direct linkage.[159]

Among the consequences of being under US jurisdiction is that the government can ask for the production of business records that are under the company's "possession, custody or control". Due to this idea, the US can request this kind of documents in relation to the company that was found to have minimum contacts, and also to that same company but regarding others to which the first one might have documents under control.[160]

Furthermore, it is considered that a company has control over another one when the parent company has shares in a subsidiary or affiliate, when the parent has control over the management and/or employees of the other company, or if the parent company would benefit from litigation in case of non-disclosure of the records. [161]

When talking about Cloud Computing, even when there are certain things that can be framed into the definitions mentioned, there are others, like the transferring of data and governmental access to data that are more difficult to enclose.

As we know, for cloud computing to work properly, it is necessary to transfer data from different servers and data centers that can be located anywhere on the globe. Such transfers are known too as trans- border data flows because it means that there are "movements of personal data across national borders"[162].

---

[159] Waage, Torben; et.al. *"Government access to Information in the cloud"*. Kromann Reumert, Denmark, 2012, p. 8. Available at: < http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf> Consulted on May 29, 2012.

[160] Ibid. P.8.

[161] Ibid. p.8.

[162] OECD. "*Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data*". Art.1 (c). Available at: < http://www.oecd.org > Consulted on May 22, 2012.

In each trans-border transfer, it is expected that personal data would be subject to more than one jurisdiction, meaning that several privacy and data protection laws may apply, due to the fact that as its location changes, it can be accessed by governments in which servers are located; making it very difficult for providers to comply with all different regulations.

So far, as already stated, it seems that what is common practice among cloud providers is to comply with legislation of the State with better enforcement mechanisms and more penalties in case of non compliance.[163]

Before going there, it is important to analyze in parts the system of Cloud Computing, in order to realize how jurisdiction affects each of them and how this relates to governmental access to data.

Concerning cloud **service providers**, we need to consider multiple factors. First, the State in which a company is seated is often the provider's main place of business; and if following the two principles that are being discussed, the provider would then be located within the limits of this State (territoriality) and, at the same time, it would be a national of that country (nationality)[164]. This means that service provider is, in the first place, subject to all regulations of the country of incorporation.

Now, if we consider that providers normally have agreements with other corporations in charge of either processing, connectivity through a network or of providing other functionalities, jurisdiction problems begin to show.

[163] See Kuner, Christopher. *"Data Protection Law and International Jurisdiction on the Internet. Part II."* Op.cit. p.12-14.

[164] "Even when this principle is mainly used in criminal law, there are examples of it being applied to civil law… (It) is used as the basis for jurisdiction in a number of areas… an example of the personality principle in data protection law is provided by Greek law. See: Kuner, Christopher. *"Data Protection Law and International Jurisdiction on the Internet. Part I."* International Journal of Law and Information Technology, Oxford University Press, Vol. 18, No. 2, 2010, p.188. Available at: <http://ijlit.oxfordjournals.com/> Consulted on March 23, 2012.

If these intermediaries or cloud carriers have the same nationality and are located in the same place as the cloud provider, then there would be no problem since all of them fit into the same jurisdiction.

However, if cloud carriers are located in the same or another State and were incorporated in yet a different one, then the jurisdiction of both countries would apply to them. What this would mean for the cloud provider, if we go back to *the "possession, custody or control"* of documents theory, is that cloud carriers could be asked to disclose records of provider under their control. This also works vice versa; provider may disclose data of cloud carriers.

Now, cloud service providers can have branches or subsidiaries/affiliates (normally the latter). A **branch** is "an offshoot, lateral extension, or division of an institution".[165] It is not a separate legal entity[166]; hence it does not have an independent personality. All its responsibilities and liabilities are part of the parent corporation.

In the case of a parent company being located within the US, and with branches in Europe, then each branch would be under American jurisdiction and under the one of the country of location. Assuming the parent company is requested to provide data regarding a European branch, then the parent would have to comply, since it is the same entity and the parent has complete control over its branches.

But, there would be a breach of European regulations because data from the EU branch, having data from European citizens, would be processed. This would mean that the branch in Europe violated European laws and it would be liable for that. In this scenario, liability would be assumed by the entire corporation: parent and branches.

[165] Garner, Bryan. Op.cit. p.76.

[166] See: Working Party 29. *"Opinion 10/2006 on the processing of personal data by the Society of the Worldwide Interbank Financial Telecommunication (SWIFT)."* WP29, 2006, p.21. Available at: < http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm> Consulted on May 24, 2012.

Subsidiaries, on the other hand, are corporations in which provider (Parent Corporation), owes a controlling share[167]. They are a different entity and have their own legal personality different from the one of the parent; hence liabilities are as well separated.

Concerning territoriality, parent corporation is under one jurisdiction, and its subsidiaries, located in countries x and y, would give jurisdiction to each of the countries of their location.

Even when subsidiaries are different legal persons, as the majority of shares of subsidiaries are controlled by the parent, due to the existing property-related link between them, the State of the parent corporation would too have jurisdiction over its subsidiaries located in countries x and y. This because, as set in the definition of jurisdiction, the power of an entity also refers to "the interests of persons in things".

As a result of the above, if either a parent company or a subsidiary is requested to produce data by US authorities, the same situations as explained with respect to a branch would apply.

In relation to provider's **data centers**, jurisdictional issues would be somehow similar to the ones for subsidiaries and branches. Location is important because States can assess jurisdiction over their territory, and as data centers are property of a provider, even if data is not physically located within the company, is considered to be under its control, possession and custody. This fact gives jurisdiction as well to the State of provider's incorporation, when located in a different country.

It is important to consider where data centers are because is common practice among cloud providers, to have data centers with countless servers, in places where they can get the most of their investment. Consequently, they take into consideration the costs of buying land, power supply and its affordability, capacity for high-speed internet connections, weather, taxes, criminality and of

[167] Garner, Bryan. Op. Cit. P. 149.

course, laws and regulations of the country. To this last respect, how intrusive a government can be is also to be taken into account. [168]

Regarding cloud **consumers**, there are also a number of issues to be examined. Due to the connection of nationality, a State has jurisdiction over its nationals, whether if they live in the State's territory or even if they are abroad.[169]

For purposes of the following analysis, consumers are enclosed in three large categories: individuals, legal persons or businesses and governments.

Individuals, for instance are under jurisdiction of the country of their nationality. When they are in another place then the State of their location also has jurisdiction over them. Regarding their relationship with cloud providers, this one is normally based on a contract that is set by provider, it cannot be negotiated and therefore no changes are allowed. As in most of this kind of agreements, individuals either sign the contract or otherwise they cannot make use of the services provider offers. They could only change this situation if they can influence provider or if their requirements and needs are significant for provider's business.

As to governmental access to data, they obviously suffer the consequences if their provider chooses to disclose their data, and if so, they could ask provider for compensation. As established in the second chapter, NSL's are often used to get individuals data, such as in the case of "Wikileaks" or Doe v. Ashcroft.

Yet, to enlarge the range of possibilities, even when people cannot receive NSL's or FISA orders, they could be subpoenaed in order to disclose data as well. So, if it was the case that an employee of a cloud provider received such

[168] Jaeger, Paul. "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. First Monday Journal, Vol.14, No. 5, 2009. Available at: < http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2456/2171#p4> Consulted on February 2nd, 2012.

[169] Lecours, Alain. "USA Patriot Act". The legal Insider, Canada, 2006. Available at: < http://www.lecourshebert.com/Extraterritorial-Effects-of-the-USA-Patriot-Act.html> Consulted on March 17, 2012.

an order, if they were to comply with it, data to which they could have access to or under their control could too be leaked to US authorities. Since this is not the topic of this dissertation we will not go further on this scenario.

For **Legal persons**, especially if they are large businesses, governmental access to their data is more troublesome since data of great importance such as Intellectual property, financial information and all business' activities can be in the cloud and if disclosed, it could cause serious problems to corporations.

Businesses, as we saw with cloud providers, would first be under jurisdiction of the country of establishment. If they have subsidiaries or branches, then the country of their location as well as the one of the incorporation of the parent would have jurisdiction.

Concerning governmental access to business data in the clouds, we saw that it is a reality and businesses can find themselves in the same situations that individuals on this matter but probably vulnerable to more jurisdictions.

It seems that some enterprises beware of the dangers of the PATRIOT Act and of being submitted to the US jurisdiction when their only connection with this country is the cloud provider; for this reason, some have declined hiring US providers or have terminated their agreements with them, even if their services and prices could be more competitive than providers within the EU. A situation like this took place last December with a UK Company named "BAE Systems" that ended negotiations with Microsoft because they could not give assurance that their data was not to be accessed by the US.[170]

It is very interesting the scenario of **Governments** hiring cloud services. As with businesses and individuals, if governments hire a foreign cloud service provider, their data would be exposed to the jurisdiction(s) provider is under.

[170] Mandalia, Ravi. "BAE Systems Abandons Microsoft Cloud Plans Citing Patriot Act". IT ProPortal, 2011. Available at: < http://www.itproportal.com/2011/12/08/bae-systems-abandons-microsoft-cloud-plans-citing-patriot-act/> Consulted on January 21, 2012.

Since governmental data can be very sensitive it is not desirable for any country to be spied on by another.

Governments have already come to realize this situation and the consequences it could have on their sovereignty; therefore some have opted to forbid their agencies, ministries and in general all the governmental structure hiring and external cloud provider, especially from the US. [171]

Despite all of the above, we should keep in mind that States not only need to respect the privacy of personal data of its nationals, but also, as other rights (freedom, equality, etc) they have to guarantee it. This represents a problem in reality because as we saw, a lot of countries, like the US, under national security or counter terrorism pretexts try to access as much data as possible, but at the same time, States are attempting to limit the export of data of their own countries or geographical regions by enacting laws with extraterritorial application.

As data of more and more people are in the clouds, governments try to assess jurisdiction over providers, because then, one of the instruments explained in chapter two or some others that are also available are used to access such data.

But, if there is no link between the State and the provider that could lead the former to have jurisdiction over the latter, then such instruments, at least in theory, are not bound to succeed and they would be seen just as requests for voluntary disclosure of data.

[171] See Whittaker, Zack. *"Dutch government to ban U.S. providers over Patriot Act concerns*". ZD Net, 2011. Available at: < http://www.zdnet.com/blog/btl/dutch-government-to-ban-us-providers-over-patriot-act-concerns/58342> Consulted on March 12, 2012.
See Gallagher, Sean. "*PATRIOT Act and Privacy laws take a bite out of US cloud business"*. Arstechnica, Law and Disorder, 2011. Available at: < http://arstechnica.com/tech-policy/2011/12/patriot-act-and-privacy-laws-take-a-bite-out-of-us-cloud-business/> Consulted on January 30, 2012.

In either of these situations, service providers become controllers[172] of their customer's data and they have the last saying regarding its disclosure, notification to the real data owners or, if it is just a voluntary request, its denial.

In practice, as seen before, the USA, country that is being studied in this dissertation, has been using its judicial powers over American providers (that at the moment are the strongest ones and with data of people from all over the world), to access not only data of its nationals, but also from foreign citizens with whom the only connection it has, is the cloud provider.

Furthermore, this problem is accentuated with branches and subsidiaries that even when located in other countries, would comply with the PATRIOT Act and disclose data from all their customers, employees, etc., whether American nationals or not, since this piece of legislation belongs to the country of jurisdiction of the parent corporation and it is a long- arm statute.[173]

In the subsequent years to the terrorist attacks on US soil, other countries have as well enacted regulations to fight terrorism and in which mechanisms similar to the American ones have too been created.[174] This could be due to either, a real concern towards terrorism or, we could think that these were enacted to somehow have the same capabilities that the country setting the example.

As we can see, all of this means that due to the nature of the cloud in which it is necessary to transfer data between data centers, some States can have jurisdiction even beyond their territorial limits; extraterritorial jurisdiction.[175]

---

[172] Hon, Kuan. *"US Patriot Act- Can UK cloud customers use US cloud providers?* "Computer World UK, 2012. Available at: < http://blogs.computerworlduk.com/cloud-vision/2012/05/us-patriot-act---can-uk-cloud-customers-use-us-cloud-providers/index.htm> Consulted on June 1st, 2012.

[173] Miller, Paul. *"Microsoft, the USA PATRIOT Act, and European Cloud Computing"*. Paul Miller the Cloud of Data, 2012. Available at: < http://cloudofdata.com/2012/01/microsoft-the-usa-patriot-act-and-european-cloud-computing/> Consulted on February 17, 2012.

[174] See Reumert, Kromann. Op.cit.

[175] Ibid. P. 383

As it is not uncommon for States to require cooperation from other States in various matters, and particularly concerning security, there are other international mechanisms that have been implemented with the objective of allowing cooperation between different legal enforcement agencies. These instruments are called Mutual Legal Assistance (MLA) arrangements.

Despite their possible benefits, MLA's are known to be ineffective in matters in which timing is of the essence, due to their complexity and bureaucratic procedures involved.[176] This is why, when referring to cloud computing and other new technologies, countries are implementing new methods that are far more effective but, as seen before, tend to violate basic concepts of International Law.

4.3 Analysis of Scenarios

Having now a clear idea of how jurisdiction may work in relation to Cloud Computing, it is time to focus on the scenarios that were proposed on the first chapter, to see in which cases the USA PATRIOT Act would apply or how its application can be avoided.

Scenario	Provider	Subsidiary	Data center	Customer
First	American	None	America	European
Second	American	European	Europe	European
Third	European	None	Europe	European
Fourth	European	None	Europe	American
Fifth	European	American	America	Both
Sixth	European	American	Europe	Both

[176] Walden, Ian. "*Accessing Data in the Cloud: the Long Arm of the Law Enforcement Agent".* Queen Mary University of London, UK, 2011, p. 11. Available at: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067> Consulted on April 17, 2012.

First. - In this case, since both, provider and data center are Americans, the regulations that apply are the ones from the US; hence the USA PATRIOT Act applies.

Second. - This scenario is the one that has caused more conflict around the world because it proves that clouds are unsecure when talking about disclosure of data to foreign governments.

Even when a subsidiary is located in Europe, with data centers also in Europe, but from an American provider or parent company, NSL's and any other instruments can be served upon the subsidiary and this one would be compelled to comply. Besides, the parent company can also be asked to disclose information and as it is directly under US jurisdiction it would have to make the disclosure.

The USA PATRIOT Act applies.

Third. - Since provider is European with data centers in Europe and European customers as well, then the USA PATRIOT Act does NOT apply[177] but the Member States would have jurisdiction, which means that subpoenas and other instruments can still be issued by them.

This scenario can be particularly useful for consumers that wish to limit the number of countries that have jurisdiction over their data, in order to reduce the possibilities of governmental access to it.

Fourth. - In this case, being a European provider with data centers in Europe, the USA PATRIOT Act would NOT apply[178] because provider does not have to comply with US laws but rather European's, and as the Data Protection Directive safeguards not only citizens from the Member States but any natural person, data of Americans shall not be disclosed to the US government,

[177] The US government could still have access to data if it was the case that the US and the EU sign a MLA regarding this topic or if there were an International agreement, but the PATRIOT Act would not apply directly.
[178] Ibid.

unless duly agreed by the EU and the US, which requires more formalities, time and bureaucracy.

This is an interesting situation for Americans that wish to keep their data away from their government, because even when the US has jurisdiction over it and can actually request European providers for its disclosure, if providers follow European Directives, then only the EU agrees would hand in the data.

Fifth. - The USA PATRIOT Act applies. On the one hand, it applies to provider because all its data centers are located in America, and on the other, it applies directly to the subsidiary because it is located in America.

Sixth. - Since data centers and provider are Europeans, the USA PATRIOT Act would only apply to the subsidiary located in the US.

In scenarios 2nd, 5th and 6th, service providers would have a conflict because they are bound by both, US and European regulations.

As we saw, providers have been dealing with this problem by complying with the US and disclosing all data requested through NSL's or other mechanisms. If the new European Data Protection Regulation is modified to leave it as it was in the first draft, regarding this issue, then they would be necessarily facing sanctions from the US or the EU.

4.4 Conclusions

- Jurisdiction can be understood as the power a State has to make its laws applicable and enforceable over persons, activities and things within its territory.

- There are essentially two ways of analyzing whether a State has jurisdiction over something. Through the principles of territoriality, nationality and with the "minimum contacts" test.

- In cloud computing is difficult to assess jurisdiction, especially because normally cloud computing services are subject to more than one jurisdiction.

- States are enacting laws that allow them to have extraterritorial jurisdiction; fact that conflicts with principles of International Public Law.

- Jurisdiction regarding service providers with their corresponding branches or subsidiaries, data centers and consumers were analyzed.

- The findings for each scenario were presented. In all scenarios in which there was some sort of link to the US (except for costumers) the USA PATRIOT Act applies. The Act does not apply when providers, data centers and subsidiaries/branches, if any, are all European.

Chapter V

Recommendations

5.1 Introduction

At this point in which I have addressed the problem concerning governmental access, in particular from the US, to data in the clouds, the reader can come to realize that in order for this situation to change, several measures would need to be followed, since there is no one real solution to the problem.

Given that the USA PATRIOT Act modified some laws to facilitate authorities in charge of security their access to data, now it is easy for them to issue these instruments that go against the right of privacy, data protection, freedom of expression and unreasonable searches of the worldwide population.

Furthermore, making use of this new technology that allows the gathering of data in huge amounts, from anywhere in the world and that can be accessed all the time independently of location, States are avid to have possibilities of exercising their powers even beyond geographical limits; creating an unbalance between States and conflicting with International Law principles.

The purpose of this chapter is to provide some ideas of possible actions that could help find an International solution for this problem.

5.2 Harmonization of International Regulations

Cloud Computing providers are aware of the fact that governmental access to data in their clouds affects their business because it encourages distrust by consumers towards the cloud system.

The USA PATRIOT Act poses such a risk for American cloud providers' business, especially outside of the US, that they have been encouraging changes in this Act to make it more adequate for the international needs and standards.

The example set by Microsoft is remarkable, since it is promoting the creation of a consumer- friendly piece of legislation in the US that would be based on the right to privacy of citizens and would make the clouds "safe and open". This provider is also in favor of a robust international agreement on data protection.[179]

This last idea is, at the moment, an increasing international necessity that would give certainty regarding disclosures of data in the clouds. Certainty not only for providers that do not know with what law to comply but also for consumers that want to know what requirements and procedures authorities need to follow to be able to access their data without easily violating their fundamental rights.

States also have an interest in this kind of regulation because of sovereignty issues and respect to their power. With the creation of a Treaty, instead of having countries enacting regulations with extraterritorial applicability in order to gain jurisdiction over providers, each signing State would enjoy the same possibilities of requesting data disclosure independently of whether they have jurisdiction or not.

Besides, an international agreement would prevent making the cloud ineffective due to more and more regulations and all other restrictions providers need to comply with, or because under consumers' requests they try to avoid be subjected to more than one jurisdiction.

It is an undeniable fact that authorities in charge of security need to be able to access some vital information that could lead them to avoid crimes or detain criminals, but such access should be strictly regulated in order to circumvent abuses in the gathering of data.

[179] Brooks, Carl. *"Microsoft pushes for cloud computing legislation".* Search Cloud Computing, 2010. Available at: < http://searchcloudcomputing.techtarget.com/news/1381303/Microsoft-pushes-for-cloud-computing-legislation> Consulted on January 29, 2012.

The desirable International agreement should, first of all, be binding. Without a real commitment of States, this conduct will continue to take place in the secrecy and mystery with which it has been sustained till now.

The agreement would need to contain unique mechanisms for requests of data disclosure, with specific requirements and characteristics to be fulfilled by governments; among which the authorization from a Court of Justice or an equivalent organ is to be included.

Moreover, circumstances in which disclosures would be permitted should be limited to those compelling and justified by the commonwealth, and in which there is no other way of avoiding a cloud intervention.

As to a “gag order” or non disclosure requirement, this can be left for issues in which disclosure of the existence of an order could compromise a whole investigation; in any case, its effect should last only a short period of time, reasonable for an investigation to go forward but without becoming an overburden on recipient of the order.

By creating these mechanisms with all the characteristics mentioned above, service providers will know what requirements the order need to have for it to be truthful or valid, and with that assurance comply with it.

Despite all of the above, it is true that this kind of agreement is far from happening because the States that are profiting from this access will not be willing, at least any time soon, to compromise their capacity to deal with national security issues as they are now doing it. Also, years have passed since the enactment of the first comprehensive legislation on data protection and even when there have been efforts to harmonize laws; at least between regions, up until now, these have not been successful.

For this reason, it is advisable to follow another one of the recommendations proposed herein.

5.3 Industry Standards and Codes of Best Practices

In the second chapter we saw that Internet Service Providers in the US, cloud providers and other organizations are challenging in Court orders and NSL's with basis on the violation of their constitutional rights; and that so far, the rulings obtained in these cases are positive.

We have also talked about the predicament cloud providers find themselves in when they are subject to more than one jurisdiction; they are served with an order for disclosure from one State, and they need to decide if comply with it or not, knowing that its observance necessarily means a breach of the laws of another country.

Right now, it is up to the provider to decide with what regulations to comply with, in accordance to their business' convenience; scenario that should change and be based instead in a consumer's perspective.

For these reasons, regulation by the industry seems to be a possible way of making clouds more secure. If American providers make it an industry standard to go to Court to challenge the gag order contained in some governmental instruments, especially in NSL's; as rulings so far have eliminated this requirement, then it is likely that they will obtain a favorable resolution and will be able to notify costumers of the existence of such document.

Even when this does not mean that disclosure ultimately will not take place, it does, however, show commitment to security from the side of provider, their disapproval towards this kind of data access, and if successful, they would give data subjects the possibility of challenging the orders themselves.

All of this would acquire more relevance if it becomes a cloud industry standard, at least in the US, where regulations have been most damaging for providers' businesses outside the country.

Besides the explained above, Cloud providers worldwide should agree on certain security principles and acceptable conduct to enhance costumer's privacy and to regulate and set essential safeguards particularly for transborder data flows. Such Code can also contain model clauses to be used by providers in their contracts with costumers.

As the solution to the problem requires conjunction of efforts, setting industry standards shall be complemented with other mechanisms pro- privacy.

5.4 Encryption

One of the most viable solutions to security problems in the clouds is, without a doubt, data encryption and for disclosures by providers it is not the exception.

Providers should be keen of costumers using this method because it would mean they have fewer responsibilities regarding security and privacy of such data. As to requests for disclosures to governments, if data is duly encrypted, then they would have no access to it and no reason or possibilities of complying with this kind of petitions.

There are different ways of encrypting data that can be very useful for external menaces but in most of them cloud providers would still be able to access the data, which means that to avoid disclosure of data to governments, encryption with specific characteristics is needed.

First of all, data encryption has to take place before transferring the data to the cloud, because if it is done once data is in the cloud, providers would know the key encryption and would be able to access it. One way of accomplishing this, is through the use of a "network based encryption proxy[180]" that works as explained in the following lines:

[180] Proxy is "a hardware device that acts on behalf of other devices for purposes such as data storage and security. A proxy server can locally cache frequently accessed documents in order to reduce the level of internet traffic to a remote server. A proxy server also may support a proxy firewall, thereby

> "The proxy is placed on the network and works like a Web gateway. When a user goes to access the SaaS website, they are redirected through the proxy. The proxy relies on deep knowledge of the SaaS application and intercepts key form fields in the webpages. Sensitive data placed in these fields is encrypted before going to the provider, and decrypted before going back to the user."[181]

In spite of its advantages, this system is only available for major cloud needs, meaning that individuals with small requirements cannot make use of it yet. There is, nonetheless, ongoing research to make the encryption system easier and usable in normal basis.

Another way of encryption is called "Searchable and structured". With this kind of encryption a consumer can store data in the cloud and still be able to search over it since a token is generated to allow the search over the encrypted data. [182]

As the latter examples there are some other types of encryption that enhance security of costumers' data and more research is still taking place to create new and better ways of encrypting data. Hence, this would be a good technical solution to the problem.

5.5 Strict Liability for Providers

As seen before, cloud providers that disclose consumer's data and breach the laws of a country by transferring such data to third countries; have not faced a lot of consequences, if any for said disclosures. Therefore, States should do at the moment is to establish provisions in which it is made clear that providers are subject to a strict liability regime if they export data to third countries

---

serving as both a logical and physical barrier. Webster's New World Telecom Dictionary. Wiley Publishing, Indiana, 2010. Available at: < http://computer.yourdictionary.com/proxy-server>

[181] Mogull, Rich. *"Saas Security: Weighing Saas Encryption options"*. Search Cloud Security, 2012. Available at: < http://searchcloudsecurity.techtarget.com/tip/SaaS-security-Weighing-SaaS-encryption-options> Consulted on May 3rd, 2012.

[182] Microsoft Research. *"Cloud Cryptography*". 2012. Available at: < http://research.microsoft.com/en-us/projects/cryptocloud/> Consulted on May 3rd, 2012.

outside of the ways in which this is allowed, making them responsible before data subjects, who could seek redress for compensation of damages.

If providers are liable data disclosures not authorized by consumer, sanctions are heavy and enforcement effective, then providers would be more careful before disclosing data.

5.6 Contracts

In connection with the creation of industry standards and codes of best practices; as well as with the challenging of orders before Courts, if providers commit to consumers by making a privacy friendly contract in which provisions such as going to Court when possible, to be able to notify clients before disclosures take place; are established, then providers with the best safeguards and guarantees would be the ones to retain and gain more clients.

5.7 Conclusions

Even though the problem of governmental access to data in the clouds is complex and, as it involves authorities from different parts of the world that exercise power over providers is difficult (if not impossible) to solve and to avoid; some ideas were herein presented as a guide for finding an integral solution.

These ideas are: Harmonization of international regulation on data protection issues, adoption of industry standards and codes of best practices, strict liability for providers, privacy-friendly contracts with consumers, and especially technological solutions, such as encryption of data.

Concluding Remarks

Nowadays, Cloud Computing has grown so rapidly that it can be considered as a necessity for the functioning of the information technology era as we know it.

As all technological advances, the advantages offered by cloud computing are enormous but it also has important risks to be taken into account. Among such risks, we particularly identified those related to privacy and data protection, in relation to governmental access to data in the clouds.

For the analysis of this problem, six scenarios were set to explain how jurisdiction affects cloud computing stakeholders, and whether or not providers should comply with requests for disclosure with basis in the PATRIOT Act.

Since the USA PATRIOT Act is cause of great concern for cloud consumers in the whole world, and also it is now of concern for US providers since their businesses have been affected with bad publicity of their competitors of other nationalities; in the second chapter this piece of legislation was analyzed. From its background, to its content and specific sections of it regarding the methods the US government can use to request data disclosures and the characteristics of each or them, to later provide some examples of recent case law.

In the third chapter, there was a brief explanation of the most relevant regulation on data protection and some of the basics of its content. This, to realize that by complying with US orders for disclosure, providers that are under US and European jurisdiction, breach European laws.

After that, jurisdiction was explained in general, and then regarding the functioning of cloud computing, to finally see how all of this would apply to the scenarios presented in the first chapter, and how providers can be subject to more than one jurisdiction, which puts them in the position of having to decide with what regulations to comply.

To conclude this dissertation, in the last part it was establish that there is no one real solution to the problem, but rather a combination of steps to be followed in order to ameliorate it. These go from creating an international agreement, to making use of technologies available to protect data in the cloud from all possible types of access, including providers'.

For further research it would be desirable to look into other countries' regulations on privacy and data protection, as well as regarding transfers of data to third countries. Moreover, to make a detailed examination of the legal instruments other governments have to request disclosure of data to providers, the reasons for issuing them and the requirements they need to fulfill in order for the documents to be valid. Additionally, it would also be interesting to know how countries are making use of them.

References

Legislation

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, O.J. L 281, 23.11.1995

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. L 201, 31.7.2002

European Charter of Human Rights

United States Code

United States of America Bill of Rights

Universal Declaration of Human Rights

USA PATRIOT Act

Articles and Websites

Abrams, Jim. "*Patriot Act Extension signed by Obama*". Huff Post Politics, USA, February 2011. Available at: < http://www.huffingtonpost.com/2011/05/27/patriot-act-extension-signed-obama-autopen_n_867851.html> Consulted on January 20, 2012.

ACLU. *"National Security Letters*". USA, 2011. Available at: < http://www.aclu.org/national-security-technology-and-liberty/national-security-letters> Consulted on February 18, 2012.

American Civil Liberties Union. "*Reclaiming Patriotism: A call to reconsider the PATRIOT Act".* ACLU, USA, 2009, p.32. Available at:

<http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf> Consulted on April 02, 2012.

Article 29 Data Protection Working Party. “Opinion 4/2007 on the concept of personal data.” Europe, 2007, p. 6. Available at: <http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm> Consulted on January 25, 2012.

Associated Press. *“Patriot Act Extended for three months*” New York Times, USA, 2011. Available at: < http://www.nytimes.com/2011/02/18/us/politics/18brfs-PATRIOTACTEX_BRF.html> Consulted on January 25, 2012.

Babbar, Muhammad; Chauhan, Muhammad. “*A tale of Migration to Cloud Computing for Sharing Experiences and Observations”*. ACM Press, 2011, 50-56 pp. Available at: <http://www.ics.uci.edu > Consulted on March 03, 2012.

Brenner, Susan; Koops, Bert- Jaap. “Approaches to Cybercrime Jurisdiction”. Journal of High Technology Law, V. 4, N.1, 2004, p. 5.

Bort, Julie. *“The ten most important companies in cloud computing.”* Business Insider, 2012. Available at: < http://www.businessinsider.com/the-10-most-important-companies-in-cloud-computing-2012-4?op=1> Consulted on May 24, 2012.

Brooks, Carl. “Microsoft pushes for cloud computing legislation”. Search Cloud Computing, 2010. Available at: < http://searchcloudcomputing.techtarget.com/news/1381303/Microsoft-pushes-for-cloud-computing-legislation> Consulted on January 29, 2012.

CNN Politics. "*Congress approves extension of expiring Patriot Act provisions*". CNN online, USA, 2011. Available at: < http://articles.cnn.com/2011-05-26/politics/congress.patriot.act_1_lone-wolf-provision-patriot-act-provisions-wiretap?_s=PM:POLITICS> Consulted on February 03, 2012.

CNN Politics. *"House approves PATRIOT Act renewal"* CNN online, USA, 2006. Available at: < http://articles.cnn.com/2006-03-07/politics/patriot.act_1_patriot-act-renewal-controversial-provisions?_s=PM:POLITICS> Consulted on February 03, 2012.

Crime and Federalism. *"Doe v. Gonzales: Disclosure under the Stored Communications Act".* 2006. Available at: <http://federalism.typepad.com/crime_federalism/2006/05/doe_v_gonzalez_.html> Consulted on February 22, 2012.

Dan Svantesson, Roger. *"Privacy and consumer risks in cloud computing".* The computer law and security report vol. 26 (2010) nr. 4, pp.391-397. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364910000828> February 7, 2012.

Dinh, Viet. *"USA PATRIOT Act".* German Law Journal, Vol. 5, Number 5, USA, 2004. Available at: < http://www.germanlawjournal.com/pdfs/Vol05No05/PDF_Vol_05_No_05_461-467_special_issue_Dinh.pdf> Consulted on January 25, 2012.

Doyle, Charles. *"National Security Letters in Foreign Intelligence Investigations: A Glimpse of the legal background and recent amendments*."Congressional Research Service, USA, 2010, p.1. Available at: <www.crs.gob> Consulted on February 10, 2012.

Doyle, Charles; et.al. "*USA PATRIOT Act Sunset: Provisions that expire on December 31st, 2005*." CRS Report for Congress, The library of Congress, USA, 2004, p.1. Available at: < http://www.fas.org/irp/crs/RL32186.pdf> Consulted on February 12, 2012.

Electronic Privacy Information Center. "*Foreign Intelligence Surveillance Act Court Orders 1979- 2011*". Available at: < http://epic.org/privacy/wiretap/stats/fisa_stats.html> Consulted on May 31, 2012.

European Commission. *"What are EU Directives?"* European Commission, 2011. Available at: < http://ec.europa.eu/eu_law/introduction/what_directive_en.htm> Consulted on June 12, 2012.

Fine, Glenn. "A *Review of the Federal Bureau of Investigation's Use of National Security Letters*." US Department of Justice, USA, 2007.

Gallagher, Sean. "PATRIOT Act and Privacy laws take a bite out of US cloud business". Arstechnica, Law and Disorder, 2011. Available at: < http://arstechnica.com/tech-policy/2011/12/patriot-act-and-privacy-laws-take-a-bite-out-of-us-cloud-business/> Consulted on January 30, 2012.

Garner, Bryan. *"Black's Law Dictionary*". Second edition, West Group, Minnesota, 2001, p. 383.

Greenleaf, Graham. *"76 Global Data Privacy Laws*". Privacy Laws and Business, 2011. Available at:<http://ssrn.com/abstract=1946700> Consulted on May 25, 2012.

Henning, Anna, et.al. "*Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization.*" Congressional Research Center, USA, 2010, p. 11. Available at: <http://www.fas.org/sgp/crs/intel/R40980.pdf> Consulted on February 12, 2012.

Hogan, Michael; et. al. *"NSIT Cloud Computing Standards Roadmap*". USA, 2011, p. 24. Available at: <http://www.navigatingthroughthecloud.com/wp-content/uploads/2012/03/NIST-Cloud-Computing-Standard-Roadmap-2011.pdf?9d7bd4> Consulted on February 4th, 2012.

Hon, Kuan et.al. *"Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part II".* Queen Mary University of London, Legal Studies Research Paper No.77/2011, 2012, p. 10. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130> Consulted on April 29, 2012.

Hon, Kuan. "US Patriot Act- Can UK cloud customers use US cloud providers? Computer World UK, 2012. Available at: < http://blogs.computerworlduk.com/cloud-vision/2012/05/us-patriot-act---can-uk-cloud-customers-use-us-cloud-providers/index.htm> Consulted on June 1st, 2012.

Jaeger, Paul. "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. First Monday Journal, Vol.14, No. 5, 2009. Available at: < http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2456/2171#p4> Consulted on February 2nd, 2012.

Kamal, Dahbur, et al. *"A Survey of Risks, Threats and Vulnerabilities in Cloud Computing"*. New York Institute of Technology. Mendeley. Available at:<

http://www.mendeley.com/research/survey-risks-threats-vulnerabilities-cloud-computing/> Consulted on February 20, 2012.

Kane, Muriesl. "*Judge rules that Twitter must hand over information on Wikileaks supporters*". The Raw Story, 2012. Available at: <http://www.rawstory.com/rs/2012/01/06/judge-rules-that-twitter-must-hand-over-information-on-wikileaks-supporters/> Consulted on February 20, 2012.

Kuner, Christopher.

Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet. Part 2.". International Journal of Law and Information Technology, Vol. 18, No. 3, Oxford, 2010, p. 1. Available at: < http://ijlit.oxfordjournals.org/content/18/3/227.full.pdf> Consulted on March 28, 2012.

Kuner, Christopher. *"The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law."* Bloomberg BNA, Privacy and Security Law Report, 2012, p. 10. Available at: < http://www.huntonprivacyblog.com/wp-content/uploads/2012/02/Kuner-EU-regulation-article.pdf> Consulted on June 6, 2012.

Lecours, Alain. "USA Patriot Act". The legal Insider, Canada, 2006. Available at: < http://www.lecourshebert.com/Extraterritorial-Effects-of-the-USA-Patriot-Act.html> Consulted on March 17, 2012.

Left and right news. "*Patriot Act faces renewal in 2011*". Left and right news, USA, 2011. Available at: < http://www.leftandrightnews.com/2011/01/17/patriot-act-faces-renewal-in-2011/> Consulted on February 22, 2012.

Liu, Edward. *"Amendments to the Foreign Intelligence Surveillance Act (FISA) extended until June 1, 2015"*. Congressional Research Service, USA, 2011, p.10. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf> Consulted on March 01, 2012.

Mandalia, Ravi. "BAE Systems Abandons Microsoft Cloud Plans Citing Patriot Act". IT ProPortal, 2011. Available at: < http://www.itproportal.com/2011/12/08/bae-systems-abandons-microsoft-cloud-plans-citing-patriot-act/> Consulted on January 21, 2012.

Marrero, Victor. "*Opinion Doe v. Ashcroft*". United States District Court, New York, 2004. Available at: < http://www.aclu.org/FilesPDFs/nsl_decision.pdf> Consulted on April 2, 2012.

Marston, Sean; et al*. Cloud Computing: The business perspective*. April 2011, Elsevier Journal, Decision Support Systems, Volume 51, Issue 1, 176- 189 pp. Available at: <http://www.sciencedirect.com/science/article/pii/S0167923610002393> Consulted on February 16, 2012.

Mell, Peter; Grance, Timothy. *The NIST Definition of Cloud Computing*. January 2011. Available at: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> Consulted on February 01, 2012.

Microsoft Research. "Cloud Cryptography". 2012. Available at: < http://research.microsoft.com/en-us/projects/ cryptocloud/> Consulted on May 3rd, 2012.

Miller, Paul. "Microsoft, the USA PATRIOT Act, and European Cloud Computing". Paul Miller the Cloud of Data, 2012. Available at: < http://cloudofdata.com/2012/01/microsoft-the-usa-patriot-act-and-european-cloud-computing/> Consulted on February 17, 2012.

Moerel, Lokke, et. al. "*U.S. Subpoenas and European Data Protection Regulation*". Privacy and Data Security Law Journal, 2009, p. 654

Moerel, Lokke. *"Binding Corporate Rules: Corporate Self- regulation of Global Data Transfers*." Chapter 7, Oxford University Press, 2011, p.210.

Mogull, Rich. "Saas Security: Weighing Saas Encryption options". Search Cloud Security, 2012. Available at: < http://searchcloudsecurity.techtarget.com/tip/SaaS-security-Weighing-SaaS-encryption-options> Consulted on May 3rd, 2012.

Nakashima, Ellen. *"Plaintiff who challenged FBI's national security letters reveals concerns*." Washington Post, USA, 2010. Available at: < http://www.washingtonpost.com/wp-dyn/content/article/2010/08/09/AR2010080906252.html> Consulted on March 02, 2012.

Nieland, Andrew. *"National Security Letters and the Amended Patriot Act"* Cornell Law Review, Vol. 92, USA, 2007, p. 1208.

OECD. "Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data". Art.1 (c). Available at: < http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html> Consulted on May 22, 2012.

Office of the Inspector General. *"A Review of the Federal Bureau of Investigation's use of National Security Letter*s". US Department of Justice, USA, 2007. Available at: <http://www.justice.gov/oig/special/s0803b/final.pdf> Consulted on February 20, 2012.

Scassa, Teresa; Currie, Robert. *"New First Principles? Assessing the Internet's Challenges to Jurisdiction".* Georgetown Journal of International Law, 2011. Available at: < http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF> Consulted on March 20, 2012, p. 1025.

Singel, Ryan. "*Twitter's response to Wikileaks Subpoena should be the Industry Standard*". Wired, 2011. Available at: < http://www.wired.com/threatlevel/2011/01/twitter/> Consulted on March 12, 2012.

Slemmons, Jean; Stratford, Juri. "*Data Protection and Privacy in the United States and Europe".* IASSIST Quarterly. P. 17. Available at: < http://www.iassistdata.org/downloads/iqvol223stratford.pdf> Consulted on June 13, 2012.

Sluijs, Jasper; et.al. "*Cloud Computing in the EU Policy Sphere"*. TILEC Discussion Paper, 2011, p. 10. Available at < http://ssrn.com/abstract=1909877> Consulted on February 10, 2012.

Standler, Roland. *"Brief History of the USA PATRIOT Act of 2011".* 2008, p.3. Available at: <http://www.rbs0.com/patriot.pdf> Consulted on February 13, 2012.

Svantesson, Dan. *"Protecting Privacy on the Borderless Internet: Some thoughts on Extraterritoriality and Transborder Data Flow*". Bond Law Review, Vol.19, Iss.1, Article 7, 2007, p.3. Available at: <http://epublications.bond.edu.au/blr/vol19/iss1/7> Consulted on March 3rd, 2012.

Svantesson, Dan; Clarke, Roger. "*Privacy and Consumer Risks in Cloud Computing*." Elsevier, Computer and Security Law Review, 26, 2010, p.392. Available at: <http://www.sciencedirect.com/science/article/pii/S0267364910000828> Consulted February 9, 2012.

Timofeeva, Yulia. "Worldwide Prescriptive Jurisdiction in Internet content controversies: A comparative analysis." Connecticut Journal of International Law, Vol. 20, USA, 2004, p.4.

US Department of Justice." *The Foreign Intelligence Surveillance Court*". Membership, 2007. Available at: <http://www.fas.org/irp/agency/doj/fisa/court2007.html> Consulted on May 12, 2012.

Van Bergen, Jennifer. *"The USA PATRIOT ACT was planned before 9/11"* Truthout, 2002. Available at: < http://www.globalissues.org/article/342/the-usa-patriot-act-was-planned-before-911 > Consulted on February 10, 2012.

Waage, Torben; et.al. "Government access to Information in the cloud". Kromann Reumert, Denmark, 2012, p. 8. Available at: < http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf> Consulted on May 29, 2012.

Walden, Ian. "*Accessing data in the Cloud: The long arm of the Law Enforcement Agent*." Queen Mary School of Law Legal Studies Research Paper No. 74/2011, United Kingdom, 2011, p. 3. Available at: <http://ssrn.com/abstract=1781067> Consulted on April 3, 2012.

Webster's New World Telecom Dictionary. Wiley Publishing, Indiana, 2010. Available at: < http://computer.yourdictionary.com/proxy-server> Consulted on May 13, 2012.

Whittaker, Zack. "Dutch government to ban U.S. providers over Patriot Act concerns". ZD Net, 2011. Available at: < http://www.zdnet.com/blog/btl/dutch-government-to-ban-us-providers-over-patriot-act-concerns/58342> Consulted on March 12, 2012.

Wikileaks. Available at:< http://wikileaks.org/About.html> Consulted on March 08, 2012.

Wittacker, Zack. *"Wikileaks: Homeland Security invoques Patriot Act on Assange; seeks server data."* ZD Net, USA, 2011. Available at: < http://www.zdnet.com/blog/btl/wikileaks-homeland-security-invokes-patriot-act-on-assange-seeks-server-data/55950> Consulted on March 18, 2012.

Working Party 29. *"Opinion 10/2006 on the processing of personal data by the Society of the Worldwide Interbank Financial Telecommunication (SWIFT)."* WP29, 2006, p.21. Available at: < http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm> Consulted on May 24, 2012.

Zetter, Kim. "Unknown Tech Company Defies FBI in Mystery Surveillance Case." Wired, Privacy, Crime and Security Online, 2012. Available at: < http://www.wired.com/threatlevel/2012/03/mystery-nsl/> Consulted on March 25, 2012.