



Does the USA PATRIOT Act Give U.S. Government Access to E.U. Citizens' Personal Data
Stored in the Cloud in Violation of the E.U. Law?

University of Tilburg

L.L.M. Law & Technology

Nicolas Christian Jean FOSSOUL
Anr : 467735

Supervisor : Prof. dr. Ronald Leenes
Second reader: Sandra Ollislaegers

2012

Table of Contents

General Introduction.....	4
Chapter 1. Privacy and Cloud Computing.....	6
1.1. Privacy and Data Protection.....	6
1.1.1. E.U. Law.....	6
1.1.2. U.S. Law.....	7
1.2. Cloud Computing.....	8
1.2.1. Definition.....	8
1.2.2. Characteristics.....	8
1.2.3. Service Models and Deployment Models.....	9
1.3. Practical cases.....	10
Chapter 2. How Could the U.S. Authorities Get Access to E.U. Citizens' Personal Data?.....	12
2.1. The USA PATRIOT Act.....	12
2.2. Criminal Law Enforcement Investigation.....	13
2.2.1. Federal Rules of Criminal Procedure	13
2.2.1.1. Search and Seizure Warrant	14
2.2.1.2. Grand Jury Subpoena Duces Tecum.....	15
2.2.2. Electronic Communication Privacy Act.....	16
2.2.2.1. Interception of Wire, Oral or Electronic Communications.....	16
2.2.2.2. Access to the Content of Stored Electronic Communication and Communication Transaction Records.....	17
2.2.2.3. Pen Registers and Trap and Trace Devices.....	20
2.3. Foreign Intelligence Surveillance Act Order.....	21
2.3.1. Background Information on the Foreign Intelligence Surveillance Act.....	21
2.3.2. FISA Orders for Electronic Surveillance	22
2.3.3. FISA Order for Physical Searches.....	24
2.3.4. FISA Pen Register or Trap and Trace Device Orders.....	24
2.3.5. FISA Order for Business Records and Other Tangible Things.....	26
2.3.6. Lone Wolf Provision.....	30
2.4. National Security Letter: Section 505 of the USA PATRIOT Act.....	31
2.5. Comparison of NSL and FISA Order.....	34
2.6. Conclusion	35
Chapter 3. European Union Data Protection.....	36
3.1. A trilateral Relationship: Controller, Processor and Data Subject.....	36
3.2. Applicability of the Data Protection Directive.....	37
3.3. Obligations	38
3.4. Legitimate Processing.....	39
3.5. E.U. Transfer Rules and Mutual Legal Assistance Treaty.....	40
3.5.1. E.U. Transfer Rules.....	40
3.5.2. How Should the U.S. Authorities Access E.U. Citizens' Personal Data?	41
3.5.2.1. Exchange of Personal Data in Absence of an Agreement.....	41
3.5.2.2. Exchange of Personal Data in Presence of an Agreement.....	42
3.5.2.2.1. Multilateral treaties.....	42
3.5.2.2.2. Bilateral Treaties	42
3.5.2.2.3. Is Mutual Legal Assistance the Panacea?.....	43
3.6. Conclusion.....	44
Chapter 4. When Two Regimes Conflict – Implications for E.U. Cloud Users.....	45
4.1. Limitation to the Reach of the U.S. Law.....	45
4.1.1. U.S. Jurisdiction.....	45

4.1.1.1. Personal Jurisdiction Based on Citizenship, Consent and Waiver.....	45
4.1.1.2. Pennoyer v. Neff.....	45
4.1.1.3. Minimum Contact and Systematic and Continuous Contact.....	46
4.1.1.4. State Long-Arm Statute.....	47
4.1.1.5. Balancing test	47
4.1.2. Possession, Custody or Control.....	47
4.1.3. Information Located Abroad.....	48
4.2. What Are the Implications for E.U. Citizens' Personal Data?	48
4.3. Conclusion.....	50
Chapter 5. Recommendations	52
5.1. Law as a Constraint	52
5.1.1. Blocking Statutes.....	52
5.1.2. Ban on Outsourcing (Sensitive) Personal Data to Cloud Computing Providers Falling Under the U.S. Jurisdiction.....	54
5.1.3. Cooperation between the E.U. and the U.S.....	54
5.2. Social Norms As a Constraint	55
5.2.1. Challenging the Gag Order.....	55
5.2.2. A Proportionate Answer to Disclosure Order.....	56
5.3. Market	57
5.4. Architecture.....	57
5.4.1. Encryption.....	58
5.4.2. Keeping Data in-House.....	59
5.5. Practical Solutions From a Customer Point of View.....	59
5.6. Conclusion.....	59
General Conclusion.....	61
Bibliography.....	62
Appendices.....	72

General Introduction

Privacy and data protection are fundamental rights in European Union law. They are important values that deserve protection. However, recent declarations have shed the light on a worrying fact. The most important one was expressed by Gordon Frazer from Microsoft UK¹. The U.S. law enforcement could access European citizens' personal data pursuant the USA PATRIOT Act.

It is not the first time that such a revelation is made. Similar concerns regarding the USA PATRIOT Act were raised in Canada. In the past, the U.S. had already asked for EU citizens' bank data to the Belgian based SWIFT Company and for passenger name record to airline companies. The E.U. and the U.S. had solved the conflict by the conclusion of three negotiated agreements: the 2007 PNR agreement,² the 2001 PNR agreement³ and the 2010 SWIFT agreement.⁴

While cloud computing offers several advantages for individuals and businesses, this new technology is not without any risk for the privacy of its users. One of these risks regards the United States and the USA PATRIOT Act. It is said that cloud computing hand over E.U. citizens' personal data the U.S. authorities without regard for E.U. data protection rules. It causes distrust from E.U. citizens and E.U. companies toward the cloud which feel that their privacy is at stake. As a result, the development of cloud computing is slowed down and E.U. companies do not make the most of the opportunities offered by this technology.

This issue deserves to be analysed for several reasons. Firstly, privacy and data protection are important value in a democratic society. Secondly, the USA PATRIOT Act makes privacy intrusion easier. Moreover, the E.U. sovereignty is weakened by the action of the U.S. Finally, the cloud computing phenomenon accentuates the problem. Indeed, it has a particular effect on the reach of the USA PATRIOT Act. Since leaders in cloud computing services are mostly U.S. based companies, it is likely that most of the data contained in the cloud fall under the U.S. jurisdiction. Examples of big cloud computing providers are Google, Microsoft or Facebook. Also, it is anticipated that, within a few years, "70% to even 90% of the world's computing and data storage will occur in the cloud".⁵ While before, personal data pertaining to corporations were unlikely to fall under the U.S. jurisdiction because they were stored in-house, cloud computing technology changes this old pattern.

My research focuses on the power the U.S. authorities have to access European citizens' personal data in the cloud. More precisely, I ask the question as to whether the USA PATRIOT Act

1 C. Carnabuci, "The long arm of the USA Patriot Act: tips for Australian businesses selecting data service providers, freshfields bruckhaus deringer law firm", November 2011, p. 3. Available at <http://www.powerretail.com.au/wp-content/downloads/macquarie/The-long-arm-of-the-USA-Patriot-Act.pdf> [accessed June 2012].

2 Agreement of the 23rd July 2007 between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), *O.J.L.*, August 4, 2007, p. 18.

3 European Commission, "New EU-US agreement on PNR improves data protection and fights crime and terrorism", *Europa.eu*, November 2011, Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1368&format=HTML&aged=1&language=EN&guiLanguage=fr> [accessed September 2012].

4 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *O.J.L.*, 195, July 27, 2010, p. 5.

5 M. N. Bashir, J. P. Kesan, C. M. Hayes, R. Zielinski, "Privacy in the Cloud: Going Beyond the Contractarian Paradigm", University of Illinois, p. 4. Available at: <http://assured-cloud-computing.illinois.edu/sites/default/files/AFRL%2520Talk%2520-%2520Privacy-Cloud-Computing%2520Dec-14-2011.pdf> [accessed July 2012].

gives U.S. law enforcement authorities access to E.U. citizens' personal data stored in the cloud in violation of the E.U. law.

After having described what cloud computing is and set the basis for this study in chapter 1, chapter 2 will explore how the U.S. laws and particularly how the USA PATRIOT Act grant U.S. authorities access to E.U. citizens' personal data. For this purpose, U.S. legal instruments will be discussed. Besides, I will make an attempt to assess the effective reach of these legal instruments. The third chapter examines the European Union privacy law related to this matter and the so-called Mutual Legal Assistance Treaty regulating the exchange of personal data between the U.S. and the E.U. The fourth chapter examines the jurisdictional scope of the U.S. law setting the basis for the description of a few practical cases. These involve U.S. requests of E.U. citizens' personal directed at cloud computing providers. Until now, the E.U. did not address the issues resulting from the Patriot Act in an adequate manner. How could or should the European Commission react to the issues raised by the Patriot Act? The last chapter of this study explores practical and legal solutions which could be implemented by both policy makers and cloud users.

What aroused my curiosity about this problem is that this topic was taken up by all the media (Znet, LesEchos, following the declaration of Gordon Frazer, managing director of Microsoft UK (source).⁶ This news came as a bombshell. Subsequently, this issue became the object of political debates between the United States and the European Union (B. Obama, J. McCain, V. Reding, S. in 't Veld). Meanwhile, the topic was picked up by the legal world. This said, what hold my interest in this research is primarily my concern for privacy and data protection in modern contexts, such as cloud computing. As (almost) everyone nowadays, I am a user of cloud computing services. I have a "Gmail" account, a "Facebook" account, a "Dropbox" account... where I can post and exchange personal data with other users. So, who can access my personal data stored in the cloud and particularly can the US law enforcement authorities access my data are questions that matter for me. Besides, what makes this problem interesting is the fact that it regards a very broad public, the European users of cloud computing services.

To answer my research questions, this study is based on law books, articles of law journals, case law and legislation relevant to the field. It also refers to articles written by practitioners working law firms and consultancy firms which ensure that this study has practical and up-to-date aspects. Besides, I refer to U.S. Congressional and WP 29 reports which enjoy a great authority.

6 J. Labeled, "Le « USA Patriot Act » : risque majeur pour la confidentialité des données dans le Cloud", *Lecercler.lesechos.fr*; March 13, 2012. Available at: <http://lecercler.lesechos.fr/entreprises-marches/high-tech-medias/internet/221144488/usa-patriot-Act-risque-majeur-confidentialit> [accessed April 2012]; J. Labeled, "USA Patriot Act: un risque majeur pour la confidentialité des données dans le Cloud", *Solutionsauxentreprises.lemonde.fr*; March 26, 2012. Available at: http://solutionsauxentreprises.lemonde.fr/cloud-computing/usa-patriot-Act-un-risque-majeur-pour-la-confidentialite-des-donnees-dans-le-cloud_a-27-630.html [accessed April 2012]; Z. Whittaker, "USA PATRIOT Act: The myth of a secure European cloud?", *Znet.com*, April 27, 2011. Available at <http://www.zdnet.com/blog/igeneration/usa-patriot-Act-the-myth-of-a-secure-european-cloud/8807> [accessed February 2012].

Chapter 1. Privacy and Cloud Computing

This chapter aims at describing general concepts relating to the issues at stake. First, privacy and data protection will be explained in E.U. law and in U.S. law. Secondly, cloud computing as such and the different service models and deployment models it can be subject to will be defined. Third, different practical cases involving cloud computing providers, subsidiaries and data center will be exposed.

1.1. Privacy and Data Protection

Since this issue regards privacy and data protection, those terms deserve to be analysed. They will be explained separately as they have different meaning in E.U. law and in U.S. law.

1.1.1. E.U. Law

The right to privacy is protected by the European Convention on Human Rights⁷ and the Charter of Fundamental Rights of the European Union.⁸

Article 7 of the Charter of Fundamental Rights of the European Union - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 of the European Convention on Human Right - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and *is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The right to data protection is governed by the article 8 of the Charter of Fundamental Rights of the European Union which reads as follow:

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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Besides, the right to data protection is also governed by the Data Protection Directive and the E-Privacy Directive.

Also, the term “personal data” deserves some explanations as it is a central concept in the study. The wording “personal data” is defined by the article 2 (a) of the DPD as meaning

⁷ Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS No. 2; 213 UNTS 222.

⁸ Charter of Fundamental Rights of the European Union, proclaimed in Nice, December 7, 2000, *O.J.* C- 364, December 18, 2000, p. 1.

“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”.

The Working Party construes the terms used in the definition above giving, thereby, meaningful information about what “personal information” is.⁹ First of all, “any information” is construed from three points of view. From the point of the nature of the information, “any information” covers objective and subjective information.¹⁰ For example, objective information can be given by a blood test. The reliability of a borrower toward its bank is a subjective information. From the point of view of the content, personal information can refer to sensitive data or other general kind of data (information about the private and family life, the job or the hobby's... of an individual).¹¹ Thirdly, the form given to the information or the medium on which the information are contained is not relevant to be considered as personal data. Indeed, data in alphabetical, numerical, graphical form contained on a sheet of paper or stored in a hard-drive could equally be considered as personal data.¹² Therefore, “term “any information” contained in the Directive clearly signals the willingness of the legislator to design a broad concept of personal data”.¹³

Secondly, considering the terms “relating to”, the WP 29 made clear that personal information can also relate to object, event or processes connected with an individual.¹⁴ For example, the price of a house, an object, could be a personal information.¹⁵

Thirdly, the terms “identified or identifiable” are explained by the WP 29. A natural person is “identified” when it is possible to distinguish him from a group of individual.¹⁶ Besides, a natural person can be identified directly, e.g. by its name, or indirectly, by a combination of pieces of information leading to the identification of an individual.¹⁷

Finally, the wording “natural person” means human being, the nationality or the place of residence being irrelevant.¹⁸ However, “information about legal persons may also be considered as “relating to” natural persons on their own merits”.¹⁹

1.1.2. U.S. Law

The United States Constitution does not refer explicitly to a right to privacy. However, some amendments were interpreted as protecting privacy. They are mainly the 1st, the 3rd, the 4th and the 5th amendment.²⁰ They respectively regard the freedom of religion, press, expression, the quartering of troops, the protection against unreasonable search and seizure and the grand jury, double jeopardy, self-incrimination, due process.

9 Working Party 29, “Opinion 4/2007 on the Concept of Personal Data”, June 20, 2007. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [accessed August 2012].

10 Ibid., p. 6.

11 Ibid., p. 6.

12 Ibid., p. 7.

13 Ibid., p. 6.

14 Ibid., p. 9.

15 Ibid., p. 9.

16 Ibid., p. 12.

17 Ibid., p. 13.

18 Ibid., p. 21.

19 Ibid., p. 23.

20 P. De Hert & R. Bellanova, “Data Protection from a Transatlantic Perspective: the EU and US Move Towards an International Agreement?”, September 2008, p. 13. Available at: <http://www.ceps.eu/content/selection-briefing-papers-prepared-european-institutions> [accessed July 2012].

Data protection is not a constitutional right in the U.S. law. Besides, the weight that is given to data protection in U.S. law does not seem as important as in E.U. law.²¹

1.2. Cloud Computing

1.2.1. Definition

There exist many definitions of cloud computing. It is beyond the scope of this study to review all the definitions that were given to “cloud computing”. Here, only two of them will be proposed. A short and easy to understand definition emanates from the EU. Another one, comprehensive and complex emanates from the U.S. National Institute of Standards and Technology (hereinafter NIST).²²

The European Commission describes cloud computing as “Internet-based computing whereby software, shared resources and information are on remote servers (“in the cloud”)”.²³

According to the NIST “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”.²⁴

In both definitions, there is the idea that customers are not any more connected to servers, located on company premises for example. On the contrary, they are connected to something remote, the cloud.

1.2.2. Characteristics

P. Mell and T. Grance set forth 5 essential characteristics of cloud computing.²⁵ First of all, they state that cloud computing is a “on-demand self-service”²⁶ meaning that users can provision cloud computing capacities without assistance of the cloud computing provider.²⁷ As a consequence, the users can access different types of services within no time. “Self-service cloud offerings must provide easy-to-use, intuitive user interfaces that equip users to productively manage the service delivery lifecycle”.²⁸ This characteristic is also named “self-provisioning of resources”²⁹ by other authors.

²¹ *Ibid.*, p. 45.

²² The NIST is an agency of the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness.

²³ European Commission, “A comprehensive approach on personal data protection in the European Union”, COM (2010) 609 final, 4 November 2010. Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [accessed November 2011].

²⁴ P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, September 28, 2011, p. 2. Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909616 [accessed November 2011].

²⁵ *Ibid.*, p. 2.

²⁶ *Ibid.*, p. 2.

²⁷ *Ibid.*, p. 2.

²⁸ D. M. Surgient, “The five defining characteristics of cloud computing”, *Znet.com*, April 9, 2011. Available at: <http://www.zdnet.com/news/the-five-defining-characteristics-of-cloud-computing/287001> [accessed August 2012].

²⁹ T. Mather, S. Kumaraswamy, S. Latif, *Cloud Security and Privacy*, Sebastopol, Mike Loukides Ed, 2009, p. 8.

Secondly, cloud computing is characterized by a “broad network access”.³⁰ It means that cloud computing is network based and that capabilities are accessible from any device such as desktops or mobile phone from anywhere. In general the users access the cloud via Internet. However, the cloud can also be accessed from a private corporate network.

“Rapid elasticity” is the third characteristic of cloud computing found by the NIST.³¹ That is to say that the user can increase or decrease computer resources in function of their needs.

Fourthly, it is also a “measured serviced”.³² This means essentially that cloud computing providers measure “the amount of service provided and [react] accordingly (both in terms of billing the client, and updating hardware and software as appropriate)”.³³

Finally, cloud computing is characterised by “resource pooling”.³⁴ In other words, the cloud computing resources are shared. Therefore, multiple users may use the same set of computer resources concurrently.³⁵ This implies a “sense of location independence” meaning that the users “generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center)”.³⁶ Consequently, the cloud computing provider may seek to store or process data where it is the most efficient or where it is the cheapest. Therefore, data may move from a jurisdiction to another according to the circumstances. Also this may imply that the data of a single customer would be spread in different data centers.

1.2.3. Service Models and Deployment Models

Cloud computing is a broad concept. There are three different service models, and four deployment models.

The service model can take the form of a *Software as a Service (SaaS)*, *Platform as a Service (PaaS)* or a *Infrastructure as a Service (IaaS)*.³⁷ Firstly, in the *SaaS*, the cloud computing provider makes available a software which cannot be managed or control by the consumer. The functionality is akin to an end-user application. For example, they are Dropbox, MobileMe and Facebook.³⁸ In the case of Facebook, users are allowed to post pictures, text, etc. on a website while Facebook keeps control over the infrastructure. Traditionally, the software itself was purchased by the customer and was then installed onto its own hardware in return for a licence fee. Here, the software is made available for free or in exchange of a periodic fee.

Secondly, in *PaaS*, the cloud computing provider makes available a development environment to customers. Thanks to this development environment, customers can develop their own applications. Simply put, customers use “building blocks (e.g. predefined blocks of code)”

30 P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, *o.c.*, p. 2.

31 *Ibid.*, p. 2.

32 *Ibid.*, p. 2.

33 D. Dix & A. Bristow, “What in the World is Cloud Computing?”, *Princeton.edu*. Available at: <http://www.princeton.edu/~ddix/cloud-computing.html> [accessed August 2012].

34 P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, *o.c.*, p. 2.

35 In traditional computing models, computing facilities are used by a single user.

36 P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, *o.c.*, p. 2.

37 *Ibid.*, p. 2.

38 Dropbox provides file hosting and backup. MobileMe provides Email, file hosting and personal information management. Facebook provides social networking services.

offered by the cloud provider to build a software.³⁹ However, the cloud infrastructure including the network, servers, the storage and even the application itself remains under control of the cloud computing provider.⁴⁰ Google's App Engine and Microsoft Window Azure are examples of *PaaS*. Microsoft Azure allows users to build or personalize applications and to distribute them to customers. Thus, PaaS democratizes the development of software.

The last service model is the *IaaS* where the consumer can install an operating system and its own softwares onto the infrastructure provided by the cloud computing provider. It means that “the service provider owns the equipment and is responsible for housing, running and maintaining it”.⁴¹ Here, the consumer has a broader control regarding storage, the applications and the operating system. Joyent Cloud, IBM Smart Business Cloud and GoGrid are example of IaaS. To briefly compare these three different models, it can be said that SaaS provides consumer with the highest level of functionality. IaaS and PaaS offer a lower level of functionality, IaaS offering the most basic services.

Those cloud based services necessitate large computing capacity and are, therefore, hosted in data centers and server farms. The data centers and server farms of a single cloud computing provider can be situated in multiple locations. Also, they can be connected together via internetworks.⁴² Therefore, data can “travel” easily and with no time from a location to another.

Besides the three service models, the NIST defines four types of deployment models.⁴³ The *Private cloud* is the one where the provider provisions the cloud infrastructure for a single organization on or off premises. With other words, the computing, network and storage infrastructure of a private cloud is not shared with other users. The IT department of the users or a third party with contractual service level agreement is usually responsible for the security and the day-to-day operation. Therefore, the users have a high degree of control security aspects.⁴⁴ In the *Community cloud*, the cloud infrastructure is shared between consumers belonging to a specific community having common concerns (e.g., mission, security requirement and policy). The third deployment model is the *Public cloud*. Here, the cloud computing provider offers services to the general public over the Internet via web applications or web services.⁴⁵ This is the traditional manner to provide cloud computing services. The cloud provider is responsible for the security management and day-to-day operations. Therefore, the users have no or a very limited degree of control over the physical and logical security aspects.⁴⁶ In that case, the cloud infrastructure exists on the premises of the cloud provider. Finally, in the *Hybrid cloud*, 2 or 3 models seen above are mixed together.

1.3. Practical cases

This section aims at describing several practical cases involving cloud computing providers, subsidiaries and data centers and the location of each of them. Because these cases are the mirror of possible combinations occurring in the daily life, they are analysed in this study. Besides, location of cloud actors is fundamental as this is a criteria used to determined whether or not the U.S.

39 T. Mather, S. Kumaraswamy, S. Latif, *o.c.*, p. 19.

40 P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, *o.c.*, p. 2.

41 M. Rouse, “Infrastructure as a Service (IaaS)”, *Searchcloudcomputing.techtarget.com*, August 2010. Available at: <http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS> [accessed August 2012].

42 T. Mather, S. Kumaraswamy, S. Latif, *o.c.*, p. 13.

43 P. Mell & T. Grance, “The NIST Definition of Cloud Computing”, *o.c.*, p. 3.

44 T. Mather, S. Kumaraswamy, S. Latif, *o.c.*, p. 24.

45 *Ibid.*, p. 23.

46 *Ibid.*, p. 23.

authorities can assert jurisdiction over them. Therefore, location of cloud actors occupies a central role in these cases. Later on in this study (*see infra* Chapter 4), an attempt will be made to determine whether or not the USA PATRIOT Act is applicable to these cases. As a matter of simplicity, these practical cases are presented in the form of a table.

No	Cloud Provider Location	Subsidiary Location	Data Center Location
1	E.U.	U.S. or no subsidiary	U.S.
1	U.S.	E.U. or no subsidiary	U.S.
2	U.S.	none	E.U.
3	E.U.	U.S.	E.U.
4	U.S.	E.U.	E.U.
5	E.U.	No subsidiary but minimum contact	E.U.
6	E.U.	E.U. or no subsidiary	E.U.

Table I: Six cases

Chapter 2. How Could the U.S. Authorities Get Access to E.U. Citizens'

Personal Data?

The European Union and the E.U. consumers are concerned about the extensive powers the USA PATRIOT Act grants U.S. authorities. Many think this Act may be used to access their personal data stored in the cloud. While E.U. cloud computing services may make the most of this situation, U.S. cloud service providers fear a loss of profit. Therefore, the United States wish to diminish the European fears with regard to the Patriot Act.

This chapter aims to identify how the U.S. authorities can access European citizen's personal data, based not only on the USA PATRIOT Act, but also on other legal instruments. The USA PATRIOT Act amends three statutory regimes used by the U.S. government to gather personal data. The choice of a particular regime depends on the purpose for which for the U.S. government want to collect personal data.⁴⁷ These regimes provide the U.S. authorities with analogous legal instruments, though standards and procedures differ from a regime to another.

First, the U.S. government will apply the Federal Rules of Criminal Procedure, the ECPA and various provisions contained in Title 18 of the U.S. Code in criminal law enforcement investigations (section 2). Second, in foreign intelligence investigations, the Foreign Intelligence Surveillance Act (hereinafter FISA) applies (section 3). Third, in national security investigations, national security letter (hereinafter NSL) statutes apply (section 4). The statutory regime applicable in criminal law enforcement investigation deserves to be analysed as criminal investigation may be conducted against E.U. citizens as well. The two last statutory regimes, the FISA and the NSL statutes, will also be explored since the risk that the U.S. government accesses E.U. citizens' personal data through these channels exists as well. These tools and the law they are part of will be described below. Besides, an attempt will be made to evaluate the extent to which these tools are used to access E.U. citizens' personal data personal data.

Before entering in the subject as such, the USA PATRIOT Act will be described to give a helicopter view of what this Act actually is.

2.1. The USA PATRIOT Act

The USA PATRIOT Act of 2001,⁴⁸ acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, was adopted in the aftermath of the terrorist attacks of the 9/11 as a legal response to the terrorism.

The aim of the USA PATRIOT Act is officially stated in its preamble: “An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes”.⁴⁹ The structure of the USA PATRIOT Act is particular. The USA PATRIOT Act contains ten parts forming a compilation of changes to several existing US

47 A. C. Henning, E. B. Bazan, C. Doyle & E. C. Liu, “Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization”, *Congressional Research Service*, March 2, 2010, p. 6. Available at: <http://fpc.state.gov/documents/organization/139232.pdf> [accessed June 2012].

48 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, Pub. L. No. 107-56 [H.R. 3162], 115 Stat. 272, approved October 26, 2001.

49 See also for a description of the USA Patriot Act emanating from the USA Department of Justice : USA Department of Justice, “The USA PATRIOT Act: Preserving Life and Liberty”, *justice.gov*. Available at: <http://www.justice.gov/archive/ll/highlights.htm> [accessed May 2012].

intelligence, communications, and privacy laws.

Regarding governmental access to personal data, title II of the USA PATRIOT Act entitled “Enhancement Surveillance Procedures” and the section 505 of the title V entitled “Removing Obstacles to Investigation Terrorism” are especially relevant. They amend the Electronic Communication Privacy Act, the Foreign Intelligence Surveillance Act and the NSL statutes by easing substantive and procedural restrictions as to how law enforcement agencies can conduct surveillance and gather information regarding terrorism and criminal activities.

The sections contained in these titles are the most controversial of the USA PATRIOT Act. “Some perceived the changes as necessary to unearth terrorist cells and update investigative authorities to respond to the new technologies and characteristics of ever-shifting threats. Others argued that authorities granted by the USA PATRIOT Act and subsequent measures could unnecessarily undermine constitutional rights over time. In response to such concerns, sunset provisions were established for many of the changes”.⁵⁰ Indeed, sixteen of these amendments were scheduled to expire on December 31, 2005. They are the sections 201, 202, 203 (b) & (d), 209, 212, 213, 217, 220, 204, 206, 207, 214, 215, 218, 223 and 225. However, the USA PATRIOT Improvement and Reauthorization Act of 2005⁵¹ made permanent 14 of the 16 expiring USA PATRIOT Act sections and extended the sunset on section 206 and 215. These two sections were extended until June 1, 2015 pursuant to the PATRIOT Sunsets Extension Act of 2011.⁵²

The USA PATRIOT Act has undergone many legislative changes since it was voted in 2001. Two major amending laws deserve attention. The first one is the USA PATRIOT Improvement and Reauthorization Act of 2005. The second one is the USA PATRIOT additional Reauthorization Amendments Act of 2006.⁵³

2.2. Criminal Law Enforcement Investigation

Federal Rules of Criminal Procedure, the ECPA and other provisions contained in Title 18 of the U.S. Code are the statutes primarily used in criminal law enforcement investigation.

2.2.1. Federal Rules of Criminal Procedure

The Federal Rules of Criminal Procedure provide federal officials with two different legal instruments to “gain access to space, document, and other private materials”⁵⁴: they are the warrant used during the investigation and the subpoena used during the prosecution.

50 A. C. Henning, E. B. Bazan, C. Doyle & E. C. Liu, “Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization”, *o.c.*, p. 15. *See also*: O. S. Kerr, “Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn’t”, *Northwestern University Law Review*, Vol. 97, Issue 2 (2002-2003), pp. 607-674; J. C. Evans, “Hijacking Civil Liberties: The USA PATRIOT Act of 2001”, *Loyola University Chicago Law Journal*, Vol. 33, Issue 4, pp. 933-990.

51 USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, approved March 9, 2006.

52 PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216, approved May 26, 2011.

53 USA PATRIOT additional Reauthorization Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278, approved March 9, 2006.

54 A. C. Henning, E. B. Bazan, C. Doyle & E. C. Liu, “Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization”, *o.c.*, p. 6.

2.2.1.1. Search and Seizure Warrant

Firstly, as a matter of qualification, the definition of search and seizure warrants should be stated. It is a legal instrument that authorises law enforcement authorities to conduct a search of a person or location in order to find evidence in a criminal investigation.⁵⁵

The Federal Rule of Criminal Procedure 41 governs the issuance of search and seizure warrant. A warrant must be approved by a U.S. court upon showing probable cause.⁵⁶ “Probable cause” may be define as the reasonable “believe [that a] suspect has committed, is committing, or is about to commit a crime”.⁵⁷ The warrant must “identify the person or property to be searched [and] identify any person or property to be seized. The term “property” includes “documents, books, papers, any other tangible object, and information”.⁵⁸ In this sense, the warrants have to be reasonable and specific,⁵⁹ and must be specific about the place to be searched or the things to be seized. Seizable things may also include “electronically stored information”.⁶⁰ A warrant may “authorize the seizure of electronic storage mediator or the seizure or copying of electronically stored information”.⁶¹ Thus, “officers may seize or copy the entire storage medium [e.g. a hard-drive] and review it later to determine what electronically stored information falls within the scope of the warrant”.⁶²

The USA PATRIOT Act amends some provisions related to search and seizure warrant. Section 504 of the USA PATRIOT Act enhances the cooperation between foreign intelligence officers and criminal law enforcement agencies by authorizing them to share information obtained from a physical search. Besides, section 213 authorizes law enforcement to delay the notice of the search warrant if some conditions are met.⁶³

Although these amendments do not change substantially how law enforcement authorities access personal data, search and seize warrant can be used to access data in the cloud. A search and seizure warrant can be used to seek electronically storage mediator which are typically hard-drive. Storage capacities in the form of hard-drive are part of the services offered by cloud computing provider. Therefore, information in the cloud may the object of a search and seize warrant.

The impact of search and seize warrant on E.U. citizens personal data is difficult to access as there is no official report relating the number of warrants. What can be said is that conducting a search on a server in the premise of a cloud computing provider requires technical knowledge and time.⁶⁴ Therefore, use of other means would be more appropriate and more efficient to access personal data. Nevertheless, search warrants could be used by the U.S. to access U.E. citizens' personal data in the cloud and cloud computing providers complying with such a request could violate the E.U. law as we will see in Chapter 3.⁶⁵

55 Fed. R. Crim. Pro. 41 (c).

56 Fed. R. Crim. Pro. 41 (d).

57 Anon., “Probable Cause”, *Lectlaw.com*. Available at: <http://www.lectlaw.com/def2/p089.htm> [accessed July 2012].

58 Fed. R. Crim. Pro. 41 (a).

59 *Murray v. United States*, 487 U.S. 533, 108 S. Ct. 2529, 101 L. Ed. 2d 472, (1988).

60 Fed. R. Crim. Pro. 41 (e).

61 *Ibid*.

62 Committee Notes on Rules — 2009 Amendment. Available at: http://www.law.cornell.edu/rules/frcrmp/rule_41 [accessed July 2012].

63 18 U.S.C. § 3103 (a)(b).

64 Searching and seizing the personal computing of a suspect is fairly easy. However, things are way more complicated when it comes to cloud computing and their giant data centers.

65 A. Lakatos, “United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud”, January 2012, p. 1. Available at: <http://www.mayerbrown.com/files/Publication/ce02dec6-f143-46ec-a0a3->

2.2.1.2. Grand Jury Subpoena Duces Tecum

A grand jury subpoenas duces tecum is a legal instrument issued by a group of civilian jurors who inquire the existence of possible criminal conduct under the control of a prosecutor allowing the collection of evidence in criminal investigations.⁶⁶ The work of the grand jury is characterized by five features.⁶⁷ First of all, the grand jury is independent from the court's supervision even if subpoenas are issued under the authority of a court.⁶⁸ Indeed, in practice, courts issue blank subpoenas to prosecutor working with a grand jury.⁶⁹ Secondly, the grand jury has significant investigative powers. It can start an investigation on the mere suspicion that the law is being violated without showing probable cause.⁷⁰ Moreover, any person or document can be served with a subpoena from a grand jury which needs not to respect many rules of evidence.⁷¹ Thirdly, subpoenas are deemed to be valid. This explains why the recipients do not usually have the right to appeal against a subpoena. However, “the court may quash or modify the subpoena if compliance would be unreasonable or oppressive”.⁷² A four prongs test is used to determine whether a subpoena is unreasonable⁷³: it asks whether the requested data are relevant, whether the information is specified, whether production of materials covers a reasonable period of time and whether compliance incur undue burden. Fourthly, a grand jury leads the investigations in secrecy.⁷⁴ The last principle that needs to be mentioned is the freedom from procedural detours and delay.⁷⁵ Not complying with a subpoena can lead the person object of the investigation to be in contempt of court.

The USA PATRIOT Act did not modify fundamentally the way a grand jury accesses personal data pursuant a subpoena. Section 203 amended the Federal Rules of Criminal Procedure to permit disclosures of “matters occurring before the grand jury” involving “foreign intelligence or counter intelligence” to “any Federal law enforcement, intelligence, protective, immigration, national defence, or national security official in order to assist the official receiving that information in the performance of his official duties”.⁷⁶

Here again, the impact of grand jury subpoenas on E.U. citizens personal data in the cloud is difficult to assess as there is no official report relating the number of the subpoenas issued by year. However, some authors give a clue regarding the actual power of grand juries subpoenas to access data in the cloud. Orin R. Kerr states that “whereas the subpoena power is fairly narrow in

53c06d770707/Presentation/PublicationAttachment/f56ea23a-7fd4-40bb-9b78-57e0787774dc/12057.PDF [accessed April 2012].

66 Fed. R. Crim. P. R 6.

67 *Whitehouse v. United States Dist. Court for Dist. of R.I.*, 53 F.3d 1349, 1357 (1st Cir. 1995).

68 M. Geist & M. Homs, “Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World”, *University of New Brunswick Law Journal*, vol. 54, 2005, p. 8.

69 Fed. R. Crim. P. 17 (a).

70 *See*: *United States v. R. Enters.*, 498 U.S. 292, 297 (1991).

71 *See*, e.g., *United States v. Calandra*, 414 U.S. 338 (1974); *Costello v. United States*, 350 U.S. 359, (1956). *See also*: *United States v. R. Enterprises*, 498 U.S. 292, 298-301, 111 S.Ct. 722, 726-28, 112 L.Ed.2d 795 (1991).

72 Fed. R. Crim. P. 17(c)(2).

73 J. Gruenspecht, “‘Reasonable’ Grand Jury Subpoenas: Asking for Information in the Age of Big Data”, *Harvard Journal of Law & Technology*, vol. 24, 2011, p. 547.

74 Fed. R. Crim. P. R 6 (e)(2)(a).

75 *See*: *Whitehouse v. United States Dist. Court for Dist. of R.I.*, 53 F.3d 1349, 1357 (1st Cir. 1995).

76 *See*: S. Levy, “The Patriot Act Grand Jury Disclosure Exception: a Proposal For Reconciling Civil Liberty and Law Enforcement Concerns”, *J.I.C.L.*, 2005, pp. 3-4. Available at: http://www.kentlaw.edu/jicl/articles/spring2005/s2005_sara_levy.pdf [accessed July 2012].

traditional cases, in computer crime cases it is incredibly broad”.⁷⁷ There are two reasons leading to this conclusion. Firstly, the limit of burdensomeness is ineffectual in a cloud computing context. It is generally easy for a cloud computing provider to copy a large amount of data and hand it over to the requesting authority. Besides, for practical reasons, it might be that the cloud computing provider hand over personal data in bulk instead of filtering carefully through the server to identify the file requested.⁷⁸ Secondly, things are not only simple for cloud computing providers but also for the requesting authority. “Officers can simply fax a copy of the subpoena to the ISP's headquarters and await a package or return fax with the relevant documents”.^{79 80}

Thus, grand juries subpoena are certainly an important legal tool giving access to large amount of personal data, putting the privacy of many cloud computing customers at stake.

2.2.2. Electronic Communication Privacy Act

Pursuant the ECPA, law enforcement can intercept wire, oral or electronic communications,⁸¹ access the content of stored electronic communication and communication transaction records⁸² and use trap and trace devices and pen registers.⁸³

2.2.2.1. Interception of Wire, Oral or Electronic Communications

Sections 2510 to 2522 govern the interception of content of wire, oral or electronic communications while in transit from an agent of a provider of wire or electronic communication service.

These terms are defined by section 2510 ECPA. “Content” means “any information concerning the substance, purport, or meaning of that communication”.

Provider of wire or electronic communication service is “any service which provides to users thereof the ability to send or receive wire or electronic communications”. “The key issue in determining whether a company provides electronic communication is that company's role in providing the ability to send or receive the precise communication at issue regardless the company's primary business”.⁸⁴ For example, e-mail service providers, message boards and website allowing users to post electronic messages are electronic communication providers.^{85 86}

The three categories of communication are also defined by section 2510. The wording “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

77 O. S. Kerr, “Digital Evidence and the New Criminal Procedure”, *Columbia Law Rev.*, Jan. 2005, p. 296.

78 *Ibid.*, p. 294.

79 The author used the wording “ISP”. But, a similar reasoning can be held regarding cloud computing provider. Besides, some ISPs provide cloud computing services.

80 *Ibid.*, p. 296.

81 18 U.S.C. §§ 2510-2522.

82 18 U.S.C. §§ 2701-2712.

83 18 U.S.C. §§ 3121-3127.

84 J. W. Rittinghouse & B. Hancock, *Cybersecurity Operations Handbook*, Burlington, J. W. Rittinghouse & B.Hancock Ed., 2003, p 85.

85 *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000).

86 *Guest v. Leis*, 255 F.3d 325, 338 (6th Cir. 2001).

the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce”. Simply put, “wire communication” is “any voice communication that is transmitted, whether over the phone company's wires, a cellular network, or the Internet”.⁸⁷ Then “oral communication” means “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication”. Basically, it is the face-to-face conversation. Finally, “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, photoelectronic or photooptical system that affects interstate or foreign commerce”. With other words, “electronic communication” encompasses “any transmitted communication that isn't a voice communication” (e.g. email, instant messaging, and websurfing).⁸⁸ For the purpose of this study, only wire and electronic communications are relevant.

The requirements that need to be met to obtain a court order are very strict.⁸⁹ Law enforcement has to show that probable cause exists to believe “that an individual is committing, has committed, or is about to commit a particular offence enumerated in section 2516 of this chapter”.⁹⁰ Besides, it must be shown that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous”.⁹¹ Finally, the authorities have the obligation to notify persons whose communications were intercepted when the court order expires.⁹²

The USA PATRIOT Act did not modify the procedure used to intercept wire, oral or electronic communications. Section 201 of the USA PATRIOT Act, however, did extend the list of offences for which a federal court may approve a law enforcement request to intercept wire, oral or electronic communication pursuant to the ECPA.

Cloud computing providers qualifying as “electronic communication providers” (e.g. e-mail service providers) can be targeted by an interception order. The impact of the interception of wire, oral or electronic on E.U. citizens' communications in the cloud seems to be relatively low. Indeed, almost 95% of the 2,119 interception orders reported in 2007 were for the interception of wire communications (voice communication).⁹³ ⁹⁴ Only one interception of electronic communications was reported.⁹⁵ This may be explained by the fact that law enforcement may reach similar results under less strict legal requirements as explained hereunder.

2.2.2.2. Access to the Content of Stored Electronic Communication and Communication Transaction Records

Under the ECPA, the FBI may request “content of wire or electronic communications”⁹⁶ ⁹⁷

87 Surveillance Self-defence, “What Can the Government Do?”, *Ssd.eff.org*. Available at: <https://ssd.eff.org/book/export/html/25> [accessed July 2012].

88 *Ibid.*

89 *See*: 18 U.S.C. § 2518

90 18 U.S.C. § 2518 (3)(a).

91 18 U.S.C. § 2518 (3)(c).

92 18 U.S.C. § 2518 (8)

93 Surveillance Self-defence, “What Can the Government Do?”, *o.c.*

94 Although wire communication can occur on the Internet, most of them occurs via the phone.

95 Surveillance Self-defence, “What Can the Government Do?”, *o.c.*

96 18 U.S.C. § 2703 (a) & (b).

97 As amended by section 209 of the USA PATRIOT Act. As a result, just like stored electronic data, stored wire

(e.g. e-mail) and “records concerning electronic communication service or remote computing service”.⁹⁸ “Section 2703 provides greater protection to communication content than to provider records relating to those communications”.⁹⁹

Contents of wire or electronic communications in electronic storage¹⁰⁰ or in a remote computing service may be accessed by a governmental entity according to different procedures.¹⁰¹
¹⁰² Subsections (a), (b) and (d) of section 2703 describe these procedures and read as follow:

18 U.S.C. § 2703 (a) - Contents of Wire or Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to 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. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

18 U.S.C. § 2703 (b) - Contents of Wire or Electronic Communications in a Remote Computing Service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire 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
obtains a court order for such disclosure under subsection (d) of this section;

18 U.S.C. § 2703 (d) - A court order 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant 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.

Records concerning electronic communication service or remote computing service may be accessed by a governmental entity under a warrant or a court order, if the subscriber has given his consent or pursuant formal written request to a law enforcement investigation concerning

communication can be accessed by law enforcement pursuant a search warrant.

98 18 U.S.C. § 2703 (c)

99 C. Doyle, “Privacy: An Overview of the Electronic Communications Privacy Act”, *Congressional Research Service*, March 30, 2011, p. 42. Available at: <http://www.fas.org/sgp/crs/misc/R41733.pdf> [accessed July 2012].

100“Electronic storage” means— (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication (18 U.S.C § 2510 (17))

101 *Guest v. Leis*, 255 F.3d 325, 338 (6th Cir. 2001).

102“Remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system (18 U.S.C § 2711 (2)). For instance, “Youtube” is a remote computing service. See: *Viacom v. YouTube*, 2008 WL 2627388 (S.D.N.Y. 2008).

telemarketing fraud.¹⁰³ Access to record need not to be notify to customer or subscriber in any case.¹⁰⁴ Two types of information are considered as records: subscriber information¹⁰⁵ (Section 2703 (c)(2) ECPA) and electronic communication transactional records (Section 2703 (c)(1) ECPA).¹⁰⁶ The former are for example the names, the addresses, the length of the service, temporarily assigned network addresses, the service payment information, including any credit card or bank account number and the session times and durations.¹⁰⁷ The latter is a residual category. It contains for example server logs, online profiles and screen name.¹⁰⁸

Four important aspects regarding access to the content of stored electronic communication and communication transaction records were amended by the USA PATRIOT Act. First, section 210 of the USA PATRIOT Act enlarges the scope of records of electronic communication accessible pursuant a subpoena. Henceforth, credit card and bank account numbers are accessible to the law enforcement officials.¹⁰⁹ Second, section 212 of the USA PATRIOT Act allows service providers to voluntarily disclose the content of electronic communication in case of emergencies.¹¹⁰ Emergencies encompass danger of death or serious physical injuries. Third, section 212 (b) of the USA PATRIOT Act expressly allows service provider to disclose non-content information.^{111 112} The wording “non-content information” refers to subscriber information (name, login records, network addresses...). Finally, section 220 of the USA PATRIOT Act authorises nationwide service of search warrant for electronic surveillance.

As such, these amendments are relatively minor. They don't modify the procedure relating to the disclosure of customer communications or records. However, it is clear that cloud computing providers can be targeted for such requests. Section 2703 of the ECPA regards cloud computing. Indeed, requests for the content of stored electronic communication and communication transaction records are directed to the electronic communication service or remote computing service.¹¹³

103 18 U.S.C. § 2703 (c)

104 18 U.S.C. § 2703(c)(3).

105 Subscriber information is similar to what is called in E.U. law ‘traffic data’. Traffic data means “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof” (art. 2 E-Privacy Directive). It may, “inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network”. (recital 15 E-Privacy Directive). *See*: 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, July 31, 2002. Data Retention Directive requires providers of publically available electronic communications services or of public communications networks to retain traffic and location data for a certain period of time for the purpose of the investigation, detection and prosecution of serious crime. *See*: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *O.J. L* 105, April 13, 2006, p. 54-63.

106 L. Deutchman, S. Morgan, “The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors”, American Prosecutors Research Institute, July 2005, p. 11. Available at: http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf [accessed February 2012].

107 *Ibid.*

108 *Ibid.*

109 18 U.S.C. § 2703(c)(1)(C).

110 P.L. 107-56, § 212, 18 U.S.C. § 2702 (b) (8).

111 P.L. 107-56, § 212, 18 U.S.C. § 2703 (c).

112 C. Doyle, “Terrorism: Section by Section Analysis of the USA PATRIOT Act”, *Congressional Research Report*, December 10, 2001, p. 9. Available at: <http://epic.org/privacy/terrorism/usapatriot/RL31200.pdf> [accessed June 2012].

113 The distinction is a legal fiction as most cloud computing provider may qualify as both electronic communication service and remote computing service. I. R. Kattan, “Cloudy Privacy Protections: Why the Stored

Service providers such as *Youtube*, *Facebook* or *MySpace*,¹¹⁴ or forum¹¹⁵ qualify as electronic communication service or remote computing service.¹¹⁶ Thus personal data of E.U. citizens using these services may be disclosed to U.S. law enforcement under its request. Besides, service providers themselves may, now, voluntarily disclose information in certain cases.

2.2.2.3. Pen Registers and Trap and Trace Devices

Law enforcement may obtain an authorization from a court upon “certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation”.¹¹⁷ The standard to obtain such an order is low since no probable cause has to be proven. However, only non-content information can be accessed through a such a court order. The aim of this type of order is to identify who a suspect is communicating with and when. A pen registers and trap and trace devices order (hereinafter PR/TT) “shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order”.¹¹⁸

Prior to the USA PATRIOT Act, information that could be intercepted was limited to phone related data. “ ‘Pen register’ device [...] identifies the telephone numbers dialed or pulsed from” and a “ ‘trap and trace’ device [...] identifies the telephone numbers to a particular telephone (incoming calls)”.¹¹⁹

Section 216 of the USA PATRIOT Act extends the scope of information that can be accessed pursuant a pen register or trap and trace order and adapts the terminology to fit with the modern communication technologies (e.g. internet). Prior to the USA PATRIOT Act, section 3123 (b)(1) of the ECPA referenced to the “telephone line” to which the pen register or trap and trace device could be attached or applied to. Henceforth, the pen register or trap and trace device can be attached or applied to a “telephone line or other facility”.¹²⁰ “Such facility includes [...] an Internet user account or e-mail address; or an Internet protocol (IP) address, port number, or similar computer network address or range of addresses”.¹²¹

Moreover, section 216 clarifies that PR/TT orders may be issued to obtain “dialling, routing, addressing, or signalling information”.¹²² Currently, the term “pen register” is defined by the FISA as meaning “a device or process which records or decodes dialling, routing, addressing, or

Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud”, *Vanderbilt J. of Ent. and Tech. Law*, 2011, p. 632. Available at: <http://www.jetlaw.org/wp-content/journal-pdfs/Kattan.pdf> [accessed July 2012].

114 *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010).

115 *Steve Jackson Games v. United States Secret Serv.*, 816 F. Supp. 432, 443 (W. Dist. Tex. 1993).

116 *Ibid.*

117 18 U.S.C § 3122 (b)(2).

118 18 U.S.C § 3123 (b)(1).

119 D. A. Jordan, *U.S. Intelligence Law: A Comprehensive Multimedia Introduction*, 2010, p. 1469. Available at:

http://books.google.be/books?id=KdsUcUIJcLEC&pg=PA1469&lpg=PA1469&dq=%22identifies+the+telephone+numbers+dialed+or+pulsed+from%E2%80%9D+%22+identifies+the+telephone+numbers+to+a+particular+telephone+%28incoming+calls+%29%E2%80%9D&source=bl&ots=35w0IU-AKP&sig=AsIPsXc5pSYWeRp0eEQwDUHfe9w&hl=fr&sa=X&ei=nE4tUK_ABOeK0AXni4HoDA&ved=0CCkQ6AEwAA#v=onepage&q=%22identifies%20the%20telephone%20numbers%20dialed%20or%20pulsed%20from%E2%80%9D%20%22%20identifies%20%20the%20telephone%20numbers%20to%20a%20particular%20telephone%20%28incoming%20calls%29%E2%80%9D&f=false [accessed July 2012].

120 Pub. L. 107–56, §216 (b)(2)(A). 18 U.S.C § 3123 (b)(1).

121 C. Doyle, “Terrorism: Section by Section Analysis of the USA PATRIOT Act”, *o.c.*, p. 12.

122 Pub. L. 107–56, §216 (a)(2). 18 U.S.C § 3123 (c).

signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, [...]”.¹²³ The term “trap and trace device” means “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialling, routing, addressing, and signalling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication”.¹²⁴ Therefore, in any case, content information is excluded from the scope of a Pen register or trap and trace device orders.

The terms “routing, addressing, or signalling”¹²⁵ information deserve some explanations. The wording “routing” information refers to internet use for either e-mail or browsing.¹²⁶ The problem is that even if the content of communication cannot be accessed pursuant pen/trap order¹²⁷, “content cannot easily be separated from internet routing information”.¹²⁸ “Further, an order could not be used to collect information other than dialling, routing, addressing, and signaling’ information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article”.¹²⁹

2.3. Foreign Intelligence Surveillance Act Order

2.3.1. Background Information on the Foreign Intelligence Surveillance Act

Foreign Intelligence Surveillance Act¹³⁰ (hereinafter FISA) was enacted following the “Keith case”.¹³¹ In this case, the U.S. Supreme Court found that every administration engaged in electronic surveillance without prior judicial approval since the 30's.

Therefore, the Congress voted in 1978 the FISA to create a statutory framework for the use of electronic surveillance to collect a certain type of information, “foreign intelligence information”,¹³² about a “foreign power” or an “agent of a foreign power”.¹³³ The terms “foreign intelligence information” refer to information necessary to protect the United States against actual or potential attack, international terrorism or clandestine intelligence activities. A “foreign power” means a faction of a foreign nation or nations, not substantially composed of United States persons and an “agent of a foreign power” means any person other than a United States person, who engages in international terrorism. Thus, FISA governs primarily the gathering of information relating to terrorism activities conducted by foreigners. However, the FISA govern also the gathering of foreign intelligence information regarding foreign affairs.¹³⁴

123 18 U.S.C. § 3127, (3).

124 18 U.S.C. § 3127, (4).

125 18 U.S.C. § 3127, (3) & (4).

126 Anon., “The USA PATRIOT Act, Foreign Intelligence Surveillance and Cyberspace Privacy”, *Cyber.law.harvard.edu*, March 11, 2002. Available at: <http://cyber.law.harvard.edu/privacy/Introduction%20to%20Module%20V.htm> [accessed May 2012].

127 18 USC, § 3121, (c).

128 Anon., “The USA PATRIOT Act, Foreign Intelligence Surveillance and Cyberspace Privacy”, *o.c.*

129 C. Doyle, “Terrorism: Section by Section Analysis of the USA PATRIOT Act”, *o.c.*, p. 12.

130 The Foreign Intelligence Surveillance Act, Pub.L. 95-511, 92 Stat. 1783, October 25, 1978.

131 *United States v. U.S. District Court*, 407 U.S. 297 (1972).

132 *See*: 50 U.S.C. § 1801 (e) (definition of foreign intelligence information).

133 *See*: 50 U.S.C. § 1801 (a) & (b)

134 *See*: 50 U.S.C. § 1801 § (e) (2) (B).

The FISA provides government agencies (e.g. the FBI) with a statutory framework by which they can obtain authorization to conduct electronic surveillance,¹³⁵ physical searches,¹³⁶ utilize pen registers and trap and trace devices,¹³⁷ and access specified business record and any tangible things.¹³⁸ Although some exceptions exist, the Foreign Intelligence Surveillance Court (hereinafter FISC) is the judicial body empowered to grant government agencies authorization in order to conduct these actions. Different standards apply for each type of FISA order. Besides, each FISA order gives access to a different type of information. Therefore, they will be analysed in different sections following the order provided above. Following this, amendments made by the USA PATRIOT Act and subsequent measures will be reviewed in order to understand what difference they make.

2.3.2. FISA Orders for Electronic Surveillance

FISA orders for electronic surveillance give access to the contents of any wire or radio communication.¹³⁹ The wording “wire communication” is defined by the FISA as “any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications”.¹⁴⁰ Besides, the content of wire communication refers to “the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication”.¹⁴¹ “FISA applies both when foreign agents are physically located within the United States and when foreign agents’ communications are routed through the United States. FISA does not apply to communications occurring wholly outside of United States territory”.¹⁴²

Aggrieved persons are not allowed to claim any damage to “any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance”.¹⁴³

Whether or not a court order is necessary to issue a FISA order for electronic surveillance depends on the targeted persons. The Attorney General may authorize surveillance without a court order provided that communication occurred “exclusively between or among foreign powers”.¹⁴⁴ It means that there must be “no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party”.¹⁴⁵ Requirements to issue a FISA electronic surveillance order are low. No predicate crime is required and no “probable cause” that the law is being violated has to be proven.

Section 1804 of the FISA governs FISA order for electronic surveillance of wire communication non “exclusively between or among foreign powers”. An application for a court

135 50 U.S.C. §§ 1801-1808.

136 50 U.S.C. §§ 1822-1826.

137 50 U.S.C. §§ 1841-1846.

138 50 U.S.C. §§ 1861-1862.

139 50 U.S.C. § 1801 (f) (1).

140 50 U.S.C. § 1801 (l).

141 50 U.S.C. § 1801 (n).

142 C. Wolf, “The Role of Government in Commercial Cybersecurity”, *Hldataprotection.com*. Available at: <http://www.hldataprotection.com/uploads/file/WOLFITU%281%29.pdf> [accessed July 2012].

143 50 U.S.C. § 1805 (h).

144 50 U.S.C. § 1802 (a) (1) (A).

145 50 U.S.C. § 1802 (a) (1) (B).

order shall include a statement of the facts and circumstances relied upon by the applicant to justify his belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power,¹⁴⁶ a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.¹⁴⁷

Three sections of the USA PATRIOT Act amends the FISA. First of all, the section 206 of the USA PATRIOT Act amend FISA to allow “roving or multipoint wiretaps”.¹⁴⁸ Prior to the enactment of this provision, the location or facilities subject to the surveillance and the third parties assisting the government (e.g. a cloud computing provider) had to be identified.¹⁴⁹ It was difficult to identify the third parties when a suspect thwarted the identification of any assisting third party by “rapidly changing hotel accommodations, cell phones, Internet accounts, etc, just prior to important meetings or communications”.¹⁵⁰ Therefore, section 206 allowed FISA orders to be directed at “other person” to assist with electronic surveillance if the “Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons”.¹⁵¹

Secondly, section 207 of the USA PATRIOT extended the duration of the FISA Electronic Surveillance Orders up to 120 days, with extensions for up to one year.¹⁵² This amendment will have for effect to facilitate the gathering of personal data.

Finally, Section 218 of the Patriot Act expands the use of FISA requests. Orders may be issued on condition that foreign intelligence gathering is "a significant purpose" of the investigation. Formerly, this requirement was formulated differently. Indeed, orders could be issued as long as the intelligence gathering was the “primary purpose”. Therefore, this change allows the FBI to obtain FISA orders in situations where an investigation is mainly of criminal nature.¹⁵³ “The more lenient standards that the government must meet under FISA (as opposed to the stringent requirements of Title III) are justified by the fact that FISA's provisions facilitate the collection of foreign intelligence information, not criminal evidence. This traditional justification is eliminated where the lax FISA provisions are applicable to the interception of information relating to a domestic criminal investigation. The change is a serious alteration to the delicate constitutional balance reflected in the prior legal regime governing electronic surveillance”.¹⁵⁴

Also, some fear that U.S. Authorities will “use spying and terrorism as an excuse for”¹⁵⁵ gathering foreign intelligence information. “They point to the fact that the number of intelligence wiretaps now exceeds the number of criminal taps. Since these probes are conducted in secret, with

146 50 U.S.C. § 1804 (a) (3).

147 50 U.S.C. § 1804 (a) (5). For the full description of the content of an application for a FISA electronic surveillance order, *see*: 50 U.S.C. § 1804.

148 E. C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *Congressional Research Service*, June 16, 2011, p. 7. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf> [accessed June 2012].

149 50 U.S.C. § 1805(c)(2)(B) (2000ed.).

150 Administration’s Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary, 107th Cong., 1st Sess. 56 (2001), p. 107. Available at: http://commdocs.house.gov/committees/judiciary/hju75288.000/hju75288_of.htm [accessed June 2012].

151 50 U.S.C. § 1805 (c) (2)(B).

152 50 U.S.C. § 1805 (e).

153 Electronic Privacy Information Center, “USA PATRIOT Act Sunset”, *Epic.org*. Available at: <http://epic.org/privacy/terrorism/usapatriot/sunset.html> [accessed May 2012].

154 *Ibid*.

155 L. Abramson & M. Godoy, “The Patriot Act: Key Controversies”, *Nrp.org*, February 2006. Available at: <http://www.npr.org/news/specials/patriotact/patriotactprovisions.html#issue4> [accessed September 2012].

little oversight, abuses could be difficult to uncover”.¹⁵⁶

Cloud computing provider might be requested to provide assistance to execute an electronic surveillance.¹⁵⁷ Provider of wire or electronic communication service can be asked to provide assistance to execute an electronic surveillance. Some providers of wire or electronic communication services are providers of cloud computing services. Therefore, cloud computing providers may provide assistance. As an example, a type of *Skype* conversation could be intercepted¹⁵⁸. Thus, FISA order for electronic surveillance could give the U.S. authorities access to certain wire communication of E.U. citizens in the cloud.

2.3.3. FISA Order for Physical Searches

Physical search is “solely directed at premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers.”¹⁵⁹ Besides, the physical intrusion must take place in the United States.¹⁶⁰ As data centers located in the U.S. are unlikely to be a property used exclusively by, or under the open and exclusive control of a foreign power, FISA physical search order is of little relevance for the purpose of this study.

2.3.4. FISA Pen Register or Trap and Trace Device Orders.

Prior to the enactment of the USA PATRIOT Act, pen register or trap and trace orders could give law enforcement access to the numbers dialled and received by a telephone. Besides, the purpose of FISA pen register or trap and trace orders was limited to investigations to gather information relevant to a foreign intelligence or international terrorism investigation and upon certification that the communications monitored would likely be those of an “agent of a foreign power”.¹⁶¹

Sections 214 of the USA PATRIOT Act amends the FISA pen register or trap and trace device procedure. Section 214 of the USA PATRIOT Act reads as follow:

¹⁵⁶ *Ibid.*

¹⁵⁷ In this sense: R. L. Krutz & R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Indianapolis, Wiley, 2010, p. 139; W. Maxwell & C. Wolf, “Global Reality: Governmental Access to Data in the Cloud”, *A Hogan Lovells White Paper*, May 23, 2012, p. 5. Available at: <http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/0fc74c1d-4dc0-4c1e-9abc-eb50ae5679c4/Hogan%20Lovells%20White%20paper%20-%20Government%20access%20to%20data%20in%20the%20cloud.pdf> [accessed June 2012].

¹⁵⁸ Does FISA order for electronic surveillance apply to *Google Docs*? There is not clear-cut answer. However, it could be considered that *Google Docs* allows its users to communicate as the cloud computing service allows its users to share their work with other users.

¹⁵⁹ 50 U.S.C. § 1822 (a) (A) (1).

¹⁶⁰ 50 U.S.C. § 1821.

¹⁶¹ 50 U.S.C. § 1842 (c)(3) (2000 ed.).

SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.

- (a) APPLICATIONS AND ORDERS.—Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended—
- (1) in subsection (a)(1), by striking “for any investigation to gather foreign intelligence information or information concerning international terrorism” and inserting “for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution”;
- (2) by amending subsection (c)(2) to read as follows: “(2) a certification by the applicant 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 or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.”;
- (3) by striking subsection (c)(3); and
- (4) by amending subsection (d)(2)(A) to read as follows:
- “(A) shall specify—
- “(i) the identity, if known, of the person who is the subject of the investigation;
- “(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
- “(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.”.
- (b) AUTHORIZATION DURING EMERGENCIES.—Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—
- (1) in subsection (a), by striking “foreign intelligence information or information concerning international terrorism” and inserting “foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution”; and
- (2) in subsection (b)(1), by striking “foreign intelligence information or information concerning international terrorism” and inserting “foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution”.

Section 214 (a) (1) of the USA PATRIOT Act expands the purpose for which FISA pen register or trap and trace device orders may be used. Such an order may, now, be authorized “for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities”. Thus, it is no longer necessary to show that the suspect was communicating with an “agent of a foreign power”. As a result, obtaining a FISA Pen register or trap and trace device order is less burdensome than before. Besides, section 214 prohibits any investigation involving a United States person that is “conducted solely upon the basis of activities protected by the first amendment to the Constitution”.¹⁶² The same prohibition applies with respect to emergency procedure (Section 214 (b) USA PATRIOT Act). Therefore, E.U. citizens are more likely to be the target of such an order than a U.S. person.

Also, section 128 (a) of the USA PATRIOT Improvement and Reauthorization Act specifies what customer information relating to the use of the service may be requested. These information include, for example, the name, the address, the temporarily assigned network address or associated

162 50 U.S.C. § 1842, (a), (1).

routing or transmission information, the number of credit card, etc.¹⁶³ “The information to be made available is more extensive than what is available under 18 U.S.C. 2709, or to law enforcement officials, but it is not as extensive as the scope of information under a FISA section 215 “tangible item” order”.¹⁶⁴

Currently, the “pen register” definition and the “trap and trace device” definition are identical to the definitions applicable in criminal law enforcement investigation (*see supra*). Here also, in any case, content information is excluded from the scope of a FISA Pen register or trap and trace device orders.

The procedure to obtain such a FISA order directed at a provider of a wire or electronic communication service is relatively simple. The Attorney General or a designated attorney for the Government may make an application for an order to a judge who shall enter an *ex parte* order.¹⁶⁵ ¹⁶⁶ Orders are issued by the judge upon the FBI's certification that the information are relevant for the need of the investigation.¹⁶⁷ Besides, it is not required that the target of the order be notified.¹⁶⁸

So, the USA PATRIOT Act gives government access to routing information pursuant a FISA pen register or trap and trace device orders issued at a low threshold. Besides, there remains a risk that content information would be disclosed. Pen register or trap and trace orders could potentially be used to accessed U.E. citizens' personal data.

2.3.5. FISA Order for Business Records and Other Tangible Things

Section 215 of the USA PATRIOT Act amends the FISA to reduce the complexity of the procedure that needs to be followed by the Federal Bureau of Investigation to access a broadened range of business records and other tangible things.¹⁶⁹ More precisely, changes were brought to the standard of review (1), the scope of documents subject to FISA was broadened (2), a “gag” provision was introduced in the FISA order (3) and finally orders are issued on a *ex parte* basis (4).

This provision, originally set to expire on December 31, 2005, was extended multiple times until June 1, 2015.¹⁷⁰

163 50 U.S.C. § 1842 (d).

164 C. Doyle & B. T. Yeh, “USA PATRIOT Improvement and Reauthorization Act of 2005: A legal Analysis”, *Congressional Research Service*, December 21, 2006, p. 23. Available at: <http://www.fas.org/sgp/crs/intel/RL33332.pdf> [accessed June 2012].

165 50 U.S.C. § 1842 (d).

166 “Refers to situations in which only one party (and not the adversary) appears before a judge”. *See*: Anon., “Ex Parte”, *Lectlaw.com*. Available at: <http://www.lectlaw.com/def/e051.htm> [accessed July 2012].

167 50 U.S.C. § 1842.

168 50 U.S.C. § 1845.

169 M. Geist & M. Homs, “The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?”, A Submission on the USA Patriot Act to the B.C. Information and Privacy Commissioner”, July 2004, p. 6. Available at: <http://www.docstoc.com/docs/48522538/The-Long-Arm-of-the-USA-Patriot-Act-A> [accessed January 2012].

170 P.L. 112-14, The PATRIOT Sunsets Extension Act of 2011.

Section 215 of the USA PATRIOT Act reads as follows:

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE Act.

Title V of the Foreign Intelligence Surveillance Act of 1978

(50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

“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 (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

“(2) An investigation conducted under this section shall—

“(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

“(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

“(b) Each application under this section—

“(1) shall be made to—

“(A) a judge of the court established by section 103(a);

or “(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and 50 USC 1861.

“(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

“(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

“(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

“(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

“(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

“SEC. 502. CONGRESSIONAL OVERSIGHT.

“(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligencen of the Senate concerning all requests for the production of tangible things under section 402.

“(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

“(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

“(2) the total number of such orders either granted, modified, or denied.”.

First of all, the standard of review was lowered. Previously, in order to get a court order to access business records, law enforcement had to prove “specific and articulable facts” that gave reason to believe that the target of the search was “a foreign power or an agent of a foreign power”. Law enforcement had to prove that the object of the search was for a foreign intelligence or foreign terrorism investigation purpose. Section 215 lowered down the applicable standard to carry out a search. As originally enacted, it was sufficient to specify that the requested records were sought for

foreign intelligence, international terrorism or espionage investigation.¹⁷¹ It meant that particularized suspicion was not required for a court order to be issued. Indeed, the FBI did not need to “show probable cause, nor even reasonable grounds to believe, that the person whose records it seeks is engaged in criminal activity”.¹⁷² The 2005 USA PATRIOT Improvement and Reauthorization Act subsequently changed the standard. Government agencies can seek an order before the Foreign Intelligence Surveillance Court as long as “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence, international terrorism, or espionage investigation]”.¹⁷³

Secondly, the scope of document subject to compulsory production was enlarged. Prior to the USA PATRIOT Act, only some kind of companies could be served with a FISA order (e.g. hotels and motels, automobile rental agencies and storage rental facilities).¹⁷⁴ Section 215 authorizes production of “any tangible things” from any individual or organization (hospitals, bookshops, businesses...) for an investigation “to obtain foreign intelligence information not concerning an United States person or to protect against international terrorism or clandestine intelligence activities”.¹⁷⁵ Besides, there is no limitation on the number of records that can be requested by virtue of a single order.¹⁷⁶ This means that a single order could give access to an entire data base.¹⁷⁷

The term “any tangible things” has raised controversies as to whether electronic data are included in the definition. On the one hand, the word “tangible” is defined by the dictionary as something “perceptible by touch”.¹⁷⁸ Besides, the Act clears up the meaning of “any tangible things” by giving a few examples. It includes “books, records, papers, documents and other items”. In this sense, the Department of Justice has expressed that it is unlikely that the FBI uses a FISA order to access electronic data.¹⁷⁹ However, the wording “tangible things” was later interpreted as including “floppy disks, data tapes, computers and their hard drives, and any type of record in any format”.¹⁸⁰ Therefore, the term “tangible thing” would be deemed to include data electronically stored in the cloud.¹⁸¹ It is hard to consider that electronic personal data as such are “tangible things” since they

171 Pub. L. No 107-56, § 215.

172 This issue was raised by the American Civil Liberties Union. *See*: ACLU, “Reform the Patriot Act Section 215”, *Aclu.org*. Available at: <http://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215> [accessed January 2012].

173 Public Law 109 - 177 - USA PATRIOT Improvement and Reauthorization Act of 2005, § 106(b).

174 50 U.S.C. § 1862(a) (2001). *See also*: E. C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *Congressional Research Service*, June 16, 2011, p. 10. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf> [accessed May 2012].

175 50 U.S.C. § 1861(a)(1).

176 Memorandum, House of Commons Subcommittee on the Treasury, “How secure is the personal information of UK citizens in light of the USA PATRIOT Act and the limited privacy protections of the United States?”, (February 28, 2008), p. 5.

177 *Ibid*.

178 The New Oxford Dictionary of English, Oxford, Judy Pearsall Ed., 1998, p. 1894.

179 U.S. Department of Justice Office, “Questions Submitted by the House Judiciary Committee to the Attorney General on USA PATRIOT Act Implementation”, July 26, 2002. Accessible at: <http://www.fas.org/irp/news/2002/10/doj101702.html> [accessed May 2012].

180 American Library Association, “Analysis of the USA Patriot Act related to Libraries”, *Ala.org*. Available at: <http://www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis.cfm> [accessed April 2012]. In this sense, *see also*: L. Dela Rosa, “Sutdy of Legal Risks Associated With SAAS Migration”, Research paper of Concordia University, October 2011, p. 7. Available at: <http://infosec.concordia.ab.ca/files/2012/04/2011DelaRosa.pdf> [accessed May 2012].

181 A. C. Lakatos, “United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud”, *o.c.*, p. 2; T. Waage & N. Petri, “Government Access to Information in ”the Cloud””, (Kroman Reumert law firm), March 2012, p. 7. Available at: <http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf> [accessed May 2012].

are incapable of being touched. Supporting this claim, Courts in insurance law matters did not reach the conclusion that data stored in computers constitute “tangible property”.¹⁸² So, requesting hard-drives containing personal data fall within the scope the interpretation of “tangible things”. However, requesting the transfer of electronic personal data without seizing any hard-drive would be a far reaching interpretation of “tangible things”.

Thirdly, a “gag” provision is, now, included in FISA orders for tangible things meaning that the party served with such an order is prohibited from disclosing the existence of the order or the fact that information were transferred to the government.¹⁸³ Non respect of this rule might be punished by an imprisonment or a fine.¹⁸⁴ For example, a cloud service provider served with such an order is not allowed to inform the targeted customers. The USA PATRIOT Improvement and Reauthorization Act of the 2005 limits the negative impact of the “gag provision” by authorizing the recipients of a FISA order to contest the gag provision after a period of time of one year.¹⁸⁵

Finally, court order is issued on an *ex parte* basis. This means that the subject of an order cannot intervene in the proceeding.

Among FISA orders, the order for Business Records and other Tangible Things is the most privacy invasive. On basis of such an order, cloud computing provider's hard-drive containing a lot of personal data about their customers could be seized.

What is the impact of FISA order for tangible things on data protection? Section 215 of the Patriot Act turns out to be especially privacy invasive for non U.S. residents. It can't be relied upon section 215 to target U.S. residents with FISA order for tangible thing if the search regards activities protected by the First Amendment of the U.S. Constitution (e.g. freedom of speech, press, religion). However, this section is well applicable to non U.S. residents even when these activities are at stake since the First Amendment applies only to persons residing in the U.S.¹⁸⁶ Besides, the Fourth Amendment which prohibits unreasonable searches is not applicable to non-U.S. citizens or residents located outside the United States.¹⁸⁷

Section 215 opens the door to privacy invasive actions. But to what extent are FISA orders actually used to access personal data? As stated in 2005 by the “Electronic Privacy Information Centre”, FISA order were used to access driver's license records, public accommodation records, apartment lease records, credit card records, and telephone subscriber records.¹⁸⁸ Also, real estate agents, car dealers, casinos, jewellers, boat dealers, insurance brokers, and Internet services providers are the businesses the most at risk to be targeted by a FISA order.¹⁸⁹ Through those companies, it is customers' data that are at risk.

According to some other sources of information, less than 10 business records applications were filed to the Foreign Intelligence Surveillance Court to obtain a FISA order between 2001 and

182 J. N. Love and A. F. Ketchen, “Physical But Not Tangible: Electronic Data Losses”, (RKMC law firm), November 2010, p. 1. Available at: <http://www.rkmc.com/files/Physical-But-Not-Tangible-Electronic-Data-Losses.pdf> [accessed May 2012].

183 Pub. L. No 107-56, § 215; 50 U.S.C. § 1861 (d).

184 M. Geist & M. Homs, “The Long Arm of the USA Patriot Act...”, *o.c.*, p. 7.

185 50 U.S.C. § 1861(f)(2)(A)(i).

186 *United States ex rel. Turner v. Williams*, 194 U.S. 279, 292 (1904).

187 M. Geist & M. Homs, “The Long Arm of the USA Patriot Act...”, *o.c.*, p. 12.

188 Electronic Privacy Information Centre, “USA Patriot Act Sunset”, *o.c.*

189 R. S. Dunham, “The Patriot Act: Business Balks”, *Businessweek.com*, November 2005. Available at: <http://www.businessweek.com/stories/2005-11-09/the-patriot-act-business-balks> [accessed May 2012].

2003.¹⁹⁰ More recently, in 2010, the US government filed 96 applications for the same purpose,¹⁹¹ and in 2011, 205 applications were filed.¹⁹² Thus, while the amount of applications is growing, it remains still at a relatively low level. Alex C. Lakatos outlines three reasons explaining why only a relatively low number of applications are filed: strong protest from the public in general, availability of more efficient means to obtain data, FBI politics.¹⁹³ In an article that makes the apology of the US patriot Act, he concludes that this “Patriot Act tool poses little risk for cloud users”.¹⁹⁴ However, the amount of records actually disclosed remains uncertain since there is no limitation on the number of records that can be disclosed by virtue of a single order. The *Twitter* case illustrates this assertion.¹⁹⁵ Therefore, it would be hazardous to agree with Lakatos that the risk is low for cloud users based only on the number of applications. Moreover, no one knows how the amount of request will evolve in the future. It remains hard to assess the amount of E.U. citizens' data that were requested by FISA orders since the USA PATRIOT Act entered into force since neither the FISA annual report nor any other source gives any direction on that regard. Nevertheless, “many commercial cloud computing providers, such as Microsoft and Google, are potentially subject to such requests, which can be a source of concern for potential non-U.S. customers”.¹⁹⁶ Thus, taking into account the low threshold at which FISA order for tangible items are issued, the increasing number of applications made per years and, the large amount of personal data they may give access to, this legal instrument is a potentially a threat for data protection right of E.U. citizens.

2.3.6. Lone Wolf Provision

The “lone wolf” provision was introduced by section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter IRTPA)¹⁹⁷ and amends the FISA.¹⁹⁸ Prior to the IRTPA, the FISC could only approve a FISA order if probable cause existed to believe that the object of the FISA order was owned or used by a foreign power or its agent.¹⁹⁹ An agent of a foreign power is broadly defined as an individual “involved in international terrorism for or on behalf of those groups”.²⁰⁰ However, demonstrating probable cause to believe that an individual forms a part of a terrorism group turned out to be too difficult in some circumstances.²⁰¹

Section 6001 of the IRTPA eliminated this requirement by providing that any person other

190 *Ibid.*

191 Foreign Intelligence Surveillance Act (FISA) Report. Available at: <http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf> [accessed January 2012].

192 U.S. Department of Justice, “2011 Annual Report to Congress”, April 30, 2012. Available at: <http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf> [accessed May 2012].

193 A. C. Lakatos, “United States: The USA Patriot Act and the Privacy of data Stored in the Cloud”, *o.c.*, p. 2.

194 *Ibid.*

195 More than 600,000 people's personal data were at stake in this case. *See supra.*

196 A. Iqbal, B. Black, C. Fisher, J. Cella, J. Abrams, M. Dugi & R. Leventhal, “Cloud Computing & National Security Law”, The Harvard Law National Security Research Group, p. 20. Available at: <http://www.lawfareblog.com/wp-content/uploads/2010/10/Cloud-Final.pdf> [accessed June 2012].

197 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, approved December 17, 2004.

198 Strictly speaking, the “lone wolf” provision do not form a part of the USA PATRIOT Act. However, it is often analysed as such.

199 50 U.S.C. § 1821-1824 (2001).

200 E.C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *o.c.*, p. 6.

201 Investigations about Zacarias Moussaoui, an individual believed to be responsible for the 9/11 attacks, were hindered due to the facts that FBI agents weren't able to demonstrate that he was an agent of a foreign power.

than a United States person who engages in international terrorism or activities in preparation therefore are considered as agents of a foreign power.²⁰²

Due to this fact, in order to target an individual by a FISA order it is no longer necessary to “provide an evidentiary connection between an individual and a foreign power”.²⁰³

As a result, requirements to issue a FISA order are lowered. Therefore, it could be expected that the number of FISA orders will increase in the next years. Also, the provision targets specifically persons other than citizens or permanent residents of the U.S. Finally, the new standard could lead to “FISA serving as a substitute for some of our most important criminal case”.²⁰⁴ However, the “lone wolf” provision does not target specifically cloud users. Besides, and more importantly, the “lone wolf” has not yet been used in an investigation.²⁰⁵

2.4. National Security Letter: Section 505 of the USA PATRIOT Act

A National Security Letter (hereinafter NSL) is legal instrument comparable to administrative subpoena that “seek customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies”.^{206 207} Unlike with warrants in criminal investigation or with FISA orders, federal officials may issue a NSL without the prior approval of a judge. NSLs and FISA orders for tangible things are corresponding in some respect. Like FISA order for tangible things, NSLs gives access to business records for national security investigation purpose. However, the scope of data that may be requested with a NSL is limited to non-content information. Besides, the amount of NSLs issued by year exceeds by far the number of FISA orders for tangible things.

Prior to the adoption of the Patriot Act, the U.S. had already four statutes authorizing certain government agencies, primarily the FBI, to issue NSLs: the Right to Financial Privacy Act,²⁰⁸ the National Security Act,²⁰⁹ the Fair Credit Reporting Act,²¹⁰ and the Electronic Communications Privacy Act (hereinafter: ECPA).²¹¹ The USA PATRIOT Act added a fifth one and amended three of existing ones. For the purpose of this study, the ECPA is especially interesting as it regards wire or electronic communication service provider.

The section 505 of the Title V of the USA PATRIOT Act, entitled “Removing Obstacles to Investigating Terrorism”, facilitates the issuance of NSLs under the ECPA. This section reads as follows:

20250 U.S.C. § 1801 (b) (2) (c).

203 E.C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *o.c.*, p. 6.

204 S. Rept. 108-40 at 73. Available at: <http://www.gpo.gov/fdsys/pkg/CRPT-108srpt40/html/CRPT-108srpt40.htm> [accessed July 2012].

205 E.C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *o.c.*, p. 7.

206 C. Doyle, “National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments”, *Congressional Research Service*, p. 1. Available at: <http://www.fas.org/sgp/crs/intel/RS22406.pdf> [accessed February 2012].

207 See in appendix I for copy of an NSL.

208 Right to Financial Privacy Act, Pub. L. 95-630, 92 Stat. 3697, November 10, 1978.

209 National Security Act, Pub. L. 80-253, 61 Stat. 495, July 26, 1947.

210 Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114, October 26, 1970.

211 Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848, October 21, 1986.

SEC. 505. MISCELLANEOUS NATIONAL SECURITY AUTHORITIES.

(a) TELEPHONE TOLL AND TRANSACTIONAL RECORDS.—Section 2709(b) of title 18, United States Code, is amended—

(1) in the matter preceding paragraph (1), by inserting

“at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director” after “Assistant Director”;

(2) in paragraph (1)—

(A) by striking “in a position not lower than Deputy Assistant Director”; and

(B) by striking “made that” and all that follows and inserting the following: “made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or 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; and”;

(3) in paragraph (2)—

(A) by striking “in a position not lower than Deputy Assistant Director”; and

(B) by striking “made that” and all that follows and inserting the following: “made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”.

Section 505 of the USA PATRIOT Act gives, first, the government the power to issue NSLs in any case that is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities”.²¹² The requirement that the records sought pertain to a foreign power or an agent of a foreign power no longer exists. As a result, NSLs may be issued even when “the precise relationship (if any) of a subject to a specific terrorist organization or other foreign power has yet to be established. It also means that information is more likely to be gathered from people several steps removed from a foreign power or its agents and is more likely to pertain to individuals no ultimately of interest”.²¹³ Second, it expands the FBI's authority to serve NSL beyond its headquarters to its 56 field offices.^{214 215} Finally, it limits the NSL's reach for United States person. These cannot be the object of an investigation “conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States”. Thus, “the amendments allowed NSL authority to be employed more quickly (without the delays associated with prior approval from FBI headquarters) and more widely (without requiring that the information pertain to a foreign power or its agents)”.²¹⁶

The USA PATRIOT Improvement and Reauthorization Act has brought two major changes regarding the confidentiality requirement and the judicial review of both the NSLs and the confidentiality requirement that attend them. Prior to the USA PATRIOT Improvement and Reauthorization Act, the recipients of a NSL were prohibited from disclosing that the FBI has sought information. Section 116 of the USA PATRIOT improvement and Reauthorization Act brought a change to the confidentiality rule. Now, the wire or electronic communication service providers may disclose that the FBI has sought or obtained access to certain information to any person unless the FBI has decided otherwise. Besides, in any case, the recipient is not bound to

212 This standard is less strict than the probable cause standard to obtain a search warrant.

213 A. C. Henning, E. B. Bazan, C. Doyle & E. C. Liu, “Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization”, *o.c.*, p. 15.

214 18 U.S.C. § 2709 (b).

215 U.S. Dept. of Justice - Office of the Inspector General, “A Review of the FBI's Use of NSLs”, March 2007. Available at: www.usdoj.gov/oig/special/s0703b/final.pdf [accessed February 2012].

216 C. Doyle, “National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments”, *Congressional Research Service*, September 8, 2009, p. 4. Available at: <http://www.fas.org/sgp/crs/intel/RL33320.pdf> [accessed June 2012].

secrecy when disclosure is necessary to comply with the request or to obtain legal advice.^{217 218}

Then, section 115 of the USA PATRIOT improvement and Reauthorization states that the recipient may challenge the confidentiality requirement before a court. Besides, the recipients may also petition and be granted an order aiming to “modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful”.

Under ECPA, section 2709, the FBI may request from wire or electronic communication service providers information relating to their customers. They are the customer's name, address, length of service and billing record. The purpose of a NSL under ECPA is to acquire information relevant “an authorized investigation to an investigation to protect against international terrorism or clandestine intelligence activities”.

The analysis of the impact of National Security Letters on data protection in the cloud connects to the idea of how the cloud industry and the cloud users are affected by the NSL's.

Although some authors argue that the USA PATRIOT Act only brought minor changes to the NSL statutes and that the impact of NSLs on privacy is not that significant,²¹⁹ it is clear that the cloud industry and cloud users are affected in a great measure by the NSLs.

First of all, it should be kept in mind those authors express their opinion in a way that makes the “apology” of the US Patriot Act.

Secondly, even if the scope of data that can be accessed pursuant NSLs is limited to non-content information, the quantity of NSLs issued by years has significantly increased since the enactment of the USA PATRIOT Act. Numbers regarding NSLs concerning United States person are published by the U.S. Department of Justice.²²⁰ Even if those numbers only regard U.S. persons, they give an idea of what the worldwide tendency could be.

Year	2005	2006	2007	2008	2009	2010	2011
Numbers	9254	12583	16804	24744	14788	24287	16511

Table II: NSL - figures

Moreover, it should be noted that the major part of these requests regarded telephone or e-mail communication meaning that cloud computing providers, among others, are heavily targeted by NSLs.²²¹ As a result, the amount of data that need to be transferred to U.S. authorities is so important that certain electronic communications service providers served with NSLs no longer comply with all requests.²²² This tendency which began in late 2009 was revealed by the FBI in a

217 18 U.S.C § 2709, (c)

218 *Doe v. Ashcroft* 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004).

219 A. C. Lakatos, “United States: The USA Patriot Act and the Privacy of data Stored in the Cloud”, *o.c.*, p. 3.; W. Maxwell & C. Wolf, “A Global Reality: Governmental Access to Data in the Cloud”, *o.c.*, p. 5.

220 Report of the Department of Justice. Available at: <http://www.fas.org/irp/agency/doj/fisa/2012rept.pdf>
<http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>; <http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>; <http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf>; <http://www.fas.org/irp/agency/doj/fisa/2006rept.pdf> [accessed July 2012].

221 *Ibid.*

222 E. Nakashima, “FBI going to court more often to get personal Internet-usage data”, *Washingtonpost.com*, October 25, 2011. Available at: <http://www.washingtonpost.com/world/national-security/fbi-going-to-court-moreoften-to-get->

response to a question from the Senate Judiciary Committee. On the one hand, this factual situation limits the invasion of privacy in the cloud. How long this factual situation will continue is, however, uncertain. On the other hand, it implies that the amount of requests is so important that some cloud providers are overloaded and turn out to be unable to answer all of them.

Thirdly, cloud computing providers often disclose more data than actually requested. By doing so, they make sure that they fully comply with a NSL. Also, they avoid wasting time looking for the exact data in the server. While it would be possible for cloud computing providers to disclose the strict minimum of information and thus cooperate with the U.S. authorities in the lesser way, most cloud users have very limited power to request this from their cloud computing provider. Conversely, Lakatos argues that “users also can reasonably ask that their cloud service providers limit what they share in response to a NSL to the minimum required by law. If cloud service providers do so, then their customers’ data should typically face only minimal exposure due to NSLs”.²²³ How can users “ask” their cloud provider to share only the minimum required by law since the contracts are usually not negotiated? In the scenario of an important company, this could be conceivable. However, individual users have no or very limited power to do this kind of request. Moreover, is this “minimum” of information not already too much?

While it is clear that NSLs can give personal information in the cloud, their impact of E.U. citizens remain difficult to assess.

2.5. Comparison of NSL and FISA Order

As a matter of clarification, NSL and FISA orders will be compared in this section. Although NSL and FISA order share common characteristics, they are a significant differences between these two legal instruments. For more readability, the compared features will be presented in a table.

Features / Legal Instrument	FISA order	NSL
Purpose	Access of data “justified by national interests other than criminal law enforcement”. ²²⁴	Idem.
Legal source	Foreign Intelligence Surveillance Act which is part of the Title 50 U.S.C entitled “War and National Defence”.	There are five NSL statutes.
Sunset	Section 215 is supposed to sunset in 2015.	Amendments made to the NSL are permanent.
Procedural process	Approval from the FISC is necessary to issue a FISA order.	No court approval is required. NSLs are issued by federal agency officials.
Scope of data accessible	Broad scope. Relates to content information.	Narrow scope. Relates to non-content information.

personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html [accessed February 2012].

223 A. C. Lakatos, “United States: The USA Patriot Act and the Privacy of data Stored in the Cloud”, *o.c.*, p. 4.

224 E. C. Liu, “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *o.c.*, p.

Gag order	In principle, a “gag order” attend FISA order.	In principle, no “gag order”.
Number of orders	Low.	High.

Table III: Comparison: NSL -FISA order

2.6. Conclusion

The USA PATRIOT Act amends a broad series of laws. We are interested in those governing U.S. authorities access to data in criminal investigation, foreign intelligence investigation and national security.

Thus, USA PATRIOT Act did not create any new instrument as such. Instead, it bolstered existing ones. First, it adapts the language of existing law to make them applicable to new technologies (pen register, tap and trace device, electronic communication). Although none of these adaptations target cloud computing as such, it made possible the access of data stored by third party in the cloud. Second, it facilitates the issuance of disclosure order by lowering the substantial and procedural standards that need to be met. Third, it expands the scope of data accessible pursuant certain kind of order (e.g. FISA order for tangible things).

Among those bolstered legal instruments, two instruments have particularly raised concerns in the cloud computing community. They are so-called national security letters and the FISA order for tangible things. Both could be used to access data stored in the cloud. While the NSLs only give access to non-content information, their number is significant and has been rising since the enactment of the USA PATRIOT Act. Besides, although, the number of FISA order for tangible things remains at a low level, the scope of data accessible is really broad. Therefore, they represent the greatest cause of worrying.

It remains difficult to determine how many orders have targeted E.U. citizens. However, the rising number of orders issued by year increases, without any doubt, the likelihood that E.U. citizens' personal data are disclosed to U.S. authorities.

Chapter 3. European Union Data Protection

The U.S. authorities have powerful tools, enhanced by the USA PATRIOT Act, to require customers' personal data from cloud computing providers. Disclosure orders issued by the U.S. may result in the disclosure of personal data protected by the E.U. law, particularly the Data Protection Directive (hereinafter: DPD).²²⁵ The applicability regime of the DPD and the jurisdictional scope of the U.S. law may conflict. The result is that cloud computing providers may be subject to the obligations of the DPD and those from the U.S. at the same time. Mutual legal assistance treaties exist to avoid this conflict of jurisdiction.

First, the cloud actors will be described. Secondly, the scope of applicability of the DPD will be explained. The third part of the Chapter sets forth the obligations resulting from the applicability of the DPD. Among those obligations, a particular one, legitimate processing, will be deeply analysed in the fourth part of this chapter. Finally, rules on transfer of data and cooperation treaty will be reviewed.

3.1. A trilateral Relationship: Controller, Processor and Data Subject

This section aims to identify the actors of cloud computing and the complex relationships they entertain with each other giving, thus, a clear a picture of what cloud computing is from a legal point of view. There are three main actors in the cloud computing relationship: the controller, the processor and the data subject. After having defined the cloud actors, I will underline the fact the distinction is not that clear cut. Finally, their respective obligations will be set forth. The DPD defines all three actors.

The “data subject” is the natural person “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” and whose personal data are processed.²²⁶

The controller is “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”.²²⁷ Therefore, to be qualified as a controller one must be position to take the decision regarding the “purpose and means of the processing”.

The processor is “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”.²²⁸ Therefore, the processor is the one which acts according to the instruction of the controller without taking any decision regarding “purpose and means of the processing”. It only executes material acts. “Processing of personal data” is defined by the DPD as “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

225 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 n 28*, November 23, 1995, p. 31.

226 Art. 2 (a) DPD.

227 Art. 2 (d) DPD.

228 Art. 3 (e) DPD.

making available, alignment or combination, blocking, erasure or destruction”.²²⁹

The qualification of controller or processor might be more complex than it seems to be in some circumstances. It can be considered that the data subject is the data controller and the cloud service provider is the data processor. However, a single actor may be at the same time processor and controller.²³⁰ For example, “Facebook” might be considered as a data processor when an individual, data controller, posts personal data about himself. However, “Facebook” will be considered as a data controller when it determines the purpose of the processing, e.g. if it hands over these data to a marketing company or to the U.S. authorities without the consent of the data subject.

3.2. Applicability of the Data Protection Directive

The applicability regime of the EU data protection directive is very broad. The connecting factor of the directive is based on the territoriality principle.²³¹ The applicability regime is based on two rules.

The main rule which regards cases where the controller has an establishment on the territory of the member state is contained in article 4(1)(a) of the Data Protection Directive:

“Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable”.

Three comments need to be made about this provision. First, the wording means that not only the primary establishment of the controller triggers the application of the DPD, but also any secondary establishment based on a Member state territory.²³² Indeed, the processing of data carried out in the context of the activities of an establishment of a controller located on in the E.U. triggers the applicability of the Directive. Otherwise, it would be enough to relocate the processing outside the E.U. to circumvent the application of the DPD. Thus, the place where the processing take place is irrelevant. Second, the Directive applies even when the processing is carried out by a third party located outside the E.U. but in the context of the activities of an establishment in a Member State.²³³ Third, the nationality of the people's data involved is irrelevant.²³⁴

The default rule regards cases where the controller has no establishment on the Community territory (art. 4(1)(c) DPD).

229 Art. 2 (b) DPD.

230 For more details about the these concepts, *see*: W. Kuan Hon, C. Millard and I. Walden, “Who is Responsible for ‘Personal Data’ in Cloud Computing? The Cloud of Unknowing, Part 2”, *International Data Privacy Law*, 2012, Vol. 2, No. 1. Available at: <http://idpl.oxfordjournals.org/content/2/1/3.full.pdf+html> [accessed on April 2012].

231 E.M.L. Moerel, *Binding Corporate Rules – Fixing the Regulatory Patchwork of Data Protection*, P.H.D. Thesis, University of Tilburg, 2011, p. 57.

232 E.M.L. Moerel, *o.c.*, p. 49.

233 E.M.L. Moerel, *o.c.*, p. 67.

234 E.M.L. Moerel, *o.c.*, p. 57. *See also*: Working Party 29, “Opinion 8/2010 on Applicable Law”, December 16, 2010, p. 8. Available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf [accessed on April 2012].

“Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community”.

In such a case, the DPD will be applied when the controller “make use of equipment” for the purposes of processing personal data situated on the territory of a Member States (art. 4(1)(c) DPD). The term “equipment” refers to automated or non-automated physical objects.²³⁵ Also, a controller “makes use” of equipment “if he is in actual control of this equipment”. This provides the legitimation to subject him to the laws of a Member State. “Decisive here for is the control over the manner of processing personal data, whereas the private law ownership and the bearing of costs are not decisive”.²³⁶

Whether or not article 4(1)(c) applies to data collected by means of cookies by a U.S. website remains subject to controversy. A cookies is a small piece of data sent from a website and thereafter stored in a user's computer. Cookies usually contain an identification code that allows the website to recognize the user when the website is visited from the same computer again.²³⁷ They can fill three different purposes: session management, personalization and tracking.²³⁸ Users have the possibility to change the cookies settings on their web browser. Today cookies are used by almost all websites. Let's take the case of an E.U. citizen who visit a U.S. company's website not supported by any local advertisements within the E.U. and which merely provides product information. The website doesn't use cookies to collect personal information.²³⁹ The WP 29 is of opinion that the article 4(1)(c) does apply. It considers the user's computer as equipment located on the territory of a member state that a controller uses for the purpose of processing personal data leaving the data subject without any control of many operations.²⁴⁰ Therefore, the DPD applies to all processing of personal data of E.U. visitors of non-E.U. Websites.²⁴¹ The Working Party 29 construes the territoriality principle as protecting all individuals on the E.U. territory.

Therefore, following the opinion of the WP 29, the Directive has a long-arm reach. The directive applies to large variety of cases whether or not the cloud computing provider has an establishment on the EU territory.

3.3. Obligations

Individuals or companies subject to the DPD have to observe different obligations.

The controller has to process the personal data legitimately (art. 7 DPD). Also, the controller

235 E.M.L. Moerel, *o.c.*, p. 105.

236 C. Kuner, *European Data Protection Law: Corporate Compliance Regulation*, Oxford, Oxford University Press, 2007, at 121.

237 E.M.L. Moerel, *o.c.*, p. 113.

238 Wikipedia, “HTTP Cookies”, *Wikipedia.org*. Available at: http://en.wikipedia.org/wiki/HTTP_cookie [accessed June 2012].

239 This case is taken from: E.M.L. Moerel, *o.c.*, p. 114.

240 Working Party 29, “Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites”, May 2002, p. 11. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf [accessed May 2012].

241 However, a contrary opinion is expressed by Lokke Moerel. The reasoning of this author can be summarized in two points. First, “there is no making use of equipment as there is no control”. Indeed, users can change the cookies settings and even disable cookies. Second, “there is no physical equipment that is physically situated on EU territory” as cookies are only pieces of text. *See*: E.M.L. Moerel, *o.c.*, p. 115.

has to provide the data subject with information regarding collected data (art. 10 DPD), the right to access (art. 12 DPD) and to correct (art. 6(d) DPD) their personal information. Besides, the controller bears also obligations regarding the confidentiality and the security of the data (art. 16 and 17,1 DPD). To name a last one, the controller has to notify the supervisory authority of its processing operation (art. 18 DPD). Therefore, the controller has the obligation to offer compensation to “any person who has suffered damage as a result of an unlawful processing operation”.²⁴²

The processor must only process the personal data under instruction of the controller. Also, the processor is bound to ensure the security of the data.

3.4. Legitimate Processing

The legitimate processing obligation borne by cloud computing provider deserves more explanations. Does a cloud computing provider process data subjects' personal data legitimately when it complies with a Disclosure request from the U.S?

Criteria to make the processing legitimate are set forth by the article 7 of the DPD. In these circumstances, three of these criteria could make the processing legitimate, ie the disclosure of personal data to the U.S. authorities: Data processing would be legitimate if “the data subject has unambiguously given his consent” (art. 7 (a) DPD); if the “processing is necessary for compliance with a legal obligation to which the controller is subject” (art. 7 (c) DPD) or if “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)” (art. 7 (f) DPD).

The processing is legitimate if the data subject gave its consent. Consent has to be “specific”, “informed” and “freely given” (art. 2 (h) DPD). “Consent implies that the data controller has given the relevant information about the purposes and extent of the data processing for which consent is given”.²⁴³ This could hardly be the case since a “gag order” often attends disclosure order. Therefore, cloud computing providers are not allowed to inform their customer of the disclosure. Besides, a data subject should be allowed to withdraw its consent without prejudice.²⁴⁴ This is difficult to imagine in these circumstances. Hence, the data subject is not in a position to give its consent that could make the disclosure of its data to the U.S. authorities legitimate. However, the situation is different when the data subject gave its consent to the terms of service allowing such processing. In this case, such a processing is deemed legitimate. The validity of the consent may, nevertheless, “be questioned in case of repeated or even structural transfers or if the transfer in question is disproportionate”.²⁴⁵

Subsidiarily, when the data subject did not give its consent, a legal obligation borne by the cloud computing provider could justify such a processing. Does a legal obligation directly imposed by the U.S. authorities on a cloud computing provider make the processing legitimate? A literal interpretation of article 7 (c) of the DPD would lead to a positive answer. However, the WP 29 drew a different conclusion on basis of a teleological interpretation of article 7 (c) of the DPD.

242 Art. 23 DPD.

243 E.M.L. Moerel, *o.c.*, p. 208.

244 *Ibid.*

245 E.M.L. Moerel, *o.c.*, p. 209.

According to the WP 29 “an obligation imposed by a foreign legal statute or regulation [...] may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive”.²⁴⁶ Hence, article 7 (c) of the DPD can not be invoked to make the processing legitimate.

Finally, legitimate interest of the cloud computing providers could suffice to legitimate the processing according to article 7 (f) of the DPD.²⁴⁷ Cloud computing providers certainly have an interest in complying with an order from U.S. Indeed, by doing so, they avoid being sanctioned. However, a balance between the cloud computing provider's interests and the data subject's interests has to be struck. Indeed, interests for fundamental rights and freedoms (ie privacy and data protection) of the data subject have to be taken into account as well. It is unsure whether these interests are generally taken into account by the cloud computing providers. Moreover, when data processing is based on article 7(f), article 14 (a) of the DPD states that the data subject has the right to object at any time on compelling legitimate grounds to the processing of data relating to him. Even when no “gag order” attends a Disclosure order, it is unlikely that the data subject is in a position to oppose the disclosure as provided by the DPD. Therefore, cloud computing providers could hardly invoke article 7 (f) of the DPD to legitimate disclosure of personal data to the U.S. authorities.

Depending on the situation and on the interpretation of the DPD, the disclosure of personal data to the U.S. authorities may or may not be considered as a legitimate processing.

3.5. E.U. Transfer Rules and Mutual Legal Assistance Treaty

3.5.1. E.U. Transfer Rules

This part aims to briefly discuss rules regarding the transfer of personal data outside the EEA and more particularly to the U.S. The transfer of personal data to third countries is subject to the rules of Chapter 4 of the DPD. Chapter 4 sets out a principle followed by series of exceptions.

In principle, the DPD only authorises data transfers from the E.U. to third countries on condition that they ensure an adequate level of protection (art. 25 DPD). This principle suffers from two main exceptions.²⁴⁸ First, data subject is authorised to give its consent for such a transfer (art 26(1)(a)). Consent has to be “freely given”, “specific and informed” as required by article 2(h) DPD.²⁴⁹ Second, the companies that adhere to the E.U.-U.S. “Safe Harbour” framework are

246 Working Party 29, “Opinion 1/2006 on the application of the EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against, banking and financial crime”, p. 8. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf [accessed July 2012].

247 See also the opinion of the WP 29 in the SWIFT case: Working Party 29, “Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)”, pp. 18-19. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf [accessed July 2012].

248 There is a third exception. Transfer of personal data to countries which received the adequacy finding is allowed. However, the USA did not receive the adequacy finding meaning that the USA do not ensure an adequate level of protection. Therefore, it is unnecessary to further explore this exception.

249 See discussion about the validity of consent: Working Party 114, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995”, November 2005. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf [accessed in May 2012].

authorised to transfer personal data between the E.U. and the U.S.²⁵⁰

Do the exceptions apply to the transfer of personal data to the U.S.? When the data subject gave its consent to the terms of service allowing such transfer, such processing is lawful. Nevertheless, the validity of the consent can be questioned. Besides, if the data subject did not give its consent for such a data transfer, this processing should be deemed unlawful.

The second derogation, the “safe harbour”, is a set of seven privacy principles deemed to provide adequate protection for transfers of personal data from the EU.²⁵¹ Cloud computing provider adhering to the safe harbour may transfer E.U. citizens' personal data from the E.U. to the U.S. lawfully. “The remote risk of a data access by U.S. authorities based on the Patriot Act does not preclude this”.²⁵²

In conclusion, E.U. data protection regime might render such a data transfer to the U.S. authorities pursuant unlawful depending on the situation.

3.5.2. How Should the U.S. Authorities Access E.U. Citizens' Personal Data?

It is beyond the scope of this thesis to expose extensively the procedural requirements for the exchange of personal data.²⁵³ This part rather illustrates that formal procedures exist to exchange personal data between the U.S. and the E.U. Therefore, it shows that there is an alternative to the U.S. unilateral requests.

Cooperation between the U.S. and the E.U. may take place in presence of a multilateral or bilateral agreement or outside the scope of such an agreement.

3.5.2.1. Exchange of Personal Data in Absence of an Agreement

The exchange of personal data in absence of an agreement take place via two different manners: letters rogatory and “cop to cop” exchange.²⁵⁴

Letters rogatory are the “customary method of obtaining judicial assistance from abroad in the absence of a treaty or executive agreement. Letters rogatory are requests from courts in one country to a court of a foreign country to assist in effecting service of process or taking of evidence if permitted by the laws of the foreign country”.²⁵⁵ Rules governing the letters rogatory originate from national legislation. However, the principles laid down in the data protection directive have to be complied with. Due to the absence of definite standards about their content, the process can be

250 Decision of the Commission of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US, 2000, *O.J. L* 215/7.

251 About “safe harbor”, see: Anon., “Safe Harbor Workbook”, *Export.gov*. Available at: http://export.gov/safeharbor/eg_main_018238.asp [accessed in May 2012].

252 J. Whelan & S.-A. Hinfey, “No Cloud Over the Patriot Act”, (A&L Goodbody law firm), March 2012, p. 15. Available at: <http://www.irelandip.com/uploads/file/No%20Cloud%20over%20Patriot%20Act%281%29.pdf> [September 2012].

253 For a very detailed analysis, see: E. De Busser, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities*, Antwerpen, Maklu, 2009.

254 E. De Busser, *o.c.*, p.305.

255 U.S. Department of State, “Preparation of Letters Rogatory”, *Travel.state.gov*. Available at: http://travel.state.gov/law/judicial/judicial_683.html [accessed June 2012].

slow.²⁵⁶ As a consequence, the efficiency of letters rogatory is limited.

“Cop to cop” cooperation is the second way to exchange personal data in absence of a treaty. This method can be defined as the cooperation between police officers from an E.U. Member-state and from the U.S. whose aim is to exchange data as long as no compulsory process is required.²⁵⁷ This suggests that this type of cooperation is lawful. However, some Member-states have the perception that such “contacts may trigger violations of domestic privacy laws”.²⁵⁸

3.5.2.2. Exchange of Personal Data in Presence of an Agreement

U.S. and E.U. can exchange personal data by means of bilateral or multilateral mutual legal assistance treaties (MLATs). Besides, the adequacy of the third state's level of data protection must be assessed in certain cases.

3.5.2.2.1. Multilateral treaties

The conclusion of multilateral agreement between the U.S. and one or more E.U. Member State(s) is a common practice to regulate mutual assistance in criminal matters.²⁵⁹ The transfer of personal data is a part of the mutual assistance.

These conventions share a number of common characteristics aiming to protect personal data. First, they leave the possibility open for a party to refuse assistance. Secondly, they contain provisions limiting the use that can be made of the transferred data. Thirdly, most of them contain a speciality rule stating that the transferred personal data cannot be used by the requesting party for other investigation or proceeding than those stated in the in the request.

3.5.2.2.2. Bilateral Treaties

There is a certain number of bilateral MLATs between E.U. Member-states and the U.S. The treaties usually contain provisions regarding grounds for refusal, use limitation and a speciality rule. They offer some privacy safeguards. However, their usefulness is limited since they are applicable only in certain situations (*see infra*).²⁶⁰

“In an MLAT process, an LEA in Country A formally requests an LEA in Country B to conduct the evidence-gathering. If the request is granted, Country B lets its LEA serve the production order or subpoena on the Country B CSP. In the process it provides any notice or judicial approval required by Country B. Once the CSP retrieves the suspect data from its repository, it delivers the data to the Country B LEA, and the Country B LEA forwards it to the

256 E. De Busser, *o.c.* p. 305; *See also*: M.M. Richard, “International Assistance in Combating Crime”, in B. De Ruyver, G. Vermeulen and T. Vander Beken (eds.), *Strategies of the EU and the US in Combating Transnational Organized Crime*, Antwerpen, Maklu, 2002, p. 233.

257 *Ibid.*

258 M.M. Richard, “International Assistance in Combating Crime”, *o.c.*, p. 232.

259 Example of these are the 1997 International Convention for the suppression of Terrorist Bombings, the 1999 International Convention for the Suppression of the Financing of Terrorism and the 2000 Convention against Transnational Organized Crime.

260 Noerr LLP & SNR Denton LLP, “The USA PATRIOT Act - Implications for Cloud Computing”, *Snrrenton.com*, April 2012, p. 18. Available at: http://www.snrrenton.com/pdf/USA_Patriot_Act_Cloud_Computing.pdf [September 2012].

Country A LEA”²⁶¹.

These bilateral treaties are now subject to the provisions of the 2003 Agreement on Mutual Assistance between the E.U. and the U.S.^{262 263} This agreement aims to enhance cooperation and mutual legal assistance between the U.S. and the E.U. (art 1 MLA). This mutual legal assistance includes the exchange of data between administrative authorities contemplating to start a criminal investigation or prosecution (art 8 (1) MLA). This means that requests for assistance will be refused if the requested “administrative authority anticipates that no prosecution or referral, as applicable, will take place” (art. 8 (1) MLA). This provision might explain the reason why the U.S. are reluctant to use this agreement to obtain personal data from the E.U. Besides, the use of the exchanged data is not unlimited. Indeed, the article 9 of the 2003 Agreement limits the use that can be made of these personal or other data. Apart from this provision, the explanatory note on the agreement states that refusal of assistance is justified only in exceptional cases. Indeed, article 9(2) (b) excludes “generic restrictions with respect to the legal standards of the requesting State”.

3.5.2.2.3. Is Mutual Legal Assistance the Panacea?

Mutual legal assistance Treaties or Agreement governing the exchange of personal data were negotiated between the E.U. and the U.S. If it cannot be denied that procedures are available to govern the exchange of data, one question remains: do they offer sufficient safeguards to protect privacy of the E.U. citizens. To answer this question, the 2003 Agreement on Mutual Assistance between the E.U. and the U.S. is analysed.

The 2003 Agreement on Mutual Assistance between the EU and the US is not exempt from critics. First of all, the adequacy requirement is disregarded as article 9 (2)(b) of the Agreement bans all generic restrictions with respect to the legal standards of the requesting State.²⁶⁴ Secondly, the Agreement does not contain a speciality rule. It means that the information exchanged pursuant to a particular request can be used for other cases than the one specified in the request.²⁶⁵ As a consequence, the door is opened for “use of personal data by the requesting party for a number of cases in which the exchange should have been refused”.²⁶⁶ Thirdly, the quality of personal data requirement is not included in the Agreement. Fourthly, article 9 of the Agreement contains very wide purpose limitation rules. Concretely, it means that the U.S. could use the exchanged information for “a range of purposes that are not necessarily related to the original request”.²⁶⁷ Finally, the Agreement does not contain any data retention rule. Since the U.S. do not have a general data retention standard, some exchanged information might be stored forever by the U.S.

It shows that even when legal solutions are negotiated, privacy and data protection are far from being protected. As Els De Busser noted: “the objective 'to protect personal data' and other data sounds rather ironic”.²⁶⁸

261 J. M. Margolis, “The European Union v. the Patriot Act: Do U.S. Criminal Investigations Violate E.U. Civil Rights”, White Paper Prepared for: International Communication and Information Policy Group Bureau of Economic, Energy, and Business Affairs U.S. Department of State, *Subsentio.com*, November 2011, p. 11. Available at: <http://www.subsentio.com/index.php/eng/Site-Archive/White-Papers> [September 2012].

262 Agreement on Mutual Legal Assistance Between the European Union and the United States of America, *O.J.* L 19 July 2003, p. 41.

263 For more details about the MLA agreement, see: E. De Busser, *o.c.*, pp. 346-358.

264 E. De Busser, *o.c.*, p. 352.

265 E. De Busser, *o.c.*, p. 336.

266 E. De Busser, *o.c.*, p. 356.

267 E. De Busser, *o.c.*, p. 358.

268 E. De Busser, *o.c.*, p. 356.

3.6. Conclusion

This chapter aimed at describing some aspects the E.U. data protection law with respect to cloud computing. The main actors of cloud computing and their obligations were described. The upshot is that it is not always easy to determine who is the controller and the processor. Secondly, the scope of applicability of the DPD was clarified to understand when cloud computing providers fall under the its scope. It can be said that the scope of applicability of the DPD is very broad. Then, obligations of stakeholders subject to the DPD were described. It was subsequently demonstrated that handing over E.U. citizens' personal data to the U.S. authorities does not breach the legitimate processing obligation and the E.U. transfer rules under certain condition. However, even if the U.S. authorities access these personal lawfully, it does not mean that this factual situation is desirable for E.U. citizens or E.U. companies who care about their privacy. Finally, the negotiated solutions to exchange personal data between the U.S. and the E.U. were discussed.

Chapter 4. When Two Regimes Conflict – Implications for E.U. Cloud

Users

The primary aim of this chapter is to show, concretely, what the implications are for E.U. cloud customers. To this end, six scenarios illustrating the extra-territorial effect of the U.S. disclosure orders on E.U. citizens will be discussed. To understand the cases, three notions will be explained first. These are limitations to the reach of the U.S. law that the U.S. authorities have to take into account when requiring personal data. First of all, the U.S. court must have “personal jurisdiction” over the recipient of an order. Then, whether or not a company has “possession, custody or control” over the requested data may exempt it from complying with the request. Finally, a balancing test for compelling disclosure must be applied in certain cases.

4.1. Limitation to the Reach of the U.S. Law

4.1.1. U.S. Jurisdiction

Only entities falling under the U.S. personal jurisdiction can be served with a disclosure order. This is a limitation to the reach of the Patriot Act. The question is whether a “person”, a corporation or other entities can be sued in the U.S. Assertions of jurisdiction over a person by a court of the U.S. must comport with due process.²⁶⁹

4.1.1.1. Personal Jurisdiction Based on Citizenship, Consent and Waiver²⁷⁰

Firstly, a defendant is subject to the personal jurisdiction of its home state. For individuals, home state can be defined as the place of residence, citizenship or domicile.²⁷¹ For corporations, home state means the state of incorporation or the state where the corporation carries its principal operations. Secondly, a non-resident may consent to the court's personal jurisdiction in the state of its choice. Expressly given, the consent will cure any jurisdiction defects that might otherwise prevent the case from being decided. An example of jurisdiction based on consent is the case where foreign companies give their consent to state authorities in order to be allowed to conduct a business in the forum. Thirdly, it may happen that a non-resident defendant waives to object to the a state's personal jurisdiction defect.

4.1.1.2. *Pennoyer v. Neff*²⁷²

In seminal case of *Pennoyer v. Neff*, the U.S. Supreme Court decided that U.S. court can obtain jurisdiction over a person who is present in the state where the court sits.²⁷³ The Court held that the defendant “must be brought within its jurisdiction by service of process within the State, or his voluntary appearance”.²⁷⁴ The term “presence” was construed as the physical presence of the person within the border of the state. In this perspective, it may be that a employee of an E.U. cloud

269 Anon., “An Overview of the Law of Personal (Adjudicatory) Jurisdiction: the United States Perspective”, *Kentlaw.edu*. Available at: http://www.kentlaw.edu/cyberlaw/docs/views/usview.html#N_4_ [accessed March 2012].

270 Anon., “Personal Jurisdiction”, *Lexisnexis.com*. <http://www.lexisnexis.com/lawschool/study/outlines/html/civpro/civpro02.htm> [accessed on April 2012].

271 28 U.S.C. §§ 1783-84.

272 *Pennoyer v. Neff*, 95 U.S. 714 (1877).

273 G. B. Delta & J. H. Matsuura, *Law of the Internet*, 2001, Volume 1, p. 3-3.

274 *Pennoyer v. Neff*, 95 U.S. 733 (1877).

computing provider present on the U.S. territory would be under the U.S. jurisdiction and could, therefore, be compelled to disclose personal data contained in the cloud. For example, an employee of a foreign company was subpoenaed while present in the United States.²⁷⁵

4.1.1.3. Minimum Contact and Systematic and Continuous Contact

This narrow construction of “presence” was later expanded because more exchanges and travels were made possible by way of technology.²⁷⁶ In *International Shoe Co. v. Washington*, the U.S. Supreme Court held the term “presence” even includes “contact” by a out-of-state person.²⁷⁷ The US Supreme Court states that the jurisdiction comports with due process if the defendant has “certain minimum contacts with [the forum] such that maintenance of the suit does not offend traditional notions of fair play and substantial justice”.²⁷⁸ In fact, this case and its progeny established a three-part test. This test is applied with slight differences within the Federal Circuit. Here is how the Ninth Circuit applies the test²⁷⁹: (1) “The nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections[;] (2) [t]he claim must be one which arises out of or results from the defendant's forum-related activities[; and] (3) [e]xercise of jurisdiction must be reasonable”.²⁸⁰ For example, in *Starlight Int'l LTD v. Lifeguard Health LLC* court found jurisdiction found based on only 0.24% of sales to Californian on-line customers, which amounted to \$ 2559 total.²⁸¹ This case demonstrates that the minimum contact threshold is rather low.

Besides, in *International Shoe*, the Supreme Court made the distinction between contacts that are related to the controversy and contacts that are unrelated.²⁸² Regarding the contacts related to controversy, three degrees of contracts can be distinguished.²⁸³ The single or isolated activities having “substantial connection” with the forum state which could support personal jurisdiction.²⁸⁴ Secondly, where some defendant's contacts are sufficiently related to the controversy in a particular forum, this forum can exert jurisdiction.²⁸⁵ In *World-Wide Volkswagen v. Woodson*, the Court decided that the defendant's contact was insufficient with the state where the case had to be decided. The Court added that “critical to due process analysis is that the defendant’s conduct and connection with the forum State as such that he should reasonably anticipate being haled into court there”.²⁸⁶ Finally, when the contacts between a non-resident defendant and the forum are unrelated to the controversy, a Court cannot exert jurisdiction. However, a Court can obtain jurisdiction over a defendant on condition that it has “systematic and continuous”²⁸⁷ contact with the forum state. So, when a claim is unrelated to the in-state activities a greater contact is required between the state and the defendant.

275 See: *United States v. Field*, 532 F.2d 404 (5th Cir.).

276 G. B. Delta & J. H. Matsuura, o.c., p. 3.

277 *International Shoe Co. v. Washington*, 326 U.S. 310 (1945)

278 *Ibid.*

279 Ninth Circuit is quoted because it gives a very good glimpse of how other Circuits apply the test.

280 *Ballard V. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995).

281 *Starlight Int'l, Ltd. v. Lifeguard Health, LLC*, C 08-1894, 2008 WL 2899903 (N.D. Cal. July 22, 2008)

282 L. Brilmayer, *Fundamentals of American law*, New York, Alan B. Morrison Ed., 1998, p. 181.

283 Anon., “Personal Jurisdiction”, o.c.

284 See: *McGee v. International Life Ins. Co.*, 355 U.S. 223 (1957).

285 *Burger King Corp. v. Rudzewicz*, 471 U.S. 462. (1985).

286 *World-Wide Volkswagen v. Wnoodson*, 444 U.S. 286, 297, 100, S. Ct. 559, 567 (1980).

287 *Perkins v. Benguet Consolidated Mining Co.*, 342 U.S. 437 (1952).

4.1.1.4. State Long-Arm Statute

Long-Arm Statute allows a state to obtain jurisdiction over a defendant that could not otherwise be served. There are three types of long-arm statute²⁸⁸: those that confer jurisdiction to the full extent allowed by right to due process of the 14th Amendment (1), those listing specific cases where a state can exercise jurisdiction (2), hybrid system combining both previous types (3).

4.1.1.5. Balancing test

Even when the U.S. can assert jurisdiction, the exercise of such jurisdiction has to be reasonable.²⁸⁹ In order to determine whether or not the exercise of jurisdiction is reasonable, the U.S. courts are required to operate a balance of interest. These factors have notably to be taken into account: “the link of the activity to the territory of the regulating state [...], the connections, such as nationality, residence, or economic activity, between the regulating state and the person” to be regulated [...], the existence of justified expectations that might be protected or hurt by the regulation [...], the extent to which the regulation is consistent with the traditions of the international system”.²⁹⁰ This approach, contained in the *Restatement (Third) of the Foreign Relation Law of the United States* (1987),²⁹¹ is broadly respected by U.S. federal and state court.²⁹²

4.1.2. Possession, Custody or Control

Only organizations that have “possession, custody or control” over the requested documents have to comply with a U.S. disclosure order.²⁹³ Control is construed as “the legal right, authority, or practical ability to obtain the materials sought upon demand”.²⁹⁴

In principle, determining whether or not a company has “control” over the requested information must be made on a case-by-case basis.²⁹⁵ Any scenario is possible: a parent company might have control over the document held by its subsidiary and vice-versa. Similarly, Courts have found that a sister corporation might have control over document held by another sister corporation.²⁹⁶ However, the “documents and records that a corporation requires in the normal course of its business are presumed to be in its control unless the corporation proves otherwise”.²⁹⁷

These rules have implications on the disclosure of document held outside the U.S. A corporation subject to U.S. jurisdiction has to disclose not only the information held in the U.S. but also information in its control held outside the U.S. whether by a parent, a subsidiary or a sister

288 Anon., “Personal Jurisdiction”, *o.c.*

289 Restatement (Third) of Foreign Relations Law (1987), § 403 (1).

290 Restatement (Third) of Foreign Relations Law (1987), § 403 (2), *o.c.*

291 Restatement (Third) of the Foreign Relation Law of the United States (1987). Available at: <http://www.maclester.edu/courses/intl114/docs/restatement.pdf> [accessed February 2012].

292 M. Geist & M. Homsy, “The Long Arm of the USA Patriot Act...”, *o.c.*, p. 16.

293 T. Waage & N. Petri, “Government Access to Information in ”the Cloud””, *o.c.*, p. 8; A. Lakatos, “United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud”, *o.c.*, p. 5.

294 *Sec. & Exch. Comm’n. v. Credit Bancorp, Ltd.*, 194 F.R.D. 469, 471 (S.D.N.Y. 2000).

295 A. M. Berman & L.R. Chorlak, “So Simple to State, so Hard to Apply Interpreting 'Possession, Custody and Control' in Today's Complex Corporate World”, *New York Law Journal*, May 16, 2011. Available at: <http://www.velaw.com/uploadedFiles/VEsite/Resources/VinsonElkinsNewYorkLawJournalLitigationArticle.pdf> [accessed March 2012].

296 *Credit Bancorp*, 194 F.R.D. At 472.

297 *Cooper Indus. v. British Aerospace Inc.*, 102 F.R.D. 918, 919 (S.D.N.Y. 1984).

corporation. For example, the U.S. could require Google U.S., a parent company, to ask Google UK, its subsidiary, to disclose personal data pertaining to its E.U. customers. If Google U.S. have control over the E.U. citizens' personal data contained in the server in UK, it would be obliged to comply with the disclosure order. Conversely, let's assume that an U.S. subsidiary of an E.U. parent company has control over personal data held by the E.U. parent company in E.U. These personal data would thereby be accessible to the U.S. authorities.

4.1.3. Information Located Abroad

The section 442 of the Restatement states that a court of an agency in the U.S. may order an entity subject to its jurisdiction to produce data or object necessary for an investigation even if “the information or the person in possession of the information is outside the United States”.²⁹⁸ In that case, court must notably consider these factors: the importance of the record to the investigation, the availability of alternative means, and the extent to which noncompliance with the request would undermine important interest of the United States, or the extent to which compliance with the request would undermine important interests of the state where the information is located.²⁹⁹ If the foreign law prohibits the disclosure of requested data, sanction should not be ordinarily imposed. However, the targeted person should “make good faith effort to secure permission from the foreign authorities to make the information available” (Section 442 (2) (a)).

It appears that, although such a balancing test exists, U.S. courts have been willing to enforce disclosure of data held abroad.³⁰⁰ Indeed, when it comes to the USA PATRIOT Act and terrorism cases, the U.S. would rather give significant weight to their own interests.

4.2. What Are the Implications for E.U. Citizens' Personal Data?

E.U. citizens' personal data are at risk whether held by a U.S. cloud service provider or by a E.U. one. U.S. authorities may obtain personal data from any cloud service provider under two conditions: having the possession, custody or control over the data and falling under the U.S. jurisdiction. Six cases will be analysed. They summarized in table IV.

No	Cloud Provider Location	Subsidiary Location	Data Center Location
1	E.U.	U.S. or no subsidiary	U.S.
1	U.S.	E.U. or no subsidiary	U.S.
2	U.S.	none	E.U.
3	E.U.	U.S.	E.U.
4	U.S.	E.U.	E.U.
5	E.U.	No subsidiary but minimum contact	E.U.

298 Restatement (Third) of Foreign Relations Law (1987), § 442 (1) (a).

299 Restatement (Third) of Foreign Relations Law (1987), § 442 (1) (c), *o.c.*

300 Information & Privacy Commissioner Report for British Columbia, “Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing”, 2004, p. 12. Available at:

<http://web.docuticker.com/go/docubase/5431> [accessed May 2012].

6	E.U.	E.U. or no subsidiary	E.U.
---	------	-----------------------	------

Table IV: Six cases

The first case regards E.U. or a U.S. cloud computing providers that store E.U. personal data in a data center located on the U.S. territory. As the data center falls under the U.S. jurisdiction, personal data it contains can be accessed by the U.S. authorities.^{301 302} The DPD would apply to a E.U. cloud computing provider pursuant to article 4(1)(a) and to a U.S. cloud computing provider without establishment in the E.U. pursuant to article 4(1)(c).

The second case regards the situation where an E.U. cloud computing user outsources the processing of its personal data to a U.S.-based cloud computing provider. For the purpose of this example, let's assume that the data are located in a data center located in the E.U. Since the cloud computing provider falls under the U.S. jurisdiction and has the possession, custody or control over the data, the U.S. authorities are entitled to issue an order on the cloud provider to access these E.U. citizens' personal data.

The third case regards the situations where an E.U. cloud computing user outsources the processing of its personal data to a E.U.-based cloud computing provider which is a parent to a U.S. subsidiary. For example, it could be the case of an E.U. hotel company outsourcing the processing of its customers' data to ProfitBricks, a parent cloud computing company based in Germany, which has a subsidiary in the U.S.³⁰³ Besides, for the purpose of this scenario, let's assume that the data are stored in a data center located on the E.U. territory. In this scenario, the U.S. authorities could issue a disclosure order on the U.S. subsidiary of the E.U. cloud computing provider to produce data if the data are in the possession, custody or control of American citizens.³⁰⁴ It would mean that the U.S. subsidiary of Profitbricks could be compelled to disclose E.U. citizens personal data located in the E.U. to the U.S. authorities.

The fourth case regards the situations where an E.U. cloud computing user outsources the processing of its personal data to an E.U.-based cloud computing provider which is a subsidiary to a U.S. parent company.³⁰⁵ For example, this would be the case of an E.U. hotel company that outsources the processing of its customers' data to Google UK, subsidiary of Google U.S. (the parent company).³⁰⁶ For the purpose of this scenario, let us assume that the data are stored in a data center located on the E.U. territory. In this scenario, the U.S. authorities could issue a disclosure order on the U.S. parent of the E.U. cloud computing provider to produce data since the data are in the possession, custody or control of American citizens.³⁰⁷ It would mean that Google U.S. could be compelled to disclose E.U. citizens personal data located in the EU to the U.S. authorities. However, the E.U. cloud computing provider should respect the DPD pursuant article 4 (1) (a). This scenario is the most probable situation. Three U.S. based cloud computing providers have already admitted that data stored on its servers are subject to the USA PATRIOT Act. First, in March 2011, Ojima Hideki, managing director at Amazon Data Services Japan KK, declared that "because Amazon is a U.S. company, the data centre of Amazon Web Services in Tokyo will fall within the scope of the USA Patriot Act".³⁰⁸ During the launch of Microsoft office 365, Gordon Frazer for

301 D. T. S. Fraser, "The Cloud Thing: Privacy and Cloud Computing", (Mc Innes Cooper law firm), July 2011, p. 27.

Available at http://www.unb.ca/its/_resources/pdf/about-its/privacy-cloud-davidfraser.pdf [accessed May 2012].

302 The situation remains unchanged whether the data center belongs to the cloud computing providers or not.

303 Let's assume for the purpose of this example that "ProfitBricks" has a subsidiary in the U.S.

304 T. Waage & N. Petri, *o.c.*, p. 12.

305 D. T. S. Fraser, "The Cloud Thing: Privacy and Cloud Computing", *o.c.*, p. 27.

306 Let's assume for the purpose of this example that Google UK is a subsidiary of Google U.S.

307 T. Waage & N. Petri, *o.c.*, p. 11.

308 C. Carnabuci, "The Long Arm of the USA Patriot Act: Tips for Australian Businesses Selecting Data Service

Microsoft UK admitted that data stored in Microsoft servers are subject to the USA PATRIOT Act irrespective of where the servers are located as Microsoft is a U.S.-headquartered company.³⁰⁹ Thirdly, Google's spokesperson declared that “as a law abiding company, we comply with valid legal process, and that – as for any U.S.-based company – means the data stored outside of the U.S. may be subject to lawful access by the U.S. government”.³¹⁰

Fifth, even if an E.U.-based cloud computing provider has no office on the U.S. territory, it may fall under its jurisdiction. It is the case when there is a minimum contact between the E.U.-based cloud computing provider and the U.S. For example, this could be the case if it markets its products or services in the U.S.³¹¹ As for the previous case, the Data Protection Directive applies pursuant article 4 (1) (a).

The sixth case regards a situation where an E.U. cloud customer contracts with an E.U. cloud computing provider storing data on the territory of the E.U. Because this cloud computing provider has no office in the United States and conducts little enough U.S. business, it does not fall under the U.S. jurisdiction.³¹² However, it might be obliged to disclose personal of its customers pursuant to a MLAT.

Besides, it is worth noting that the cloud computing customers themselves may be served with a FISA order, a NSL or a grand jury subpoena. The customers that have minimum contact with the U.S. territory fall under the U.S. jurisdiction as well. This would be the case of an E.U.-based company that has a US subsidiary or that is a subsidiary of a U.S. parent company. Also, an E.U.-based company could fall under the U.S. jurisdiction if it conducts systematic or continuous business in the US.³¹³ As a consequence, they may be required to disclose information to U.S. law enforcement authorities regardless the situation of their cloud service provider.³¹⁴ In order to avoid to be compelled by the US to disclose data, EU customers and their cloud service provider must have no presence in the United States.³¹⁵

4.3. Conclusion

The five first cases demonstrate that the U.S. jurisdiction is extremely broad so that they can potentially access personal data in a variety of situations. The fourth scenario is the most likely to occur as the biggest cloud computing providers are headquartered in the U.S. The sixth case shows that even if the U.S. authorities cannot assert jurisdiction, they may access request these personal data through the auspices of a MLAT concluded between an E.U. Member-state and the U.S.

It is clear that cloud computing has a particular effect on the reach of the USA PATRIOT Act. Millions of customers transfer personal data about themselves to a few cloud computing providers so that they create a giant data base easily accessible for law enforcement authorities.

Providers”, *o.c.*, p. 3. See also: H. Tropman, “Cloud Technology: When Locating Isn't Everything”, *Australasian Legal Business*, Issue 10.3, April 2012, pp. 42-43. Available at: <http://issuu.com/albaustralia/docs/ozlb10.3> [accessed June 2012].

309 *Ibid.*

310 *Ibid.*

311 T. Waage & N. Petri, *o.c.*, p. 8; A. C. Lakatos, *o.c.*, p. 5.

312 Alex C Lakatos, “The Patriot Act and the Cloud: Part 2”, *Mayerbrown.com*, January 2012, p. 3. Available at: <http://www.mayerbrown.com/news/article.asp?id=12176&nid=20> [accessed March 2012].

313 A. C. Lakatos, *o.c.*, p. 5.

314 *Ibid.*

315 *Ibid.*

Storing personal in the cloud offers several advantages to companies and natural person. However, many did not think about adverse consequences this may have. Since leaders in cloud computing services are mostly U.S., it means that most of the data contained in the cloud fall under the U.S. jurisdiction. While before, personal data pertaining to E.U. corporations or to E.U. citizens were unlikely to fall under the U.S. jurisdiction because they were stored in-house, cloud computing technology changes this old pattern. Nowadays, cloud computing customers are somehow dispossessed of their control over their personal data.

Chapter 5. Recommendations

To answer this problem and reduce U.S. access to E.U. personal data, several recommendations can be put forward. An attempt will be made to discuss these recommendations from Lawrence Lessig's angle.

According to Lawrence Lessig, the world is governed by four sorts of constraints³¹⁶: the law, the social norms, the market and the nature or architecture. Sanctions imposed ex-post are the way by which law regulates. Regarding law as a constraint, three different ways will be explored: blocking statutes, ban on outsourcing (sensitive) personal data to cloud computing providers falling under the U.S. jurisdiction and cooperation between the E.U. and the U.S. Social norms dictate how individuals have to behave. Protection of privacy as a general social norm gives rise to two specific rules that could be followed by cloud computing providers. First, cloud computing provider should challenge systematically the gag order. Secondly, they should provide the U.S. authorities with a proportionate answer to disclosure orders. The market regulates by price. As understood by Lessig, the market can do little protect the privacy of E.U. cloud users. However, the cloud market could adopt a strategy to prevent the U.S. from accessing E.U. personal data. Finally, the nature or architecture regulates through the “world as I find it”.³¹⁷ In this sense, encryption and keeping the data in-house could reduce the impact on privacy of the U.S.

These four sorts of constraints can be exploited to understand how EU citizens' personal data could stay out of reach of the U.S. Besides, some practical solutions that customers may implement will be analysed.

5.1. Law as a Constraint

Law can regulate directly or indirectly.³¹⁸ It regulates directly when it imposes a punishment ex-post and it regulates indirectly when it shapes the other modalities of constraints. The first recommendation regards the enactment of a blocking statute. It is an example of direct regulation by the law. The second recommendation is to forbid outsourcing of personal data to cloud computing providers falling under the U.S. jurisdiction. The last recommendation is to enhance cooperation regarding the exchange of personal data between the U.S. and the E.U. The last two recommendations are examples of indirect regulation.

5.1.1. Blocking Statutes

A blocking statute is a law enacted in one jurisdiction enabling “a petitioner to mount a foreign compulsion defence to a U.S. court action”.³¹⁹ In concreto, a blocking statute would prevent an entity subject to the jurisdiction of the one E.U. Member-state from complying with a specific U.S. law. Should the targeted entity comply with the foreign order, it would then get a penalty.

316 L. Lessig, “The Law of Cyberspace”, Essay presented at the Taiwan Net '98 conference, Taipei, March, 1998, p. 2. Available at: http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf [accessed May 2012].

317 *Ibid*, p. 3.

318 *Ibid*, p. 11.

319 M. Geist & M. Homs, “Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World”, *o.c.*, p. 26. See also: Memorandum, House of Commons Subcommittee on the Treasury, “How secure is the personal information of UK citizens in light of the USA PATRIOT Act and the limited privacy protections of the United States?”, (February 28, 2008), p. 11.

However, compliance might not lead to any penalty when explicitly authorised by the domestic government.

According to U.S. case law three conditions must be met for a blocking statute to successfully prevent disclosure of E.U. personal data in a U.S. court. These factors were developed by the Supreme Court in *Société Nationale Industrielle Aerospatiale v. United States Dist.*³²⁰ Firstly, the blocking statute must be specific and exclusive. It means that the targeted entity cannot comply with both the E.U. law and the U.S. law. Secondly, a real sanction must be attached to the blocking statute meaning that the steady enforcement of the law must appear to be serious for the U.S. courts. Thirdly, the defendant has to try to comply with U.S. law in good faith.

Thus, a blocking statute is not an absolute defence to prevent the disclosure of E.U. personal data. A blocking statute only constitutes one factor that U.S. courts take into account to make a decision as to whether to order the disclosure of data. According to the U.S. Supreme Court the blocking statute is “relevant to the court's particularized comity analysis only to the extent that its terms and its enforcement identify the nature of the sovereign interests in non-disclosure of specific kinds of material”.³²¹ It means concretely that the blocking statute has to be based on essential E.U. privacy law objectives.

Cases where a blocking statute did not prevent the disclosure of data are numerous.³²² For example in *Accessdata Corp v. Alste Tech. Gmbh*,³²³ a civil law case, Accessdata sought the production of information concerning customer complaints. Alste objected, arguing that disclosure of information would violate the German law. The Supreme Court held that Alste failed to demonstrate such a blocking statute. Besides, the Supreme Court stated that even if the German Data Protection Act prohibited such disclosure “it is well settled that such [blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the Act of production may violate that statute”. Also, in *Société Nationale Industrielle Aerospatiale v. U.S. Dist.*, the court held that France had not enforced the blocking statute for years. Partly for that reason, the French blocking statute did not prevent the disclosure of the requested data.

Examples of blocking statute can be found in Switzerland or in British Columbia. Switzerland, for example, has a very strong blocking statute in its banking secrecy law. Similarly, British Columbia imposes huge fine up to \$500.000 on corporation for unauthorized disclosure.

The version 56³²⁴ of the Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) contained such a blocking statute. Article 42 stated that “no judgement of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any

320 *Société Nationale Industrielle Aerospatiale v. United States Dist.*, 482 U.S. 522 (1987).

321 *Ibid.*, at 544.

322 S. Rothman & C. Cohen, “The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes”, *hugheshubbard.com*, January 2011, p. 14. Available at: <http://www.hugheshubbard.com/files/FileControl/c71f7d89-f6fc-4194-bae4-82e24dc8184d/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Data%20Protection%20in%20the%20EU%20and%20Its%20Impact%20on%20US%20Discovery.pdf> [accessed September 2012].

323 See: *AccessData Corp. v. Alste Tech. Gmbh*, 2010 WL 318477 (D. Utah Jan. 21, 2010). Available at: <http://www.elawexchange.com/cases/AccessDataAlste.pdf> [accessed August 2012]; *Societe Nat. Ind. Aero. v. U.S. Dist. Court*, 482 U.S. 522 (1987).

324 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), version 56, November 29, 2011.

manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State”. Article 79 (4) (j) of the version 56 of the proposal imposed huge fines (up to 5% of the annual worldwide turnover) to dissuade corporation from disclosing E.U. personal data. Unfortunately, provision of article 42 was abandoned in the proposal of January 25, 2012³²⁵. This can be deplored. This blocking statute could have been a effective tool to prevent unauthorized disclosure of E.U. personal data to the U.S. The reason why this part of the proposal was amended is unclear. It could be because of pressure coming from the U.S. or the will of the E.U. to deal carefully with corporations under its jurisdiction.

5.1.2. Ban on Outsourcing (Sensitive) Personal Data to Cloud Computing Providers Falling Under the U.S. Jurisdiction

A ban on outsourcing sensitive data to cloud computing providers falling under the U.S. jurisdiction might seem to be a good answer to the issue at stake. A similar rule was proposed by the British Columbian Government and Service Employees' Union in Canada.³²⁶ Such an interdiction would prevent U.S. authorities from requiring access to data considered as the core of privacy.

However, this option is not the panacea. First, it would not only affect U.S. companies and their subsidiaries located in the E.U. but also E.U. cloud providers subject to U.S. jurisdiction. On the one hand, the European Union understands the difficult position in which the U.S. companies are and on the other hand it is not in the interest of the European Union to affect negatively E.U. cloud providers' business. Second, applying this rule would turn out to be tedious. How to split non sensitive personal data and sensitive personal data in two different clouds pertaining possibly to two different cloud providers? Third, E.U. cloud providers that do not fall under the U.S. jurisdiction are rare since the U.S. law has a long arm reach.

5.1.3. Cooperation between the E.U. and the U.S.

Instead of fighting against the U.S., the European Union could achieve better result by way of cooperation. Mutual legal assistance treaties are not suited to the cloud computing context. As Professor Ian Walden wrote: “MLA procedures have historically been notoriously complex, slow and bureaucratic”.³²⁷

Therefore, improvements are required. In this sense, Ian Walden is proposing two guidelines. On the one hand, national law enforcement agencies (hereinafter LEAs) should be encouraged “to spontaneously (i.e. proactively) disclose information to foreign LEAs where it appears relevant to conduct seemingly connected to the foreign territory, rather than waiting for the

325 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), January 25, 2012. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [accessed July 2012].

326 M. Geist & M. Homsy, “Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World”, *o.c.*, p. 26.

327 I. Walden, “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent”, Queen Mary University, Research Paper No. 74/2011, p. 11. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067[accessed June 2012].

foreign LEA to commence an investigation and initiate a formal MLA request”.³²⁸ On the other hand, co-operation could be improved by “legitimising certain extra-territorial conduct by LEAs”.³²⁹

Also, in this perspective, the E.U. and the U.S. are negotiating a comprehensive EU-U.S. data privacy and protection agreement that would provide a “high level of privacy protection for all individuals and thereby facilitates the exchange of data needed to fight crime and terrorism. [...] Such an agreement will allow for even closer transatlantic cooperation in the fight against crime and terrorism, through the mutual recognition of a high level of protection afforded equally to citizens of both the United States and the European Union, and will thus facilitate any subsequent agreements concerning the sharing of a specific set of personal data”.³³⁰

The following principles are being or will be negotiated: data security, transparency of data processing or use, accountability, maintaining the quality and integrity of information, the existence of effective authorities ensuring data protection oversight, purpose limitation, retention of personal data, and effective administrative and judicial redress.³³¹

5.2. Social Norms As a Constraint

In the context at stake, social norms might be considered as an inappropriate constraint. However, privacy and data protection are moral values that could be “used” as a social norm. Philosophers have been writing about it for a long time. Therefore, it can't be denied that the respect of privacy and data protection is recognized in our society as a social norm. For example, searching into the hard-drive or the e-mail box of someone else's computer is not an acceptable behaviour in our society. This behaviour is sanctioned in different ways by the society: loss of reputation, distrust toward the actors which make the disclosure possible, the exclusion of the group, etc.

While this social norm can hardly influence the behaviour of the U.S. towards cloud computing providers, these providers have an interest in respecting private live of their customers. Two different ways will be discussed.

5.2.1. Challenging the Gag Order

Cloud computing providers are in a position to challenge the gag order that may attend a Disclosure order. If successfully challenged, cloud computing providers are allowed to inform their customers that information about them has been sought by the U.S. government. As a consequence, the process would gain in transparency. Besides, cloud computing users would be in position to challenge the disclosure order itself. When successfully challenged, the Disclosure order can be reduced or cancelled.

An interesting case regarding the challenging of a gag order came up recently. *Twitter*, a cloud computing provider, received a subpoena pursuant article 2703 of the ECPA ordering the disclosure of personal data of five of its subscribers,³³² members of *Wikileaks*, and hundreds of

328 I. Walden, “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent”, *o.c.*, p. 12.

329 *Ibid.*

330 E. Holder & V. Reding, “Joint Statement on the Negotiation of a EU-U.S. Data Privacy and Protection Agreement by Attorney General Eric Holder and European Commission Vice-President Viviane Reding”, *Justice.gov*, June 2012. Available at: <http://www.justice.gov/opa/pr/2012/June/12-ag-783.html> [accessed June 2012].

331 *Ibid.*

332 Jacob Appelbaum is a U.S. computer programmer; Rop Gonggrijp is a Dutch hacker; Julian Assange is the

thousands of their followers.^{333 334 335} Information about *Wikileaks* members was requested following the publication of leaked U.S. classified documents on the Internet as they were “relevant and material to an ongoing criminal investigation”.³³⁶ The scope of personal data requested encompasses “mailing addresses and billing information known for the user, all connection records and session times, all IP addresses used to access Twitter, all known email accounts, as well as the “means and source of payment,” including banking records and credit cards”.³³⁷

Twitter could have handed over the requested information without notifying its subscribers. However, the famous micro-blogging website has a privacy policy that it is willing to enforce. The *Twitter's* privacy policy guarantees its subscribers that they would be notified if Twitter had to process their information in such a way.³³⁸ Therefore, *Twitter* challenged the “gag order” which was eventually lifted. As a result, *Twitter* was allowed to notify its subscribers that the U.S. law enforcement had sought information about them. Hence, notified subscribers were in position to oppose the disclosure of their personal data to the U.S. law enforcement.

Similar disclosure orders are likely to be issued on other social networking websites.³³⁹ Assange’s lawyer Mark Stephens³⁴⁰ went even further declaring that “similar information was sought from Google Inc., Facebook Inc. and EBay Inc.’s Skype unit”.³⁴¹ Anyway, “if other companies did receive and quietly comply with these orders, it will be a long time before we know, if we ever do, given the prohibition in these orders on disclosing even its existence to anyone”.³⁴² Some commentators noted that *Twitter's* reaction to the subpoenas should become an industry standard.³⁴³

If challenging the gag order become an industry standard observed by cloud computing providers, privacy invasion of cloud computing users would be greatly reduced.³⁴⁴

5.2.2. A Proportionate Answer to Disclosure Order

spokesman of Wikileaks; Bradley Manning was United States Army soldier; Birgitta Jónsdóttir is a member of the Icelandic Parliament. All of them are Wikileaks activists.

333 G. Greenwald, “DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers”, *Salon.com*, January 8, 2011. Available at: http://www.salon.com/2011/01/08/twitter_2/ [accessed July 2007].

334 This case shows that a single order may in fact be used to access personal of a lot of people.

335 See in appendix II a copy of the order.

336 18 U.S.C. § 2703 (d).

337 G. Greenwald, “DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers”, *o.c.*

338 "To help users protect their rights, it's our policy to notify users about law enforcement and governmental requests for their information, unless we are prevented by law from doing so." declared a *Twitter* representative to *Cnet*. See: D. McCullagh, “DOJ Sends Order to Twitter for WikiLeaks-related Account Info”, *Cnet.com*, January 7, 2011. Available at: http://news.cnet.com/8301-31921_3-20027893-281.html [accessed July 2011].

339 G. Greenwald, “DOJ subpoenas Twitter records of several WikiLeaks volunteers. *o.c.*

340 M. Stephen is specialized “in International, Appellate and Complex litigation, Constitutional, Human Rights, IP, Media & Regulatory work, defamation, privacy, media, art and cultural property, data protection and freedom of information and intellectual property, Mark Stephens has undertaken some of the highest profile cases in the country and abroad”. See: <http://www.fsilaw.com/our-people/profile/88-mark-stephens-cbe/> [accessed July 2012].

341 E. Larson, “U.S. Twitter Subpoena Is Harassment, Lawyer Says”, *Bloomberg.com*, January 10, 2011. Available at: <http://www.bloomberg.com/news/2011-01-10/u-s-twitter-subpoena-on-wikileaks-is-harassment-lawyer-says.html> [accessed July 2012].

342 G. Greenwald, “DOJ subpoenas Twitter records of several WikiLeaks volunteers”, *o.c.*

343 R. Singel, “Twitter’s Response to WikiLeaks Subpoena Should Be the Industry Standard”, *Wired.com*, October 1, 2010. Available at: <http://www.threatlevel/2011/01/twitter/> [accessed July 2012].

344 R. Singel, “Twitter’s Response to Wikileaks Subpoena Should Be the Industry Standard”, *o.c.*

As seen previously, the handling of requests for personal data can occur in different manners. Some cloud computing providers tend to deliver data in bulk in order to avoid having to search for the particular requested file. Other cloud computing providers might be more conscientious. These would precisely disclose the requested file(s) to the U.S. authorities. As a result, privacy of their customers would be less violated.

Making public how cloud computing providers handle disclosure orders would allow customers to make an informed choice. Careless providers would be “sanctioned”, losing customers to the profit of more careful providers. This won't result in a reduction of the amount of US requests. However, it might be expected that the requests will be better handled by the cloud providers.

Putting this recommendation into practice would not be easy. An independent certification authority could control how cloud computing providers handle U.S. requests. Controls would take place on a voluntary basis. At the end of the control, privacy-friendly providers would receive a certificate. This certificate would indicate that the provider is privacy-friendly.

5.3. Market

The market regulates by the price. “Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates”.³⁴⁵ In the sense of Lessig, it is unlikely that the market could limit U.S. access to E.U. personal data. At a certain time, it was thought that the cloud market, in its common meaning, could take action to protect efficiently the privacy of their users.

It was a common belief to think that cloud computing providers could develop a business strategy that would leave them out of reach of the U.S.³⁴⁶ A 100 % EU cloud computing provider, based in the E.U. territory that has no subsidiary in the U.S. and no minimum contact with the U.S. would fall outside the scope of the U.S. jurisdiction. This business strategy would play as a selling point. E.U. customers worried about the USA PATRIOT Act and any other laws that the U.S. could use to access their personal data would be ready to pay a higher price to cloud computing providers adopting such a strategy.³⁴⁷

However, it turned out that this business model was deceptive. The U.S. authorities would still be allowed to access personal data pursuant to a MLAT. Also, this business model neglects an important aspect of the cloud computing, viz. the free flow of data in the cloud. Finally, it is worth noting that E.U. Member-state can access personal data in the cloud pursuant to their own laws.

5.4. Architecture

The nature or the architecture regulates through the “world as I find it”.³⁴⁸ Lessig names

345 L. Lessig, *o.c.*, p. 3.

346 S. Overby, “The patriot Act and your data: should you ask cloud computing provider protection?”, *Cio.com*, January 20, 2012. Available at:

http://www.cio.com/article/698432/The_Patriot_Act_and_Your_Data_Should_You_Ask_Cloud_Providers_About_Protection [accessed May 2012].

347 However, personal data may still be exchanged following data exchange cooperation schemes.

348 L. Lessig, *o.c.*, p. 3.

this the “code”, i.e. the software and hardware.³⁴⁹ In this perspective, encryption software could be used to bar U.S. law enforcement access to personal data. Secondly, keeping data in-house could also help cloud users to gain more control on their data.

5.4.1. Encryption

“[E]ncryption technologies are the most important technological breakthrough in the last one thousand years”.³⁵⁰ Simply put, encryption is “the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood”.³⁵¹

The Convention on Cybercrime of November 23, 2001 adopted by the Council of Europe and signed by the U.S. does not outlaw encryption. However, the Convention allows its Member-states to create a decryption order. Heretofore, the U.S. has not enacted any statutory law which would grant the U.S. authorities the power to compel cloud computing providers to decrypt personal data. Therefore, the issue is left to the judiciary power.³⁵²

Might encryption technologies, also called cryptography, be a way to bar U.S. governmental access to E.U. personal data in the cloud? To answer this question, it is necessary to make a distinction between data encrypted by the cloud computing provider and data encrypted by the cloud user.

Data encrypted by the cloud computing provider remain accessible to the U.S. authorities. Indeed, the U.S. court could force the cloud computing provider to decrypt the data as it possesses the encryption key.³⁵³

Data encrypted by the E.U. cloud users are more secure. Let's take the example of an E.U. citizen storing its encrypted personal data on *Dropbox*. In this case, the U.S. authorities would have no means to compel him to hand over the encryption key. Careful cloud users will make sure to encrypt their personal data before uploading them in the cloud. Also, it is recommended to not store the encryption key in the cloud.

However, the U.S. authorities could possibly rely on a MLAT to obtain the encryption key. For example, Great Britain enacted the Regulation of Investigatory Powers Act (RIPA) which allows certain governmental actors to compel decryption of encrypted data. Its section 53 criminalizes failure to comply with a disclosure order. Thus, in the case of a cooperation with Great Britain, the U.S. might get access data in plain text.

Therefore, encryption technology makes the work of law enforcement more difficult, but not impossible.

349 L. Lessig, *o.c.*, p. 4.

350 L. Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999, p. 33.

351 R. Bauchle, F. Hazen, J. Lund, G. Oakley & F. Rundatz, “Encryption”, *Searchsecurity.techtarget.com*, July 2006. Available at: <http://searchsecurity.techtarget.com/definition/encryption> [accessed June 2012].

352 B. M. Palfreyman, “Lesson from the British and American Approaches to Compelled Decryption”, *Brooklyn Law Review*, 2009, Vol. 75, Issue 1, p. 346.

353 J. Gershater, “Cloud Computing and the Patriot Act”, *Cloudbook Journal*, vol. 3, 2012, p. 19. Available at: www.cloudbook.net/resources/stories/patriot-act [accessed August 2012].

5.4.2. Keeping Data in-House

Cloud computing users concerned about their privacy could decide to store the most valuable information in-house.³⁵⁴ That way, even if the U.S. government would still be allowed to access those data, it would have to go through the cloud customer itself. Keeping data in-house has some advantages. Firstly, the cloud customer would be aware that it is the recipient of an order to disclose data. When data are kept in the cloud, the U.S. government can directly serve a disclosure order on the cloud computing provider without the cloud user knowing it. Secondly, the cloud customer would be able to control and limit the volume of data disclosed to the strict minimum. When data are stored in the cloud, it might be that the cloud provider discloses more data than what is really needed by the US government. Thus, keeping data in-house gives the cloud customer at least a bigger feeling of control over its data.

5.5. Practical Solutions From a Customer Point of View

Lakatos gives meaningful recommendations to cloud computing customers worried about their privacy in the cloud. First of all, the cloud computing customers should try to understand how the USA PATRIOT Act might be used to access their personal data.

Secondly, he recommends cloud computing customers to understand what their concerns are.³⁵⁵ Concerns are not always where they are expected to be. As Lakatos explains, numerous customers, corporations e.g., are not especially worried about the fact that the U.S. authorities could access their data. However, their clients whose personal data are contained in the cloud might be concerned by this. In this case, transparency is the solution according to Lakatos. The corporation – cloud computing customer – should clearly state what degree of risk is involved and what is done in order to mitigate them.

The last recommendation is to negotiate the contract terms covering how the cloud provider is required to respond to government requests for data.³⁵⁶ For example, they are two points that a powerful customer can discuss with its cloud provider. First, the customer can negotiate the obligation for the cloud provider to inform it that its data are requested by the U.S. government when the request does not include a gag order. Second, cloud computing provider might be imposed to disclose exclusively information strictly necessary to comply with the request.³⁵⁷ Of course, this advice is addressed to customer having a significant market power. The other customers are advised to examine different cloud computing providers' general terms and conditions regarding this matter before contracting with one of them.³⁵⁸ This way, they can choose the one that protect their privacy at the greatest level.

5.6. Conclusion

Many recommendations can be put forward. They were analysed from the Lessig's four constraints angle. Some of them require the intervention of governmental authorities. Other

354 S. Overby, *o.c.*

355 *Ibid.*

356 *Ibid.*

357 In case of breach of this provision, the cloud computing provider may be held liable to pay damages.

358 S. Overby, *o.c.*

recommendations involve directly cloud computing providers and users themselves.

The best results could be achieved by combining different recommendations. However, it can be expected that none of them could entirely prevent the U.S. from accessing E.U. citizens' personal data.

General Conclusion

Cloud computing is a new technology that is booming. Nowadays, this technology is present in the life of everyone. However, it involves risks for privacy of cloud users. One of these risks regards the USA PATRIOT Act. Once E.U. citizens' personal data are stored in the cloud, they might fall into the U.S. jurisdiction and be accessed by U.S. law enforcement authorities pursuant to the USA PATRIOT Act. This fear is exacerbated by the fact that the U.S. cloud computing providers dominate the cloud market.

This Act made easier the gathering of information for law enforcement agencies. Indeed, many existing legal tools to investigate crime and gather intelligence were bolstered by the USA PATRIOT Act. The most powerful legal instruments are certainly the FISA orders and the NSLs. Pursuant to these or other legal instruments, the U.S. authorities can request cloud computing providers to hand over personal data stored in the cloud. As this personal data may belong to E.U. citizens, E.U. data protection law deserved to be analysed.

The DPD was particularly analysed. The upshot is that the scope of applicability of the DPD is broad. Even the U.S.-based cloud computing providers may have to respect the provisions of the DPD. The valid consent of the E.U. cloud customers render the transfer of their personal data to the U.S. lawful.

The U.S. authorities can request personal data to cloud computing providers in a variety of cases as the threshold to assert jurisdiction is low. Five cases were analysed to demonstrate that fear of E.U. cloud users that the U.S. access their personal data stored in the cloud is legitimate.

There are some solutions to prevent the U.S. authorities from accessing E.U. citizens' personal data. They are addressed to E.U. policy makers, cloud providers and cloud users. However, no one of these answers is the panacea. They can minimize the risk, but can't reduce it to zero.

Further research is obviously needed on the answers to give to this problem. Indeed, this study only provides a glimpse of the different solutions. Besides, it would be interesting to study how the E.U. accesses personal data in the cloud to fight against terrorism or crime. Finally, the comparison of the approach of the U.S. and the E.U. would give some relativity to this study.

Bibliography

A. Legal and policy instruments

European Union policy and legal documents

Conventions, Agreements and Directives

Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS No. 2; 213 *UNTS* 222.

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* n 28, November 23, 1995, p. 31.

Charter of Fundamental Rights of the European Union, proclaimed in Nice, December 7, 2000, *O.J. C-* 364, December 18, 2000, p. 1.

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, July 31, 2002.

Agreement on mutual legal assistance between the European Union and the United States of America, *O.J. L* 19 July 2003, p. 41.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *O.J. L* 105, April 13, 2006, p. 54-63.

Agreement of the 23rd July 2007 between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), *O.J. L* August 4, 2007.

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *O.J. L* 195, July 27, 2010.

Miscellaneous

Working Party 29, “Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites”, May 2002. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf [accessed May 2012].

Working Party 29, “Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)”. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf [accessed July 2012].

Working Party 29, “Opinion 1/2006 on the application of the EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against, banking and financial crime”. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf [accessed July 2012].

Working Party 29, “Opinion 4/2007 on the Concept of Personal Data”, June 20, 2007. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [accessed August 2012].

Working Party 29, “Opinion 8/2010 on Applicable Law”, December 16, 2010. Available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf [accessed on April 2012].

Working Party 114, “Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995”, November 2005. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf [accessed in May 2012].

European Commission, “A comprehensive approach on personal data protection in the European Union”, COM (2010) 609 final, 4 November 2010. Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf [accessed November 2011].

Decision of the Commission of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US, 2000, *O.J. L* 215/7.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), version 56, November 29, 2011.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), January 25, 2012. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [accessed July 2012].

European Commission, “New EU-US agreement on PNR improves data protection and fights crime and terrorism”, *Europa.eu*, November 2011, Available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1368&format=HTML&aged=1&language=EN&guiLanguage=fr> [accessed September 2012].

United States legal and policy instruments

Legislation

United States Codes.

National Security Act, Pub. L. 80-253, 61 Stat. 495, approved July 26, 1947.

The Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114, approved October 26, 1970.

Foreign Intelligence Surveillance Act, Pub.L. 95-511, 92 Stat. 1783, approved October 25, 1978.

Right to Financial Privacy Act, Pub. L. 95-630, 92 Stat. 3697, approved November 10, 1978.

Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848, approved October 21, 1986.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, Pub. L. No. 107-56 [H.R. 3162], 115 Stat. 272, approved October 26, 2001.

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638, approved December 17, 2004.

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, approved March 9, 2006.

PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216, approved May 26, 2011.

Miscellaneous

Committee Notes on Rules — 2009 Amendment. Available at: http://www.law.cornell.edu/rules/frcrmp/rule_41 [accessed July 2012].

Senate Rept. 108-40 at 73. Available at: <http://www.gpo.gov/fdsys/pkg/CRPT-108srpt40/html/CRPT-108srpt40.htm> [accessed July 2012].

U.S. Dept. of Justice - Office of the Inspector General, “A Review of the FBI’s Use of NSLs”, March 2007. Available at: www.usdoj.gov/oig/special/s0703b/final.pdf [accessed February 2012].

Administration’s Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary, 107th Cong., 1st Sess. 56 (2001), p. 107. Available at: http://commdocs.house.gov/committees/judiciary/hju75288.000/hju75288_of.htm [accessed June 2012].

U.S. Department of Justice Office, “Questions Submitted by the House Judiciary Committee to the Attorney General on USA PATRIOT Act Implementation”, July 26, 2002. Accessible at: <http://www.fas.org/irp/news/2002/10/doj101702.html> [accessed May 2012].

U.S. Department of State, “Preparation of Letters Rogatory”, *Travel.state.gov*. Available at: http://travel.state.gov/law/judicial/judicial_683.html [accessed June 2012].

Foreign Intelligence Surveillance Act (FISA) Report. Available at: <http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf> [accessed January 2012].

U.S. Department of Justice, “2011 Annual Report to Congress”, April 30, 2012. Available at: <http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf> [accessed May 2012].

Report of the Department of Justice (2005, 2006, 2007, 2008, 2009, 2010, 2011). Available at: <http://www.fas.org/irp/agency/doj/fisa/2012rept.pdf>
<http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf>;
<http://www.fas.org/irp/agency/doj/fisa/2006rept.pdf> [accessed July 2012].

National legislation and policy documents (not US)

United Kingdom

Memorandum, House of Commons Subcommittee on the Treasury, “How secure is the personal information of UK citizens in light of the USA PATRIOT Act and the limited privacy protections of the United States?”, (February 28, 2008).

Canada

Information & Privacy Commissioner Report for British Columbia, “Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing”, 2004. Available at: <http://web.docuticker.com/go/docubase/5431> [accessed May 2012].

B. Case Law

US Case law

AccessData Corp. v. Alste Tech. Gmbh, 2010 WL 318477 (D. Utah Jan. 21, 2010).

Ballard v. Savage, 65 F.3d 1495, 1498 (9th Cir. 1995).

Burger King Corp. v. Rudzewicz, 471 U.S. 462. (1985).

Cooper Indus. v. British Aerospace Inc., 102 F.R.D. 918, 919 (S.D.N.Y. 1984).

Costello v. United States, 350 U.S. 359, (1956).

Credit Bancorp, 194 F.R.D. At 472.

Doe v. Ashcroft 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004).

FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000).

Guest v. Leis, 255 F.3d 325, 338 (6th Cir. 2001).

International Shoe Co. v. Washington, 326 U.S. 310 (1945).

McGee v. International Life Ins. Co., 355 U.S. 223 (1957).

Murray v. United States, 487 U.S. 533, 108 S. Ct. 2529, 101 L. Ed. 2d 472, (1988).

Pennoyer v. Neff, 95 U.S. 714 (1877).

Perkins v. Benguet Consolidated Mining Co., 342 U.S. 437 (1952).

Sec. & Exch. Comm’n. v. Credit Bancorp, Ltd., 194 F.R.D. 469, 471 (S.D.N.Y. 2000).

Société Nationale Industrielle Aerospatiale v. United States Dist., 482 U.S. 522 (1987).

Starlight Int’l, Ltd. v. Lifeguard Health, LLC, C 08-1894, 2008 WL 2899903 (N.D. Cal. July 22, 2008).

United States ex rel. Turner v. Williams, 194 U.S. 279, 292 (1904).

United Sates v. Calandra, 414 U.S. 338 (1974).

United States v. Field, 532 F.2d 404, (5th Cir. 1976).
United States v. R. Enters., 498 U.S. 292, 297 (1991).
United States v. U.S. District Court, 407 U.S. 297 (1972).
Viacom v. YouTube, 2008 WL 2627388 (S.D.N.Y. 2008).
Whitehouse v. United States Dist. Court for Dist. of R.I., 53 F.3d 1349, 1357 (1st Cir. 1995).
World-Wide Volkswagen v. Woodson, 444 U.S. 286, 297, 100, S. Ct. 559, 567 (1980).

C. Literature

Books

Brilmayer, L., *Fundamentals of American law*, New York, Alan B. Morrison Ed., 1998.

De Busser, E., *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities*, Antwerpen, Maklu, 2009.

Delta, G.B. & Matsuura, J.H., *Law of the Internet*, 2001, Volume 1, p. 3-3.

Jordan, D. A., *U.S. Intelligence Law: A Comprehensive Multimedia Introduction*, 2010, p. 1469.
Available at: http://books.google.be/books?id=KdsUcUIJcLEC&pg=PA1469&lpg=PA1469&dq=%22identifies+the+telephone+numbers+dialed+or+pulsed+from%E2%80%9D+%22+identifies+the+telephone+numbers+to+a+particular+telephone+%28incoming+calls+%29%E2%80%9D&source=bl&ots=35w0IU-AKP&sig=As1PsXc5pSYWeRp0eEQwDUHfe9w&hl=fr&sa=X&ei=nE4tUK_ABOeK0AXni4HoDA&ved=0CCkQ6AEwAA#v=onepage&q=%22identifies%20the%20telephone%20numbers%20dialed%20or%20pulsed%20from%E2%80%9D%20%22%20identifies%20%20the%20telephone%20numbers%20to%20a%20particular%20telephone%20%28incoming%20calls+%29%E2%80%9D&f=false [accessed July 2012].

Krutz, R. L. & Vines, R. D., *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Indianapolis, Wiley, 2010.

Mather, T., Kumaraswamy, S. & Latif, S., *Cloud Security and Privacy*, Sebastopol, Mike Loukides Ed, 2009.

Moerel, E.M.L., *Binding Corporate Rules – Fixing the Regulatory Patchwork of Data Protection*, P.H.D. Thesis, University of Tilburg.

Rittinghouse, J. W. & Hancock, B., *Cybersecurity Operations Handbook*, Burlington, J. W. Rittinghouse & B.Hancock Ed., 2003.

The New Oxford Dictionary of English, Oxford, Judy Pearsall Ed., 1998, p. 1894.

Articles and Contributions

Abramson, L. & Godoy, M., “The Patriot Act: Key Controversies”, *Nrp.org*, February 2006.
Available at: <http://www.npr.org/news/specials/patriotact/patriotactprovisions.html#issue4> [accessed

September 2012].

ACLU, “Reform the Patriot Act Section 215”, *Aclu.org*. Available at: <http://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215> [accessed January 2012].

American Library Association, “Analysis of the USA Patriot Act related to Libraries”, *Ala.org*. Available at: <http://www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/usapatriotactanalysis.cfm> [accessed April 2012].

Anon., “Probable Cause”, *Lectlaw.com*. Available at: <http://www.lectlaw.com/def2/p089.htm> [accessed July 2012].

Anon., “Ex Parte”, *Lectlaw.com*. Available at: <http://www.lectlaw.com/def/e051.htm> [accessed July 2012].

Anon., “Personal Jurisdiction”, *Lexisnexis.com*. <http://www.lexisnexis.com/lawschool/study/outlines/html/civpro/civpro02.htm> [accessed on April 2012].

Anon., “The USA PATRIOT Act, Foreign Intelligence Surveillance and Cyberspace Privacy”, *Cyber.law.harvard.edu*, March 11, 2002. Available at: <http://cyber.law.harvard.edu/privacy/Introduction%20to%20Module%20V.htm> [accessed May 2012].

Anon., “An Overview of the Law of Personal (Adjudicatory) Jurisdiction: the United States Perspective”, *Kentlaw.edu*. Available at: http://www.kentlaw.edu/cyberlaw/docs/views/usview.html#N_4_ [accessed March 2012].

Bauchle, R., Hazen, F., Lund, J., Oakley, G. & Rundatz, F., “Encryption”, *Searchsecurity.techtarget.com*, July 2006. Available at: <http://searchsecurity.techtarget.com/definition/encryption> [accessed June 2012].

Bashir, M. N., Kesan, J. P., Hayes, C. M. & Zielinski, R., “Privacy in the Cloud: Going Beyond the Contractarian Paradigm”, University of Illinois. Available at: <http://assured-cloud-computing.illinois.edu/sites/default/files/AFRL%2520Talk%2520-%2520Privacy-Cloud-Computing%2520Dec-14-2011.pdf> [accessed July 2012].

Berman, A. M. & Chorlak, L.R., “So Simple to State, so Hard to Apply Interpreting 'Possession, Custody and Control' in Today's Complex Corporate World”, *New York Law Journal*, May 16, 2011. Available at: <http://www.velaw.com/uploadedFiles/VEsite/Resources/VinsonElkinsNewYorkLawJournalLitigationArticle.pdf> [accessed March 2012].

Carnabuci, C., “The long arm of the USA Patriot Act: tips for Australian businesses selecting data service providers, freshfields bruckhaus deringer law firm”, November 2011. Available at <http://www.powerretail.com.au/wp-content/downloads/macquarie/The-long-arm-of-the-USA-Patriot-Act.pdf> [accessed June 2012].

De Hert, P. & Bellanova, R., “Data Protection from a Transatlantic Perspective: the EU and US Move Towards an International Agreement?”, September 2008. Available at: <http://www.ceps.eu/content/selection-briefing-papers-prepared-european-institutions> [accessed July 2012].

Dela Rosa, L., “Study of Legal Risks Associated With SAAS Migration”, Research paper of Concordia University, October 2011. Available at:

<http://infosec.concordia.ab.ca/files/2012/04/2011DelaRosa.pdf> [accessed May 2012].

Deutchman, L. & Morgan, S., “The ECPA, ISPs & Obtaining E-mail: A Primer for Local Prosecutors”, American Prosecutors Research Institute, July 2005. Available at: http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf [accessed February 2012].

Dix, D. & Bristow, A., “What in the World is Cloud Computing?”, *Princeton.edu*. Available at: <http://www.princeton.edu/~ddix/cloud-computing.html> [accessed August 2012].

Doyle, C., “Privacy: An Overview of the Electronic Communications Privacy Act”, *Congressional Research Service*, March 30, 2011. Available at: <http://www.fas.org/sgp/crs/misc/R41733.pdf> [accessed July 2012].

——— “Terrorism: Section by Section Analysis of the USA PATRIOT Act”, *Congressional Research Report*, December 10, 2001. Available at: <http://epic.org/privacy/terrorism/usapatriot/RL31200.pdf> [accessed June 2012].

——— “National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments”, *Congressional Research Service*. Available at: <http://www.fas.org/sgp/crs/intel/RS22406.pdf> [accessed February 2012].

——— “National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments”, *Congressional Research Service*, September 8, 2009. Available at: <http://www.fas.org/sgp/crs/intel/RL33320.pdf> [accessed June 2012].

Doyle, C. & Yeh, B. T., “USA PATRIOT Improvement and Reauthorization Act of 2005: A legal Analysis”, *Congressional Research Service*, December 21, 2006, p. 23. Available at: <http://www.fas.org/sgp/crs/intel/RL33332.pdf> [accessed June 2012].

Dunham, R. S., “The Patriot Act: Business Balks”, *Businessweek.com*, November 2005. Available at: <http://www.businessweek.com/stories/2005-11-09/the-patriot-act-business-balks> [accessed May 2012].

Electronic Privacy Information Center, “USA PATRIOT Act Sunset”, *Epic.org*. Available at: <http://epic.org/privacy/terrorism/usapatriot/sunset.html> [accessed May 2012].

Fraser, D. T. S., “The Cloud Thing: Privacy and Cloud Computing”, (Mc Innes Cooper law firm), July 2011. Available at http://www.unb.ca/its/_resources/pdf/about-its/privacy-cloud-davidfraser.pdf [accessed May 2012].

Geist, M. & Homsy, M., “The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?”, A Submission on the USA Patriot Act to the B.C. Information and Privacy Commissioner”, July 2004. Available at: <http://www.docstoc.com/docs/48522538/The-Long-Arm-of-the-USA-Patriot-Act-A> [accessed January 2012].

——— “Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World”, *University of New Brunswick Law Journal*, vol. 54, 2005, pp. 1-34.

Gershater, J., “Cloud Computing and the Patriot Act”, *Cloudbook Journal*, vol. 3, 2012, p. 19. Available at: www.cloudbook.net/resources/stories/partiot-act [accessed August 2012].

Greenwald, G., “DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers”, *Salon.com*, January 8, 2011. Available at: http://www.salon.com/2011/01/08/twitter_2/ [accessed July 2007].

Gruenspecht, J., “'Reasonable' Grand Jury Subpoenas: Asking for Information in the Age of Big Data”, *Harvard Journal of Law & Technology*, vol. 24, 2011, pp. 543-562.

Henning, A. C., Bazan, E. B., Doyle, C. & Liu, E. C., “Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization”,

- Congressional Research Service*, March 2, 2010. Available at: <http://fpc.state.gov/documents/organization/139232.pdf> [accessed June 2012].
- Holder, E. & Reding, V., “Joint Statement on the Negotiation of a EU-U.S. Data Privacy and Protection Agreement by Attorney General Eric Holder and European Commission Vice-President Viviane Reding”, *Justice.gov*, June 2012. Available at: <http://www.justice.gov/opa/pr/2012/June/12-ag-783.html> [accessed June 2012].
- Iqbal, A., Black, B., Fisher, C., Cella, J., Abrams, J., Dugi, M. & Leventhal, R., “Cloud Computing & National Security Law”, The Harvard Law National Security Research Group. Available at: <http://www.lawfareblog.com/wp-content/uploads/2010/10/Cloud-Final.pdf> [accessed June 2012].
- Kerr, O. S., “Digital Evidence and the New Criminal Procedure”, *Columbia Law Rev.*, Jan. 2005, pp. 279-317.
- Kuan Hon, W., Millard, C., & Walden, I., “Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2”, *International Data Privacy Law*, 2012, Vol. 2, No. 1. Available at: <http://idpl.oxfordjournals.org/content/2/1/3.full.pdf+html> [accessed on April 2012].
- Kuner, C., *European Data Protection Law: Corporate Compliance Regulation*, Oxford, Oxford University Press, 2007.
- Labeled, J., “Le « USA Patriot Act » : risque majeur pour la confidentialité des données dans le Cloud”, *Lecercler.lesechos.fr*, March 13, 2012. Available at: <http://lecercler.lesechos.fr/entreprises-marches/high-tech-medias/internet/221144488/usa-patriot-Act-risque-majeur-confidentialit> [accessed April 2012].
- “USA Patriot Act : un risque majeur pour la confidentialité des données dans le Cloud”, *Solutionsauxentreprises.lemonde.fr*, March 26, 2012. Available at: http://solutionsauxentreprises.lemonde.fr/cloud-computing/usa-patriot-Act-un-risque-majeur-pour-la-confidentialite-des-donnees-dans-le-cloud_a-27-630.html [accessed April 2012].
- Lakatos, A.C., “United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud”, January 2012. Available at: <http://www.mayerbrown.com/files/Publication/ce02dec6-f143-46ec-a0a3-53c06d770707/Presentation/PublicationAttachment/f56ea23a-7fd4-40bb-9b78-57e0787774dc/12057.PDF> [accessed April 2012].
- “The Patriot Act and the Cloud: Part 2”, *Mayerbrown.com*, January 2012. Available at: <http://www.mayerbrown.com/news/article.asp?id=12176&nid=20> [accessed March 2012].
- Larson, E., “U.S. Twitter Subpoena Is Harassment, Lawyer Says”, *Bloomberg.com*, January 10, 2011. Available at: <http://www.bloomberg.com/news/2011-01-10/u-s-twitter-subpoena-on-wikileaks-is-harassment-lawyer-says.html> [accessed July 2012].
- Levy, S., “The Patriot Act Grand Jury Disclosure Exception: a Proposal For Reconciling Civil Liberty and Law Enforcement Concerns”, *J.I.C.L.*, 2005. Available at: http://www.kentlaw.edu/jicl/articles/spring2005/s2005_sara_levy.pdf [accessed July 2012].
- Lessig, L., “The Law of Cyberspace”, Essay presented at the Taiwan Net '98 conference, Taipei, March, 1998, p. 2. Available at: http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf [accessed May 2012].
- Liu, E. C., “Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015”, *Congressional Research Service*, June 16, 2011. Available at: <http://www.fas.org/sgp/crs/intel/R40138.pdf> [accessed June 2012].
- Love, J. N. & Ketchen, A. F., “Physical But Not Tangible: Electronic Data Losses”, (RKMC law firm), November 2010, p. 1. Available at: <http://www.rkmc.com/files/Physical-But-Not-Tangible->

Electronic-Data-Losses.pdf [accessed May 2012].

Margolis, J. M., “The European Union v. the Patriot Act: Do U.S. Criminal Investigations Violate E.U. Civil Rights”, *White Paper* Prepared for: International Communication and Information Policy Group Bureau of Economic, Energy, and Business Affairs U.S. Department of State, November 2011, p. 11. Available at: <http://www.subsentio.com/index.php/eng/Site-Archive/White-Papers> [September 2012].

Maxwell, W. & Wolf, C., “Global Reality: Governmental Access to Data in the Cloud”, *A Hogan Lovells White Paper*, May 23, 2012.. Available at: <http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/0fc74c1d-4dc0-4c1e-9abc-eb50ae5679c4/Hogan%20Lovells%20White%20paper%20-%20Government%20access%20to%20data%20in%20the%20cloud.pdf> [accessed June 2012].

McCullagh, D., “DOJ Sends Order to Twitter for WikiLeaks-related Account Info”, *Cnet.com*, January 7, 2011. Available at: http://news.cnet.com/8301-31921_3-20027893-281.html [accessed July 2011].

Mell, P., & Grance, T., “The NIST Definition of Cloud Computing”, September 28, 2011. Available at: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909616 [accessed November 2011].

Nakashima, E., “FBI going to court more often to get personal Internet-usage data”, *Washingtonpost.com*, October 25, 2011. Available at: http://www.washingtonpost.com/world/national-security/fbi-going-to-court-moreoften-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html [accessed February 2012].

Noerr LLP & SNR Denton LLP, “The USA PATRIOT Act - Implications for Cloud Computing”, *Snrrenton.com*, April 2012, p. 18. Available at: http://www.snrrenton.com/pdf/USA_Patriot_Act_Cloud_Computing.pdf [September 2012].

Overby, S., “The patriot Act and your data: should you ask cloud computing provider protection?”, *Cio.com*, January 20, 2012. Available at: http://www.cio.com/article/698432/The_Patriot_Act_and_Your_Data_Should_You_Ask_Cloud_Providers_About_Protection_ [accessed May 2012].

Palfreyman, B. M., “Lesson from the British and American Approaches to Compelled Decryption”, *Brooklyn Law Review*, 2009, Vol. 75, Issue 1, p. 345.

Restatement (Third) of the Foreign Relation Law of the United States (1987). Available at: <http://www.macalester.edu/courses/intl114/docs/restatement.pdf> [accessed February 2012].

Richard, M.M., “International Assistance in Combating Crime”, in De Ruyver, B., Vermeulen, G. and Vander Beken, T. (eds.), *Strategies of the EU and the US in Combating Transnational Organized Crime*, Antwerpen, Maklu, 2002, pp. 227-244.

Rothman, S. & Cohen, C., “The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes”, *hugheshubbard.com*, January 2011, p. 14. Available at: <http://www.hugheshubbard.com/files/FileControl/c71f7d89-f6fc-4194-bae4-82e24dc8184d/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Data%20Protection%20in%20the%20EU%20and%20Its%20Impact%20on%20US%20Discovery.pdf> [accessed September 2012].

Rouse, M., “Infrastructure as a Service (IaaS)”, *Searchcloudcomputing.techtarget.com*, August 2010. Available at: <http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS> [accessed August 2012].

Surgient, D. M., “The five defining characteristics of cloud computing”, *Znet.com*, April 9, 2011. Available at: <http://www.zdnet.com/news/the-five-defining-characteristics-of-cloud-computing/287001> [accessed August 2012].

Surveillance Self-defence, “What Can the Government Do?”, *Ssd.eff.org*. Available at: <https://ssd.eff.org/book/export/html/25> [accessed July 2012].

Tropman, H., “Cloud Technology: When Locating Isn't Everything”, *Australasian Legal Business*, Issue 10.3, April 2012, pp. 42-43. Available at: <http://issuu.com/albaustralia/docs/ozlb10.3> [accessed June 2012].

Waage, T. & Petri, N., “Government Access to Information in ”the Cloud””, (Kroman Reumert law firm), March 2012. Available at: <http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf> [accessed May 2012].

Walden, I., “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent”, Queen Mary University, Research Paper No. 74/2011, p. 11. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067 [accessed June 2012].

Whelan, J. & Hinfey, S.-A., “No Cloud Over the Patriot Act”, (A&L Goodbody law firm), March 2012, p. 15. Available at: <http://www.irelandip.com/uploads/file/No%20Cloud%20over%20Patriot%20Act%281%29.pdf> [September 2012].

Whittaker, Z., “USA PATRIOT Act: The myth of a secure European cloud?”, *Znet.com*, April 27, 2011. Available at <http://www.zdnet.com/blog/igeneration/usa-patriot-Act-the-myth-of-a-secure-european-cloud/8807> [accessed February 2012].

Wikipedia, “HTTP Cookies”, *Wikipedia.org*. Available at: http://en.wikipedia.org/wiki/HTTP_cookie [accessed June 2012].

Wolf, C., “The Role of Government in Commercial Cybersecurity”, *Hldataprotection.com*. Available at: <http://www.hldataprotection.com/uploads/file/WOLFITU%281%29.pdf> [accessed July 2012].

D. Appendice

Copy of a NSL. Dycus, S, Bank, W.C. & Raven-Hansen, P., *Counterterrorism Law*, New York, Kluwer, 2007.

Twitter Subpoena. Available at: <http://www.webcitation.org/5vfUQIMUS> [accessed June 2012].

Appendices

2. TECHNIQUES AND AUTHORITIES FOR COLLECTION OF TRANSACTIONAL DATA

Building on the privacy theory of *Smith*, Congress enacted several statutes that authorized the FBI to use NSLs—issued without any prior judicial order—to obtain transactional records from third-party record holders. Here is a redacted example of such a letter, followed by a judicial decision in a case testing its legitimacy.

~~SECRET~~



ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

U.S. Department of Justice
Federal Bureau of Investigation

(Drafting) Field Division
(Street Address)
(City, State, Zip)
(Month Date, Year)

File No.
In Reply, Please Refer to
[Mr./Mrs.] [COMPANY POINT OF CONTACT]
[TITLE]
[COMPANY]
[STREET ADDRESS]
[CITY, STATE NO ZIP CODE]

Dear [Mr./Mrs.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation

[REDACTED]

In accordance with Title 18, U.S.C., Section 2709 (b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States

You are further advised that Title 18, U.S.C., Section 2709 (c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

[REDACTED]

CLASSIFIED BY 65129/afk/afk/afk
DECLASSIFY ON: 6/30/2025

CLASSIFIED BY 65129/afk/afk/afk
DECLASSIFY ON: 6/30/2025
Patriot Act II-828

~~SECRET~~

DECLASSIFIED BY 65129/afk/afk/afk
ON 8/13/2024

b2-1
b7E-1

b2-1
b7E-1

~~SECRET~~

[Mr./Mrs.] [COMPANY POINT OF CONTACT]

Your cooperation in this matter is greatly appreciated
Sincerely,

[ADIC/SAC Name]
Assistant Director/Special

Agent in Charge

CLASSIFIED BY 65129/afk/afk/afk
DECLASSIFY ON: 6/30/2025
CA# 03-2522

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

CLASSIFIED BY 65129/afk/afk/afk
DECLASSIFY ON: 6/30/2025

~~SECRET~~

DECLASSIFIED BY 65129/afk/afk/afk
ON 8/13/2024

Patriot Act II-828

DEC. 14. 2010 4:14PM

NO. 2530 P. 1/4



U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION
COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: Vivian Ha, Assistant to Tracy McCormick

SENDER'S PHONE NO.: 703 299 3859

SENDER'S FAX NO.: 703 299 3981

NUMBER OF PAGES: 4

Not Including Cover Page

Level of Transmitted Information:

- Non-Sensitive Information
- Sensitive But Unclassified (SBU)
- Limited Official Use (LOU)
- Grand Jury Information
- Tax Information
- Law Enforcement Information
- Victim Witness Information

CONTENTS:

WARNING: Information attached to this cover sheet is sensitive U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited. Please notify this office immediately at the above number to arrange for proper distribution.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)))))))	MISC. NO. 10GJ3793 Filed Under Seal
---	----------------------------	--

ORDER

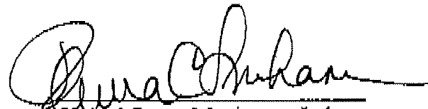
This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Twitter, Inc., an electronic communications service provider and/or a remote computing service, located in San Francisco, California, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

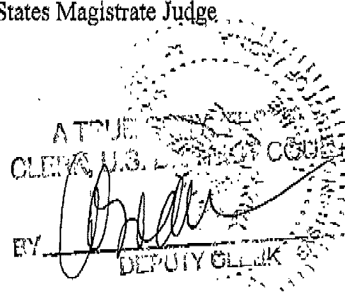
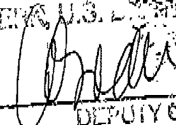
IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that Twitter, Inc. will, within three days of the date of this Order, turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that Twitter shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.


United States Magistrate Judge

12/14/10
Date


ATTORNEY GENERAL
CLERK U.S. DISTRICT COURT
BY 
DEPUTY CLERK

ATTACHMENT A

You are to provide the following information, if available, preferably as data files on CD-ROM, electronic media, or email (tracy.mccormick@usdoj.gov) or otherwise by facsimile to 703-299-3981:

- A. The following customer or subscriber account information for each account registered to or associated with Wikileaks; rop_g; ioerror; birgittaj; Julian Assange; Bradley Manning; Rop Gongrijp; Birgitta Jonsdotir for the time period November 1, 2009 to present:
 - 1. subscriber names, user names, screen names, or other identities;
 - 2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
 - 3. connection records, or records of session times and durations;
 - 4. length of service (including start date) and types of service utilized;
 - 5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
 - 6. means and source of payment for such service (including any credit card or bank account number) and billing records.

- B. All records and other information relating to the account(s) and time period in Part A, including:
 - 1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
 - 2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
 - 3. correspondence and notes of records related to the account(s).

