Can the EU protect its citizen's data while being the U.S.'s partner in the war on terror?

University of Oslo

Faculty of Law

Candidate number:
Supervisor:
Deadline of submission:..... (October/31/2011)

Number of words: 15,512 (max. 18,000)

Content

Thesis Statement: Can the EU protect it's citizen's data while being the U.S.'s partner on the war on terror?

Chapter 1,

The European Union's policies to protect their citizen's data

Chapter 2,

The Laws of the Land:

Article 12, Section 8 of the EU Directives and The United States of America Patriot Act and the precursurors of each.

Chapter 3

Counterterrorism Technology and Privacy:
How new technologies can assist and/or violate data privacy rights by using the information gained

Conclusion

References

http://www.cdt.org/privacy/eudirective/EU_Directive_.html

Article 8 of the Charter of Fundamental Rights of the European Union

http://conventions.coe.int/Treaty/Images/TreatyOffice-Nutshell.pdf

http://europa.eu/abc/symbols/9-may/decl_en.htm

http://europa.eu/legislation_summaries/institutional_affairs/treaties/treaties_eec_en.htm

http://europa.eu/legislation_summaries/economic_and_monetary_affairs/institutional_and_economic_framework/treaties_maastricht_en.htm

http://europa.eu/legislation_summaries/economic_and_monetary_affairs/institutional_and_economic_framework/treaties_maastricht_en.htm

http://www.ena.lu/ single market

http://europa.eu/pol/singl/index_en.htm

http://www.ena.lu/

European Union Law in a nut shell, Ralph H. Folsom

International Guide to Privacy, American Bar Association Privacy & Computer Crime Committee Section of Science &Technology Law, Jody R. Westby, Project Chair & Editor

Griswold v. Connecticut, 381 U.S. 479 (1965)

Katz v. United States, 389 U.S. 347 (1967)

Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age by Christopher Wolf, edition 5 (2011)

U.S. Constitution

U.S. Data Breach Notification Law: State by State by John P. Hutchins, Anne P. Caiola, Seam Park, Christian B. Turner, and Benjamin L. Young

U.S. 115 Statute 272; U.S. Patriot Act, 2001

http://definitions.uslegal.com/m/money-laundering/

ICC World Payments Systems Handbook, 1997 p. 45

Proskauer on Privacy, p 1-29

http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx

www.treasuryandfinance.info/TF/articles/eu-us-swift-agreement-new test.html

EU US Swift Agreement, 11222/1/10 Rev

New York Times, 11/27/01, A Nation Challenged: Airline Security; U.S. Pressuring Foreign Airlines Over Manifest, by Robert Pear

www.files.aea.be/news/AEA_QAPNR.pdf

Congressional Research Service, U.S. – EU Cooperation Against Terrorism, by Kristin Archick www.fas.org/sgp/crs/row/RS22030.pdf at page 12

http://news.bbc.co.uk/2/hi/europe/5028918.stm

Epic.org/privacy/pdf/pnr-agmt-2007.pdf

2007 PNR Agreement

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0018:0025:EN:PDF

EU-US PNR Agreement Found Incompatible With Human Rights, June 29, 2011; www.edri.org/edrigram/number9.13/us-eu-pnr-breaches-human-rights

International Guide to Privacy, ABA Privacy & Computer Crime Committee Section of Science & Technology Law, p.94, 95, Jody R. Westby

List of Judgements/Decisions

Treaties/Statutes: 1. U.S. Patriot Act

2. EU Directive

Secondary Literature

Annex

1.

TITLE III--INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

SHORT TITLE.

This title may be cited as the `International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001'.

SEC. 302. FINDINGS AND PURPOSES.

(a) FINDINGS- The Congress finds that--

(1) money laundering, estimated by the International Monetary Fund to amount to between 2 and 5 percent of global gross domestic product, which is at least $600,000,000,000 annually, provides the financial fuel that permits transnational criminal enterprises to conduct and expand their operations to the detriment of the safety and security of American citizens;

(2) money laundering, and the defects in financial transparency on which money launderers rely, are critical to the financing of global terrorism and the provision of funds for terrorist attacks;

(3) money launderers subvert legitimate financial mechanisms and banking relationships by using them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism, and, by so doing, can threaten the safety of United States citizens and undermine the integrity of United States financial institutions and of the global financial and trading systems upon which prosperity and growth depend;

(4) certain jurisdictions outside of the United States that offer `offshore' banking and related facilities designed to provide anonymity, coupled with weak financial supervisory and enforcement regimes, provide essential tools to disguise ownership and movement of criminal funds, derived from, or used to commit, offenses ranging from narcotics trafficking, terrorism, arms smuggling, and trafficking in human beings, to financial frauds that prey on law-abiding citizens;

(5) transactions involving such offshore jurisdictions make it difficult for law enforcement officials and regulators to follow the trail of money earned by criminals, organized international criminal enterprises, and global terrorist organizations;

(6) correspondent banking facilities are one of the banking mechanisms susceptible in some circumstances to manipulation by foreign banks to permit the laundering of funds by hiding the identity of real parties in interest to financial transactions;

(7) private banking services can be susceptible to manipulation by money launderers, for example corrupt foreign government officials, particularly if those services include the creation of offshore accounts and facilities for large personal funds transfers to channel funds into accounts around the globe;

(8) United States anti-money laundering efforts are impeded by outmoded and inadequate statutory provisions that make investigations, prosecutions, and forfeitures more difficult,

particularly in cases in which money laundering involves foreign persons, foreign banks, or foreign countries;

(9) the ability to mount effective counter-measures to international money launderers requires national, as well as bilateral and multilateral action, using tools specially designed for that effort; and

(10) the Basle Committee on Banking Regulation and Supervisory Practices and the Financial Action Task Force on Money Laundering, of both of which the United States is a member, have each adopted international anti-money laundering principles and recommendations.

(b) PURPOSES- The purposes of this title are--

(1) to increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism;

(2) to ensure that--

(A) banking transactions and financial relationships and the conduct of such transactions and relationships, do not contravene the purposes of subchapter II of chapter 53 of title 31, United States Code, section 21 of the Federal Deposit Insurance Act, or chapter 2 of title I of Public Law 91-508 (84 Stat. 1116), or facilitate the evasion of any such provision; and

(B) the purposes of such provisions of law continue to be fulfilled, and such provisions of law are effectively and efficiently administered;

(3) to strengthen the provisions put into place by the Money Laundering Control Act of 1986 (18 U.S.C. 981 note), especially with respect to crimes by non-United States nationals and foreign financial institutions;

(4) to provide a clear national mandate for subjecting to special scrutiny those foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions or types of accounts that pose particular, identifiable opportunities for criminal abuse;

(5) to provide the Secretary of the Treasury (in this title referred to as the `Secretary') with broad discretion, subject to the safeguards provided by the Administrative Procedure Act under title 5, United States Code, to take measures tailored to the particular money laundering problems presented by specific foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions or types of accounts;

(6) to ensure that the employment of such measures by the Secretary permits appropriate opportunity for comment by affected financial institutions;

(7) to provide guidance to domestic financial institutions on particular foreign jurisdictions, financial institutions operating outside of the United States, and classes of international transactions that are of primary money laundering concern to the United States Government;

(8) to ensure that the forfeiture of any assets in connection with the anti-terrorist efforts of the United States permits for adequate challenge consistent with providing due process rights;

(9) to clarify the terms of the safe harbor from civil liability for filing suspicious activity reports;

(10) to strengthen the authority of the Secretary to issue and administer geographic targeting orders, and to clarify that violations of such orders or any other requirement imposed under the

authority contained in chapter 2 of title I of Public Law 91-508 and subchapters II and III of chapter 53 of title 31, United States Code, may result in criminal and civil penalties;

(11) to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities, and that jurisdictional disputes do not hinder examination of compliance by financial institutions with relevant reporting requirements;

(12) to strengthen the ability of financial institutions to maintain the integrity of their employee population; and

(13) to strengthen measures to prevent the use of the United States financial system for personal gain by corrupt foreign officials and to facilitate the repatriation of any stolen assets to the citizens of countries to whom such assets belong

Can the EU protect its citizen's data while being the U.S.'s partner in the global war on terror?

Data comes in all types and forms. In terms of terrorism, the data that is important is referred as personal data. Personal data is data that helps identify particular individuals from the masses. Personal data can include the following: all medical information that can distinguish an individual from others, government numbers such as a national identification number or social security numbers. Financial information such as bank accounts or credit history are other forms of personal data. Also, any credit card data that can show types of purchases and location of the transactions are forms of personal data. All of this data is collected and stored by the each respective institution or company for their records. Consumers are given a copy of their transactions for their records as well. But the fundamental question(s) are who owns or controls this data and if people's privacy rights are being violated by government authorities or agencies that collect personal data?

Imagine you are a citizen of a European Union member state. You travel to another European Union country and your personal data are stolen. Someone is using your personal data to commit a crime and concealing their real identity. After an investigation by the proper authorities you are cleared of any wrongdoing. You also find out that there are measures protecting your data from misuse and more importantly to clean your records of the misleading information from being shared with other authorities. But imagine as a European citizen traveling to the United States of America and you are mistaken for a terrorist. After the initial investigation by the proper authorities finds you innocent there is no way to have your information deleted from the American's files. Your data is their property now. This issue and

other privacy issues are a major concern within the EU and this thesis will discuss the strengths and weakness for privacy standards in data sharing with the U.S., and how or if that data is ever destroyed by the United States of America due to its global fight on terror.

After September 11, 2011 the United States of America conducted a so-called "war" on terrorism. But this war was not against a country or nation-state, rather many groups who had a hatred of America or the West. In deciding to fight this war, the area of data protection and individual civil rights became a new battlefield that would shape how the growing field of personal data/information may be handled by governments and other "interested" parties around the world. The U.S. and EU have vastly different ideas and laws on data privacy. The big players in the gathering personal data for the implied purpose of stopping terrorism are governments and/or their agencies from around the world. But these governments and/or agencies also must abide by rules and laws that can conflict with their partners from around the globe. So far in the last few years there have been many issues concerning data protection. More and more people have access to devices that keeps personal data and they use these devices to surf the internet for work and leisure. This paper will discuss what personal data is being collected, who is collecting it, and why it is being collected. Also, the paper will discuss the agencies within the United States that have the authority to view and use the data and discuss who watches the watchers. After the comment by a senior U.S. official that stated the intelligence sharing between the CIA and FBI as "third world", understanding the laws and

concerns of the EU nations between sharing data between the United States and European Union will be brought forth in the paper.[1]

As discussed earlier in the introduction of this thesis, the major question about this topic will be concerning whether all citizen's (especially European Union citizens) personal data is being protected as required by law or are laws being violated in pursuit of the fight on terror around the world.

Chapter 1: The European Union's policy to protect the personal data of its citizens.

Each country has their distinct set of laws and regulations that regulate privacy of personal information of their citizens. In Europe, the European Union has a big influence on data privacy laws and regulations on the continent. In general, each country within the European Union makes its own laws on data privacy but the laws are usually based on the EU's data protection directive. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 deals with the protection of the individuals with regard to the processing of personal data and on the free movement of such data.[2] Article 1 of the directive explains the reason behind the directive as the following: (1) Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and (2) Member states shall neither restrict nor prohibit the free flow of personal data between Member state for reasons connected with the protection afforded under paragraph 1

[1] The Practitioner's Guide to Biometrics, ABA Section of Science & Technology Law, William Sloan Coats, editor, 2007

[2] http://www.cdt.org/privacy/eudirective/EU_Directive_.html

of the directive.[3] By following the directives, member states have been able to model their laws to protect their citizens and their borders but the issue that is at the heart of the matter is how are their citizen's data protected by other countries outside of the European Union? Countries like the United States, China, and Australia among others have their own views of data protection and how personal data should be used and gathered. The possibility that data may never be deleted is a real possibility. The European Union data protection rights are outlined in Article 25 of the directive which allows for the transfers of personal data to third countries.

The principles are described in 6 subsections:[4]

- The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,
- The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

[3] *Id*

[4] *Id*

- The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
- Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
- At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
- The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.[5]

With the directives in place, all European Union citizens know that their rights and data will be protected and they have remedies if their rights are violated. But there are still issues concerning what European countries fall under the directives. What happens to citizens that travel to non-EU European countries like Turkey? These issues are truly important in the aspects of data protection. But personal data is tied to civil rights and Article 8 of Charter of

[5] *Id*

Fundamental Rights of the European Union states that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life."[6] Countries in the European Union, and more specifically security agencies and forces can use personal data to help in their respective jobs but must be mindful not to violate European Union citizen's civil rights in their job duties.

In terms of universal standards what does that mean? Both the US and EU have procedures unique to each country and state in the implementation of data sharing between the internal agencies of each county but having a universal system that all countries and regions can follow and abide by is something different. In this paper, I will discuss why a universal standard may be a better option for data sharing between the EU and US and discuss how the present system it insufficient for the purpose of data sharing for fighting global terror and how EU privacy rights may be in violation by the current system.

What countries fall under the European Union's Data Protection Directive?

The European Union was founded after World War II. The purpose for the Union initially was to ensure another great war between European countries did not happen again. The primary purpose of the European Union is in essence sharing resources, ideas, and becoming a unified society in terms of peace and prosperity so to avoid another potential war across the continent of Europe. And information, all information is a part of this sharing theory. The growth of the European Union is a factor in data protection as well. When the European Union was first founded there were only a few countries. These countries included the Netherlands,

[6] Article 8 of the Charter of Fundamental Rights of the European Union, EU Constitution

Luxembourg, Germany, Italy, Belgium, and France. These countries wanted to present a unified front on many issues facing the continent, especially with the USSR (Soviet Union) having a greater presence on the continent after World War II and their occupying of numerous European countries. One big advent of this new union was the 1957 Treaty of Rome or Treaties of Rome. The Treaty of Rome helped establish major core principles: (1) Establishment of the European Economic Community. The European Economic Community or EEC helped to bring about integration and unification of the member states through economic expansion, which included business, trade, and other forms of economic growth.[7] In implementing the policies of this treaty, all member states and future members would be bound to the idea that the union's goal is greater than the particular country's goal. For many nations this would be a hard concept to embrace and adopt. Another important factor out of this treaty came in the resulting Treaty of Maastricht. The Treaty of Maastricht helped pave the way for integration for the member states in policy areas other than economics and created the modern European Union. The Treaty of Maastricht stated its five main goals as:

(1) Strengthen the democratic legitimacy of the institutions;

(2) improve the effectiveness of the institutions;

(3) establish economic and monetary union;

(4) develop the community social dimension, and

(5) establish a common foreign and security policy.[8]

---

[7] http://europa.eu/legislation_summaries/institutional/affairs/treaties_eec_en.htm

[8] http://europa.eu/legislation_summaries/economic_and_monetary_affairs/institutional_and_economic_framework/treaties_maastricht_en.htm

This treaty went beyond the original goal of the Council of Europe economic policies. Not only did it establish and define the role of the current European Union, it also created the three pillars of the European Union which are the European Communities, common foreign and security policy, and police and judicial cooperation in criminal matters.[9] The second and third pillars are important in the matter of security, data protection and individual rights.

The second pillar of the European Union deals with common foreign and security policies. But what does this mean? All European Union members may face similar security issues and by having a unified decision process a unified set of standards to deal with major security issues can be a major plus. With so many countries making up the European Union, a common set of "rules" is key in implementing any changes and sustain fairness for smaller nations without the influence of the major economic powers within the European Union. Security and Foreign policy is just as "political" as economics and in essence the two are intertwined. With the advent of data, especially electronic data being so key this pillar is very important in terms of overall safety with the worldwide terrorism threat. The United States of America has tremendous influence over certain countries and how these countries comply with the pillars of cooperation in terms of justice and home affairs (3rd pillar) and security (2nd pillar) along with Article 8, protecting citizens civil rights will be a challenge for the European Union member states and their traditional ally, The United States of America.

[9] *Id*

B .The "Single Market and Four Freedoms": How they affect data protection and security between countries.

The European Union began to grow slowly throughout the years. The European Union grew to nine member countries with the addition on the United Kingdom (England), Denmark and Ireland in 1973. The European Union continued its growth from its infancy after the fall of dictatorships in Spain and Portugal, plus the unification of Germany. More nations were included into the ranks due to their citizens voting for membership into the European Union. (Norwegian citizens have vetoed membership in the EU on at least two occasions.) As it stands today, the European Union has twenty seven countries comprising its membership. Included in these ranks are former Soviet controlled Eastern European Countries, something that would not have been imagined thirty years ago. Once these countries joined the European Union, they adopted many of the laws and regulations in their national laws that the membership of the European Union adopted as bylaws.

One major aspect of the European Union is the "Single Market and Four Freedoms". In describing the "Single Market" the big advent of if it helped established free movement within the countries of the European Market.[10] The Single Market, as described on the website Europa.eu, "the single market is one of the EU's greatest achievements by it allowing people, goods, services and money move around as freely as they do within one country."[11] Technically

[10] http://www.ena.lu/single market

[11] http://europa.eu/pol/singl/index_en.htm

speaking the single market was the original intention of the Council of Europe in trade around the continent, the "common market".[12] To not have irrelevant restrictions and simplicity of movement within the market also was the intent of the origin of the EU. Even though this advent could be seen as more into the first pillar of the European Union, in that it deals with the community of the European Union, it still has a relationship with the other two pillars in terms of security and law.

The main focus of the four freedoms of the European Union is about free movement. Free movement of goods, people, trade, services, and capital is the main focus and intent of the European Union and its single market. Free movement of goods within Europe is based upon the creation of a customs union.[13] The union helps markets work together to move goods between borders of the member states. The other big incentive of the union is that the member states eliminated customs duties among themselves to help the intent of the single market.[14]

Free movement of people and intellectual property rights are the freedoms that have an effect on data protection and terrorism concerns. With the advent of the European Union came the invention of a European Citizen. With the signing of the Maastricht Treaty on European Union formally introduced the idea of European citizenship and brought with it a selected bundle of civil rights.[15] Citizens can move around from country to country within the union without the need for papers or getting a visa or resident permit. EU citizens could also work in every member state as the union as stipulated in various treaties. The free movement within the

---

[12] http://www.ena.lu

[13] European Union Law in a nutshell, P. 147, Ralph H. Folsom

[14] *Id at 147*

[15] *Id* at 164

European Union includes the citizen's personal data in the form of tax forms, travel documents, bank accounts, and all forms of data that is needed for identification purposes in the digital age. All of this personal data, and where it goes and who has access to it, are important factors in data protection within the European Union. Credit card applications, school information, housing and banking information are all forms of personal data that should be protected. But this data is also used to investigate crimes, especially terrorism. The free movement of people is the greatest achievement of the European Union and the greatest threat. With all of the movement of citizens between member states, the opportunity of terrorist threats comes about. In the last few years there have been bombings in many European cities, including the bombing of the tube in London by terrorists and in Spain. The London bombing during the summer 2005 especially put the European Union on alert of terrorism and in by design the civil rights of their citizens could be affected by the investigations of terrorist acts. The bombing of the London tube occurred during the day and by British citizens of Arab descent who associated themselves with the terrorist group Al Qaeda claiming responsibility for the terror attack.[16] The 2004 Madrid train bombings also injected Europe and European citizens with a first hand knowledge of terrorist and terrorist acts.[17] The terror acts on the four Madrid trains killed one hundred and ninety one people and wounded one thousand eight hundred and forty one people.[18] These two attacks by Al-Qaeda operatives that lived and worked in the United Kingdom and Spain informed the civilized world that the terror threat can happen anywhere or anytime. Not only were military locations targets, but civilian locations and population were targets as well. With the advent of immigration,

---

[16] http://news.bbc.co.uk/2/hi/4659093.stm

[17] http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/

[18] *Id*

European populations are more and more diverse. And the big consequence of the single market is the movement of these citizens around Europe and the world. With governments and businesses being in the digital age, information on citizens is everywhere in the digital domain. From business transactions, credit card uses, shopping, schooling, and every other facet of life, technology and data is intertwined and everywhere. This information can be used for to protect citizens or it can be used in insidious ways. That is why data protection laws are needed and regularly updated to evolve with the technology. Protecting the rights of EU citizens are important to the European Union, but in the global fight at terrorism protecting the civil rights of EU citizens and protecting their homeland can be in conflict.

Chapter 2: The Laws of the Land:

Article 12, Section 8 of the EU Directives and The United States of America Patriot Act and the precursurors of each.

The United States differs from the EU in that privacy laws have not been in the forefront as much as with their European counterparts. That is not to say that privacy of data is not a concern to the United States. After September 11, 2001 terrorist attacks the United States put into places laws and policies that concerned the European Union in terms of data privacy and civil rights. In the U.S., the Patriot Act was put in place to counter terrorism in many forms. International money laundering is a real concern to the United States and some these funds and bank accounts are used to fund terrorism. The United States has enacted laws and regulations that place security over personal privacy. But in dealing with European Citizens are their rights being violated at all costs by the United States government? In the E.U. data directives there are

remedies in place to protect their citizen's personal and private data. First, European citizens can view information about their personal data under Article 12, Right of Access of the EU Data Directive. Article 12 of the data directive deems that European member states shall guarantee every data right to obtain from the controller: Below is the summary of Article 12.

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

European Union citizens also have other remedies to protect their rights and data. Section VII, Article 14 gives each citizen a right to question data about them. Article 14, is referred to as the

"The data subject's right to object". Article 14 states that member states shall grant the data subject the right at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).[19] Basically, this rule allows for the citizen to object and to ensure that the countries make sure that the citizen's data may be transferred to other countries requesting the information or that their country is investigating the data. Either way it gives notice to the citizen or subject, something that is key in the new digital age of technology and information. This is unique to Europe in that the United States has its own version of laws that dictate data protection and how or who can use that data. Jody R. Westby, in his work on the ABA's book International Guide to Privacy, details key principles of the EU Data Protection Directive.[20] The book uses the text of the articles of the EU Data Protection Directive to from the ABA's view on how the EU's directive is organized around certain key principles of information use, which are the following:

---

[19] Id

[20] International Guide to Privacy, American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law, Jody R. Westby, Project Chair & Editor

Notice: Data subjects (individuals to whom personal information relates) must be informed of:

- The identity of the collector of their personal information;
- The uses or purposes for which the information is collected
- How the date subject may exercise any available choices regarding the use or disclosure of personal information;
- Where and to whom information may be transferred; and
- How data subjects may access their personal information held by an organization.[21]

Consent: The book also describes what the directive meant by consent of the citizen in using their data. As detailed in the EU directives, the authors state that the "unambiguous consent" of a data subject is required before any personal information concerning such an individual may be processed.[22] Westby states that the precise meaning of "unambiguous consent" is vague at best but is that true?[23] In the United States of American most people may not know exactly what their information is being used for but in this day and age all people so-called "digital citizens" (people who grew up in a the digital age) have common knowledge that our information is valuable and when we sign on or up for some offer we basically are giving permission for that entity to use that information how they see fit, especially if the product or service we are receiving comes free of charge. Unlike in Europe where well established data privacy laws are stronger than in most regions of the world the United States laws are still evolving to meet the

[21] *Id* at 91; taken from EU Data Protection Directive, Article 10

[22] *Id* at 91; taken from EU Data Protection Directive, Article 7

[23] *Id* at 91; taken from EU Data Protection Directive, Article 7

challenges of the new technology. This assessment may only be my belief but it can be evidenced by teenagers (and adults) signing up for music programs like Pandora which allow users free music streaming for a monthly time limit. The service even asks for information like age, and gender to help find music for the individual user. When thinking in terms of consent it can be assumed that free users of this service or other services like this must know that the currency they are really paying with is their personal information and if they want that data protected then they should use the pay option that Pandora and other services offer.

Consistency: Westby states that the EU directive in Article 6 helps in terms of consistency being the same with controllers and processors using personal information only in strict accordance with the terms of the notice given to data subjects, and any choices such data subjects have exercised with respect to its use.[24]

Access: The same controllers must give data subjects access to the personal information held about them and must allow data subjects to propose corrections to inaccurate information.[25]

Security: Article 18 of the EU Directive is used to understand data security. Organizations must provide adequate security, using both technical and other means to protect the integrity and confidentiality of personal information. The sufficiency of such means is measured with respect

[24] *Id* at 92; EU Data Protection Directive, Article 6

[25] Id at 92; EU Data Protection Directive, Article 12

to the state of the art. In practice, a "reasonable" level of information security is a constantly rising standard, subject to ever more rigorous controls and requirements.[26]

Onward Transfer: Personal information may not be transferred to a third party unless that third party or third parties has been contractually bound to use the data consistently with the notice given to data subjects, any choices that subjects have made with respect to their data's use or disclosure, and applicable law.[27]

Enforcement: The Directive grants a private right of action to data subjects when organizations do not follow the law.[28] Westby states that each EU country has established a Data Protection Authority, which is a regulatory enforcement agency that has the power to investigate complaints, levy fines, initiate criminal actions, and demand changes in businesses' information-handling practices.[29] Westby felt that the EU directives followed an easy organization that allows any citizen to understand the summary of the directive. But the United States laws are more complicated in terms of citizen's rights and the laws in general. In Proskauer on Privacy, the author also reiterates that the seven safe harbor principles are key in US and EU cooperation and every safe-harbor certified company has to follow all seven principles or face deceptive trade practices action under section 5 of the FTC Act or other statue.[30] The Safe Harbor principle is

---

[26] *Id* at 92; EU Data Protection Directive, Article 17

[27] *Id* at 92; EU Data Protection Directive, Articles 6,7,17, and 26

[28] *Id* at 92; EU Data Protection Directive, Articles 22 &23

[29] *Id* at 92; EU Data Protection Directive, Articles 29

[30] Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age by Christopher Wolf, edition 5 (2011) p. 14-22, 23

actually the U.S. – EU "Safe Harbor" Data Privacy accord that was established in June of 2000. The purpose of the Safe Harbor policy was to help United States businesses comply with the EU data directive which prohibits the transfer of personal data to non-European Union nations that do not meet the standards of data privacy protection.[31] Under the policy, the U.S. companies will comply with the data directive while engaging in data transfers but will be under the supervision of the United States government instead of the European Union's strict data protection scrutiny. [32]

The seven principles of the safe harbor agreement are:

Notice: Companies must notify consumers what information is being collected, how that information will be used, and with whom that information will be shared.

Choice: Consumers must be provided with an opt-out mechanism for any secondary uses of data and for disclosures to third parties.

Access: Consumers must be provided with reasonable access to personal information being held by the company.

Security: Companies are required to take reasonable precautions to protect personal information.

Transfer: Companies disclosing personal data to a third party must, with certain exceptions, adhere to the notice and choice principles.

Data Integrity: Reasonable steps must be taken to ensure that data collected is reliable, accurate, complete and current.

---

[31] Data Security and Privacy Law by Ronal N. Weikers, Vol. 1, 2011 Thomson Reuters, p.461

[32] *Id* at p. 461

Enforcement: Companies must ensure that are readily available and affordable independent mechanisms to investigate consumer complaints.[33]

As it shows, the safe harbor policies are similar in scope as the EU directives in data security so this policy was supposed to give the EU nations confidence that US companies would comply with the EU's vision of protecting data and the United States government would enforce the policies. As it stands now, the safe harbor policies are not instilling the confidence in the EU nations and the sharing of data between the EU and the US is still happening at a slow rate.

In the United States, one of the defining moments of privacy as a constitutional right came from the historic case Griswold v. Connecticut, U.S. 479 (1965).[34] In this case, the issue of privacy as a constitutional right was decided by the Supreme Court of the United States of America. The court had to decide on whether a woman's right to use contraceptives should overrule a state law that banned the use of female contraceptives. The United States Supreme Court ruled in favor of the defendant and the term "zone of privacy" came into effect in the United States legal terminology and legal thinking. Even though the 4th Amendment of the U.S. Constitution protected the rights of citizens of unlawful search and seizures, the court in Griswold v. Connecticut, made the case of the "right to privacy" as having a basis in the Bill of Rights of the United States.[35] The Supreme Court stated that the even though the Bill of Rights does not explicitly protect a right to privacy, the Court reason that such a right is found in the "penumbras" of many of the ten amendments of the Bill of Rights.[36] This ruling along with the

---

[33] *Id* at 462; http://www.export.gov/safeharbor/sh_overview.html

[34] Griswold v. Connecticut, 381 U.S. 479 (1965)

[35] *Id* at 484

[36] *Id* at 484

United States Supreme Court ruling in Katz v. United States, 389 U.S. 347 (1967).[37] In the *Katz* case, the Supreme Court felt that state and federal government use of wiretaps must fall under the 4th Amendment protections.[38] The ruling basically gave the impression that there is an individual right of privacy for citizens. These rulings in the 1970's helped shape the right of privacy in the United States. But privacy rights and laws would change and evolve in the United States due to many factors, with the main one being terrorism. The biggest change in law and policy in the United States came with the advent of 1974 Privacy Act.[39] This act made data protection in the United States a major concern. One might think that the 1974 Act beginnings came from business or defense agencies with the American government but it actually came from a special committee from the U.S. Department for Health, Education, and Welfare called "The Secretary's Advisory Committee on Automated Personal Data Systems".[40] The reason this committee was formed was due to concerns over the increased amount of personal information in the federal government's hands[41]. One has to understand the thinking of the American people at this time. The early 1970's was the height of the Vietnam War and the Watergate scandal that led to the resignation of President Richard M. Nixon. Watergate was the name of the office complex in Washington D.C., which was the headquarters of the Democratic National Committee headquarters. Republican Party operatives trying to gain information of the Democrat party's election strategy broke into their offices to steal the information. Their plan

---

[37] Katz v. United States, 389 U.S. 347 (1967)

[38] *Id*

[39] Privacy Act of 1974, 5 U.S.C. §552a

[40] Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age by Christopher Wolf, edition 5 (2011)

[41] *Id* at 12-3

was thwarted and then the entire operation was found out by the two journalists with the Washington Post newspaper. This event helped fuel the American public and government to start focusing on the data protection and laws. Once the committee started to work on the basis of the Privacy Act, they had five main components of it which were the following:

(1) There can be no secret personal data record keeping systems in the U.S. government,

(2) There must be an avenue for American citizens to find out what information about them is in a record and what purpose is it being used,

(3) Safeguards guards need to be in place for citizens to prevent their information being used for an unrelated purpose than originally given without their consent,

(4) A citizen must have a right and opportunity to correct or amend any personal identifiable information, and

(5) Any organization creating, maintaining, using, or dissemireliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[42]

One thing that most Europeans and other laypeople do not know is that the Privacy Act only applies to federal agencies. So what happens to state government agencies? First, one must realize that the United States of America has a unique political system which is one based on Federalism, meaning the United States has a strong central government but shares powers and authority with smaller regional governments. In the United States, the states have specific power inherent to them. Amendment ten of the U.S. Constitution states that "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States, respectively, or to the people.[43] So, in essence state governments were free to design and

---

[42] *Id* at 12-4

[43] United States of America Constitution 10th Amendment

implement privacy acts as long as they did not conflict with the federal laws. Most state laws try to mimic the federal laws so there will be no issues. But with 50 states and numerous territories, sometimes the laws can be confusing. The American Bar Association discussed these issues in the book, U.S. Data Breach Notification Law: State by State.[44] In the book, the issue of notification laws across the various states are analyzed. Various states in the in America have similar notification laws that mimic the ideals of the federal privacy law. The authors also describe how bigger states like California help led the way in new laws and policies, since smaller states usually may adopt their laws on particular topics in Data Protection. California can also be seen as a leader in the U.S. data protection policies due the large number of technology companies that call California home. Google, Apple, Facebook and various technology firms are based in California in the aptly named "Silicon Valley" region. So in looking at the origins of the American data protection rights, the basis of the federal laws seem similar in many aspects to the European Union's basic laws in protecting citizen's data and having a forum to argue the misuse of a person's information. The major difference being the EU Data Directive also applies to data held by any data controller (government and private citizens) unlike the United States where the scope of data privacy is narrower. But over time, the original intent that the Advisory committee has been gutted in favor of more government ownership and use of personal data.

[44] U.S. Data Breach Notification Law: State by State by John P. Hutchins, Anne P. Caiola, Seam Park, Christian B. Turner, and Benjamin L. Young, American Bar Association, (2007)

Terrorism and its impact on U.S. privacy law

The terror acts by members of Al-Qaeda in New York, Washington D.C., and over the skies in Pennsylvania on September 11, 2001 changed the world and the United States of America. No security analysis could have guessed that the United States of America would be so vulnerable and be attacked by terrorists flying commercial airliners into the World Trade Center twin towers in New York City or two more planes could be taken over by a few terrorist and flown into the Pentagon building and an attempted attack on the White House. After this terrorist attack, a slew of new laws were being adopted within the United States to fight terrorist. The most important law that was passed was the United States Patriot Act.[45] This act was passed hastily in the United States Senate after the terrorist attacks on New York City in 2001. The original justification for the United States Patriot Act was to ensure that terrorism would not occur or thrive within the jurisdiction of the United States Government. The primary scope of the Patriot Act was to ensure American safety by allowing unprecedented surveillance and information gathering by federal agencies in the name of safety. Two of the main focuses in this fight on terror was in the form of financial information, by first identifying potential sponsors of terror by bank records and transactions. Another facet of the Patriot Act and the fight of terrorism was the collection of private personal data, especially in the form of airline information. These two issues will be the basis of the conflict of European and American law

[45] U.S. Patriot Act (U.S. 115 Statute 272)– Annex 1

that will be further discussed in their ramifications on personal and private data sharing between the two continents and the effect on the laws further in this thesis.

The original name of the Patriot Act is the Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001.[46] As the act states, its main intent is "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[47] The Patriot Act was detailed in its makeup to include policies and laws to deal with money laundering, surveillance, collecting personal data, and removing safeguards and obstacles for federal agencies to collect any data or information deemed essential to accomplishing the mission of keeping America safe, especially in terms of reviewing banking records and international flight passenger information. Even the name of the law, "Patriot Act" can show a neutral party of the intent of the lawmakers to play on public emotion to get a swift ratification without much debate about the conflicts and issues that may arise from the passage of the law. Two sections of the original Patriot Act that are important to European interest are Sections 808, and 806. Section 808 of the original Patriot Act gives a detailed definition of terrorism.[48] Section 808 describes federal terrorism as any act that may cause destruction or harm to the United States. These acts include destruction of U.S. property like airports and government buildings, assassination or attempted assassinations of government officials.[49] Section 806 of the

[46] Annex 1; U.S. 115 Statute 272- U.S. Patriot Act

[47] *Id*

[48] *Id* at 108

[49] *Id*

Patriot Act deals with the assets of terrorists and how they are recognized by the United States. This section states that "All assets, foreign or domestic,

(1) of any individual, entity or organization engaged in planning or perpetrating any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;

(2) (ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States or their property; or

(3) (iii) derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism against the United States, citizens or residents of the United States, or their property.[50]

The United States government wanted to insure that any and all funds that may help any terrorist can be legally taken by the government if it was suspected of funding any operation or person. This is where a conflict can come into play with the European Union's civil rights laws and data protection laws due to the fact that some personal information can be illegally used to find the source of these funds. Banking protection and privacy laws are intertwined with data protection and the United States in its quest to fight terrorism is systematically tearing down all the established laws and rights in these domains. So the Patriot Act has caused two main issues of data privacy and protection between Europe and

[50] *Id*

the United States in dealing with personal data information of European citizens in the form of airline/flight information and banking data and information.

International Banking and its relationship to terrorism

Banking is a system that has endured and adapted throughout time. In the last two decades, it has become more automated and connected to technology more than ever before. In the past when the only ways to transfer money were person to person transactions or a phone call from the bank, now people are able to make bank transactions from their smart phones. These new forms of electronic transfer made money laundering a growing concern. Money laundering is basically when illegal funds are piled on top of legal funds to hide the illegal cash with the legal cash. The legal definition of money laundering is the processing of criminal proceeds (including but not limited to drug trafficking) to disguise their illegal origin or the ownership or control of the assets, or promoting an illegal activity with or legal source funds.[51] Money laundering is described as systems that have three basic elements; placement, layering, and integration.[52] The first element (placement) of money laundering deals with the launder introducing his or her illegal profits into the financial system. Examples of this illegal action is the breaking up of large amounts of cash into smaller sums that are then deposited into a bank account, or by purchasing a series of monetary instruments (money orders, checks, etc.). After the money has entered the financial system, the second, or layering, stage takes place, where the launderer moves the funds from one account to another at various banks around the world to

[51] http://definitions.uslegal.com/m/money-laundering

[52] *Id*

distance them from the original source. The funds might also be channeled through the purchase and sales of investment instruments or the transfers may be disguised as payments for goods or services. The launderer then moves into to the third stage, integration, in which the funds re-enter the legitimate economy. Afterwards, the launderer might choose to invest the funds into real estate, luxury assets, or business ventures.[53]

Money laundering was a big issue in criminal activities and authorities were able to track criminals by following the cash. But in terms of 21st century banking, all banks and accounts can be accessed throughout the world and money transfers can be made between accounts instantly. This has a great advantage for terrorist or criminals in terms of money laundering. These transfers are possible by the advent of technology and the use of banking identification codes. The most universal of these codes is the swift code. Swift stands for the society for worldwide interbank financial telecommunication. Swift is a bank-owned international financial messaging service that connects some five thousand banks and securities industry participants in one hundred and fifty countries.[54] Swift has offices and data servers located throughout the world, including the U.S. that tracks and stores all information pertaining to money transfers and the personal information used by people to make the transactions. This service has allowed people to make bank and money transfers throughout the world. Terrorist groups and individual terrorist cannot easily pass money for their illegal activities. And it would be impossible for a terrorist to carry large sums of money on his or her person without being noticed by authorities so that is why money transfers are important in terrorism. But in the United States fight against terrorism and money laundering are their requests for information infringing on European civil

---

[53] *Id*

[54] ICC World Payments Systems Handbook, 1997 p. 45

rights? Remember, EU citizens have the right to know if their personal information is being used for a particular purpose.

The United States already was criticized by not having a simple right of redress for citizens by the Gramm-Leach Bliley Act of 1999. The law allowed financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but citizens had no right to stop the companies from the sharing the data but people have the right to opt out.[55] But the opt-out procedures were so esoteric in nature not that many people opted out and thus their personal data was used without their permission in a sense. The United States government also passed the Electronic Fund Transfer Act. This law provides protection for direct debit electronic fund transfers from bank accounts.[56] The Electronic Fund Transfer Act or EFTA applies to financial institutions which include banks as well as persons who directly or indirectly hold an account belonging to a consumer.[57] The initial intent of the act was to regulate entities beyond traditional banks that may have indirect access to consumer bank accounts, as well as service providers.[58] The EFTA act was viewed in some circles as a legal backdoor attempt of collecting previously uncollectable personal and financial data in the United States with the person having notice but not having full understanding of the ramifications of their consent. To put this fear to rest disclosure requirements were enacted for the Electronic Fund Transfers Act. The disclosure requirements require that all consumers must receive certain

---

[55] Proskauer on Privacy, p, I-39

[56] Proskauer on Privacy, p, 2-78

[57] *Id* at 2-79

[58] *Id* at 2-79

information before entering into an electronic transfer contract. The disclosures that consumers must receive are the following:[59]

- A summary of the consumer's liability for unauthorized transfers,
- The telephone number and address of the person to be notified if the consumer believes that an unauthorized transfer has been or may be made;
- A statement of the institution's "business days", which is the days the institution is open to the public for normal business and the number of days the consumer has to report suspected unauthorized transfers;
- The type of transfers consumers can make, fees for the transfers, and any limits on the frequency and dollar amount of transfers
- A summary of the consumer's right to receive documentation of transfers, to stop payment on a pre-authorized transfer, an the procedures to follow to stop payment
- A notice describing the procedures the consumer must follow to report an error on a receipt for an electronic fund transfer or their periodic statement, to request more information about a transfer listed on their statement, and how long the consumer has to make the report;
- A summary of the institution's liability to the consumer if it fails to make or stop certain transactions;
- Circumstances under which the institution will disclose information to third parties concerning the consumer's account; and
- A notice that the consumer may be charged a fee by ATMs where consumer does not have an account.[60]

Some argued that this act and its related disclosure had nothing to do with security, especially in terms of terrorism. It was seen more as a grab to collect personal data information of citizens by the United States government. The United States after the Patriot Act became law, passed and enacted numerous financial laws like Sarbanes-Oxley Act and others. The United States already had some Bank Secrecy Acts on the books to deal with suspect financial activity. One of these

[59] *Id* at 2-80

[60] *Id*

acts dealt with the notification of authorities by banks for most transactions over $10,000. This was under the original Bank Secrecy Act of 1970. The act required banks to retain records and create reports to help law enforcement investigations.[61] In anticipation in trying to deal with the main issue of financiers of terror, the government had to come up with another way to track suspected terrorist funds. The United States Treasury Department set up the Terrorist Finance Tracking Program after the September 11, 2001 terror attacks in New York and Washington D.C. On the Treasury Department's website, the Terrorist Finance Tracking Program or (TFTP) describes in detail its intent to identify, track, and pursue terrorists, such as Al-Qaida and their networks.[62] The website also goes on to state that the U.S. Treasury Department is uniquely positioned to track terrorist money flows and assist broader U.S. Government efforts to uncover terrorist cells and map terrorist networks here at home and around the world.[63] When the TFTP programs finds and investigates some potential "financial" terrorist it issues subpoenas thru the Swift banks.[64] The United States was only able to review that financial information if it was a specific terrorism investigation.[65] After much deliberation, the EU stop storing data in the U.S. servers and American agencies did not have immediate access to financial information. An agreement between the two powers was needed if the United States would have access to the Swift information. The U.S. government and the agencies requesting the information had to have a real fear or belief that the country's security was in stake thus all privacy concerns could

---

[61] Proskauer on Privacy, p. 1-29

[62] http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx

[63] *Id*

[64] *Id*

[65] *Id*

be trumped by national security. In analyzing the concerns of the European Union in terms of protecting their citizens personal the data, the United States had to devise a program to appease the Europeans and still be able to get the financial data they wanted.

In 2009, the EU and the United States agreed to a 12 month deal that would create a commission to determine if the United States under the Terrorist Finance Tracking Program subpoenas for information would be given to the Treasury Department. This was due to the fact that European citizens did not have a right to access their information while in U.S. hands and the United States was accused of storing and keeping personal information on European citizens even after they were deemed not to have a right to keep the information. The European Union countries were not pleased at the policies of the United States government in their violation of EU laws respecting civil rights on data protection. During this period of the interim agreement, the two sides worked on a new agreement to satisfy the needs of all parties involved. In 2010, the United States and European Union renewed their allegiance and signed a new Swift agreement. The new/revised agreement gave the European Union the assurances they were looking for in terms on safeguards for their citizen's personal data.

The following pages contain an excerpt from the European Parliament with its summary of the new agreement as reported by www.treasuryandfinance.info;[66]

["The new version of the SWIFT anti-terrorist agreement on bank data transfers to the USA was approved by the European Parliament on July 8th, 2010. MEPs rejected the agreement in its previous form four months ago but since then have negotiated certain safeguards for Europe's citizens and won an undertaking that the EU will start work in the second half of this year on a

[66] www.treasuryandfinance.info/TF/articlues/eu-us-swift-agreement-new test.html

European data processing system that precludes the need to transfer data in bulk to the USA. The recommendation that Parliament approve the agreement, drafted by Alexander Alvaro (Alliance of Liberals and Democrats for Europe), was adopted by 484 votes to 109 with 12 abstentions. The agreement is due to take effect on 1 August this year.[67]

The key to the deal for Parliament was the eventual elimination of "bulk" data transfers. In exchange for backing the agreement, MEPs won an undertaking that work on setting up an EU equivalent to the US "Terrorism Finance Tracking Program" (TFTP), which would preclude the need for bulk data transfers, will start within 12 months. Once Europe has a system enabling it to analyze data on its own territory, it need only transfer data relating to a specific terrorist track.

Another innovation of the new agreement is that it empowers "Europol", the EU's criminal intelligence agency based in The Hague, to block data transfers to the USA. Europol will have to check that every data transfer request by the US Treasury is justified by counter-terrorism needs and that the volume of data requested is as small as possible.

The new version of the agreement also provides that the use of data by the Americans, which must be exclusively for counter-terrorism purposes, is to be supervised by a group of independent inspectors, including someone appointed by the European Commission and the European Parliament. This person will be entitled to request justification before any data is used and to block any searches he or she considers illegitimate.

The agreement prohibits the US TFTP from engaging in "data mining" or any other type of algorithmic or automated profiling or computer filtering. Any searches of SWIFT data will have

---

[67] *Id*

to be based on existing information showing that the object of the search relates to terrorism or terrorism finance.

In February 2010, MEPs demanded that under any new version of the agreement European citizens should be guaranteed the same judicial redress procedures as those applied to data held on the territory of the European Union. The new proposal says this time that US law must provide a right of redress, regardless of nationality.

Extracted data may be retained only for the duration of the specific procedures and investigations for which they are used. Each year, the US Treasury must take stock of any data that have not been extracted, and hence individualized, which will no longer be of use for counter-terrorism purposes, and delete them. Such data must be deleted after five years at the latest. The agreement is due to enter into force on 1 August 2010, for five years, and will be renewable year-by-year thereafter. However, Europeans and Americans will have to assess how the agreement's safeguards and control systems are functioning, at the latest within six months of its entry into force. The Commission is to start work in the second half of 2010 on the creation of the European TFTP and must publish a progress report within three years.] [68]

As the excerpt states, the right of redress and issue of bulk data has been fixed so European Union member states can feel confident that their citizen's rights are not be violated by the United States fight in terrorism. In reading the EU – US Swift agreement, Article 1 states that the purpose of the revised agreement was to ensure respect and protection of personal data.[69] But the main advent of the new agreement comes into view when dealing with the protections

---

[68] *Id*

[69] EU US Swift Agreement, 11222/1/10 Rev 1

that European members want for their citizens. Article 3 is titled, "Ensuring Provision of Data by Designated Providers".[70] Article 4, which is titled U.S. Requests to Obtain Data from Designated Providers works in conjunction with Article 3 in maintaining that only relevant and narrowly specified data is given to the U.S. for their investigation in the fight of terror instead of the "bulk" data that the American agency was getting in the past. Subdivision 2 (a) of Article 4 states that information request must identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; (b) clearly substantiate the necessity of the data; and (c) be tailored as narrowly as possible in order to minimize the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses.[71] Judith Crosbie detailed Europe's issue with the America's fight on terror in an article on the website europeanvoice.com. In her article, Data protection v terrorism, the author discussed how after the 2001 terror attacks the United State through its various government agencies gather more and more personal data on people.[72] These actions of gathering unlimited data without a valid reason bothered the European Union countries and the initial agreement worked out between the United States and the European Union was doomed to fail. Title III of the Patriot Act dealt exclusively with money laundering in terms of terror financing. Title III of the Patriot Act is called the International Money Laundering Abatement

[70] *Id*

[71] *Id* at 17

[72] Data protection v. terrorism, by Judith Crosbie, www.europeanvoice.com

and Anti-Terrorist Financing Act of 2001.[73] Annex 1 is the exact original text of the relevant portion concerning the reasoning and purpose of the legislation as put into law by the United States Congress (the U.S. House of Representatives and the United States Senate) and signed by President George W. Bush, 43rd President of the United States of America: The U.S. Patriot Act (Please see Annex 1)

The act works in conjunction with other sections of Title III like the Section 352, which deals with the Anti-Money Laundering Programs and amends the existing Bank Secrecy Acts like the $10,000 dollar reporting limit for any financial transaction that takes place in the United States. Section 352 states that in order to guard against money laundering through financial institutions, financial institutions shall establish anti-money laundering programs, including, at a minimum:

- The development of internal policies, procedures, and controls
- The designation of a compliance officer
- An ongoing employee training program
- An independent audit functions to test programs.[74]

In terms of regulations the act requires the Secretary of the Treasury after consultation with the appropriate Federal functional regulator may prescribe minimum standards for programs established under paragraph (1), and may exempt from the application of those standards any financial institution that is not subject to the provisions of the rules contained in part 103 of title 31, of the Code of Federal Regulations, or any successor rule thereto, for so long as such

[73] U.S. Patriot Act, Title III Money Laundering Abatement and Anti-Terrorist Financing Act of 2001

[74] Section 352 of the U.S. Patriot Act

financial institution is not subject to the provisions of such rules.[75] But in terms of pure personal data, not narrowed down and given to the government Section 626 of the Patriot Act is the one that caused the European Union so many headaches. Section 626 deals with Disclosures to governmental agencies for counterterrorism purposes.[76] Under Section 626, Consumer reporting agencies shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations or intelligence or counterintelligence activities or analysis related to international terrorism when presented with a written certification by such government agencies where the information is necessary for the particular agency's conduct or investigation, activity or analysis.[77] This is the type of bulk data that was outlawed in the new agreement between the United States of America and the European Union. There would have to be a good showing that this data is narrow enough in terms of the new requirements, but as the 2001 law was written in terms that were so vague that the United States was allowed unprecedented access to their citizen's personal information and data. Now the new agreement in place, these old arguments are moot now. The U.S. will get access to EU consumer names, addresses, accounts, and all other relevant data but the request for data must have a valid reason behind it and the request be narrowly tailored to a specific investigation as I have discussed earlier in the paper.

---

[75] *Id*

[76] Section 626 of the U.S. Patriot Act

[77] Section 626 of the U.S. Patriot Act

Flight information/Data on European Union citizens

In remembering September 11, 2001, the terrorists that high-jacked the commercial airliners came to the United States from other countries around the world. Most of them terrorist flew into the United States from European Union airports. The U.S. after 2001 began to request airline passenger information and data. This information is generally referred to as PNR or passenger name record. As reported in the New York Times article by Robert Pear on November 27, 2001, if foreign airlines did not turn over the names of their passengers so the United States could investigate potential terrorists, then all of their passengers would likely have a difficult time entering the country and their airlines could face hefty fines.[78] A PNR or Passenger Name Record is a record stored on the database of commercial airlines Computer Reservation System or in a Global distribution system.[79] A PNR or Passenger Name Record contains the travel information for a passenger or a group passengers traveling together. The travel information of the PNR consists of the following data:

(1) The PNR record locator, the travel agency or airline office identification,

(2) the date of the reservation, names of the passenger(s),

(3) the travel itinerary for this specific PNR which is the flight number, date, departure and arrival stations, and

(4) time of departure and arrival.[80]

---

[78] New York Times, 11/27/01, A Nation Challenged: Airline Security; U.S. Pressuring Foreign Airlines Over Manifest, by Robert Pear

[79] www.files.aea.be/news/AEA_QAPNR.pdf

[80] *Id* at 2

The article also states that the PNR may also contain ticketing information, fare details (like restrictions on the ticket), form of payment, additional contact information like phone numbers or business addresses and any other specific information that unique to the individual traveling.[81] International airlines carriers were not happy about the new mandatory requirements for passenger data requested by the United States. European countries protested immensely due to the lack of data security in the U.S. and the unknown factors of what would happen to the information about their passengers.

After September 11, 2001 the world found out how government agencies within the United States dedicated to security (the FBI, CIA, etc.) did not share important data on potential terrorist properly and this data could often be misused. After much negotiation, the European Union and the United States came up with a temporary PNR agreement in 2004. This agreement laid the groundwork for what and how this data would be used. The 2004 agreement gave the United States the information it was seeking but the European countries were leery of the implications to the privacy rights of their citizens. Within the 2004 PNR agreement, airlines operating flights to or from the United States had to provide U.S. authorities with passenger name record or PNR data in their reservation and departure control systems with 15 minute of a flight's departure.[82] This agreement was later stuck down by the European Court of Justice. As reported by the BBC, the court said the "decision to hand over data, including addresses and credit card details, lacked an appropriate legal basis".[83] So with Europe fears being given legal

---

[81] *Id* at 2

[82] Congressional Research Service, U.S. – EU Cooperation Against Terrorism, by Kristin Archick www.fas.org/sgp/crs/row/RS22030.pdf at page 12

[83] http://news.bbc.co.uk/2/hi/europe/5028918.stm

legitimacy, the two sides had to go back to the drawing board accommodate each other. The next stab at the PNR issue came in the form of the 2007 agreement. This agreement stayed in effect for three years. The agreement had more substantial redress opportunities for EU citizens and an exclusive remedy if the it was determined that the U.S. breached the agreement. The U.S. Department of Homeland Security made concessions in its decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that related to European citizens.[84] Also within the 2007 agreement, the Department of Homeland Security maintained a system that was accessible to individuals, regardless of their nationality or country of residence, for redress to people seeking information about them or correction of their PNR data.[85] The remedy was an entire termination of the agreement which was very significant to say the least.[86] Section 8 of the 2007 agreement discusses the new remedy in detail in that "The exclusive remedy if the EU determines that the United States has breached this Agreement is the termination of this Agreement and the revocation of the adequacy determination referenced in paragraph 6. The exclusive remedy if the U.S. determines that the EU has breached this agreement is the termination of this Agreement and the revocation of the DHS letter."[87] This issue allowed this agreement to be adopted because the EU gained some leverage over the United States in respect to their data and civil rights when the United States tried to collect information in its' fight of global terrorism. After a review last year of the 2007 act, the two sides have been in negotiation

---

[84] Epic.org/privacy/pdf/pnr-agmt-2007.pdf

[85] *Id*

[86] 2007 PNR Agreement

[87] http://eur-lex.europa.eu/LexUriServ/SexUriServ.do?uri=OJ:L2007:204:0018:0025:EN:PDF

on revising and amending the act. But in May of this year (2011), the European Commission has warned that the new draft of the European Union- United States of America (EU-US) agreement on the exchange of PNR data is not compatible with fundamental privacy rights of European citizens.[88] Sticking points in the new draft included the 15 year retention period for collected data to be stored and held by the United States.[89] Also the lack of judicial redress for data subjects, and the lack of guarantee of independent oversight among other issues cause concern for the commissioner's lawyers. The lawyers also do not agree with the PNR data being used for U.S. border security as this is being seen as being as part of the original intent of the PNR agreement.[90]

Chapter 3

Counterterrorism Technology and Privacy: How new technologies can assist and/or violate data privacy rights by using the information gained

Humans have used technology to assist the population in tasks throughout time. With the fight against terror being a high priority, new technologies have been invented to assist authorities in the fight against worldwide terror. Surveillance technologies are an important tool in the data collection. Surveillance is defined by Webster's online dictionary as – close watch kept over someone or something.[91] Surveillance can be accomplished in many ways to

---

[88] EU-US PNR Agreement Found Incompatible With Human Rights, June 29, 2011; ww.edri.org/edrigram/number9.13/us-eu-pnr-breaches-human-rights

[89] *Id*

[90] *Id*

[91] www.merriam-webster.com

gain information about a person In terms of technology, watching someone or something can be done in a number of ways, with the most widely used surveillance in modern times being electronic surveillance. Electronic surveillance under U.S. law includes interception by "electronic, mechanical, or other surveillance device of the contents of any wire or radio communication.[92] The Foreign Intelligence Surveillance Intelligence Surveillance Act rules surveillance laws in the United States.[93] In terms of video surveillance of foreign suspects for video surveillance the FISA or Foreign Intelligence Surveillance Intelligence Surveillance Act rules since most security cameras are of the silent variety, meaning that there is no sound. Under the FSIA video surveillance conducted for foreign intelligence purposes, including "silent video" that captures no aural communication.[94] Video monitoring is a widely used surveillance technology used gather information or data on individuals. Video cameras are used to monitor activity in many cities worldwide. These cameras are usually posted in open areas and high crime areas. In London, with a population of 8.615 million inhabitants is the most populous city within the European Union with numerous CCTV security cameras covering the entire city.[95] London is also one of the most diverse cities in the world, with over 270 different ethnic groups and over 300 languages spoken by the inhabitants of the city.[96] Data obtained from video cameras can be used to gain valuable information about an individual. This data can included physical traits, habits in the form of regular stops or appearances at certain places at the

---

[92] 50 USC § 1801 (f) (1)

[93] 50 USC § 1801- 1811

[94] 50 USC §1801 (f)(4)

[95] https://www.cia.gov/library/publications/the-world-factbook/geos/uk.html

[96] http://wwwhttp://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

same times each day, etc. This data can be used to create an accurate profile of a person without their knowledge and be shared with other law enforcement agencies as a working profile or file information about the potential suspect. An older form of data information gathering through surveillance is by monitoring telephone calls between individuals. Telephone surveillance is a process of monitoring phone calls between one or two or more phone lines. This type of surveillance is usually referred to as tapping the phone or phone tapping. Usually it consisted of a relay device called a "bug" to be placed physically inside the phone to monitor the telephone call. Devices also can be placed in the general vicinity of a phone call to listen and record telephone calls between individuals without the parties having knowledge of their calls being monitored. With the advent of cellular and wireless phones, phone surveillance has evolved as well. In the past, the physical bug needed to be in or near the phone, but now wireless signals from telephones can be intercepted through the air with sophisticated devices.

Another instance that surveillance through technology can be used be monitoring computers to glean information about a subject which is called data mining. Data mining is a process to gather information about a person through information on their computer which can included the history of the internet sites visited by the user of the particular computer. Data mining can be described as the process of analyzing data from different perspectives and summarizing the gleaned surveillance data from the suspect and complied into useful information for use as a deterrent to potential terror activity.[97] This information is particularly important in data privacy corners in that it can help establish a target or person's habit. This profile of an intended target person can be used by authorities to gain a working knowledge of the person's habit and or

[97] Counterterrorism Technology and Privacy, McCormick Tribune Foundation, 2005, Patrick J. McMahon, Conference Rapportuer p.46

intentions. This information can be also be used in nefarious ways as well. By gathering information this way, five important advances in surveillance occurred. The five important uses of data mining has helped with new flow of information in:

(1) inexpensive and easily dispersible sensors that can be placed almost anywhere and have the ability to locate by detection;

(2) new storage devices that have dramatically reduced data storage costs;

(3) broadband and wireless communications with the ability to transmit large volumes of information at high speed and with high reliability;

(4) dramatic increases in computational processing power;

(5) the development of advanced algorithms that allow for the development of data mining;

(6) global positioning system technologies in cell phones, vehicles and personal digital assistants; and

(7) the Internet, which makes all this data accessible at any time from any place.[98]

With these new technologies at hand, authorities are gaining access to information that previously

could not be easily attained in the past. In the Unites States of America, their Supreme Court dealt with a case in which new technology was used to find out information and the court had to analyze if that particular technology violated the privacy rights of the defendants in the case. The case is at question is Kyllo v. United States, 533 U.S. 27 (2001).[99] In the case the police used an infrared camera to take pictures of a residence to for evidence that marijuana was being grown at the residence. Under U.S. law, the fourth amendment of the United States constitution which deals with the citizen's right to privacy and if it is responsible for the police to use that

---

[98] Counterterrorism: Technology and Privacy, p. 41-42; McCormick Tribune Foundation, Patrick J. McMahon, Conference Rapportuer

[99] *Id* at 39; Kyllo v U.S., 533 U.S. 27 (2001)

camera without a warrant. With this case coming before the highest court of the land in the United States, the use of new technologies and how it affects privacy rights will be at the forefront of data issues. Another type of electronic surveillance deals with monitoring computer history. Government agencies are able to track and know which internet sites a person may visit by a variety of ways including monitoring programs or tracking/phishing programs or viruses. Trojan horse programs are a common way to gather information from a computer. A Trojan horse is a benign program or application that contains malicious code. The code is usually on some free program or software that the user may download. Once this code is activated, the Trojan horse program can major damage to a computer by erasing data, making the computer inoperable or worse. But in terms of data privacy, the trojan horse can install a keystroke logger capable of capturing everything a user types into the keyboard or allowing remote access to the computer to a hacker.[100] Computers can also be compromised by tracking programs that give access to remote sources about information on your computer and sites visited by the particular computer targeted. The German government recently was discovered to have been spying on its own citizens using a trojan horse program. The virus, called "R2D2" recorded skype calls, monitors messenger services from yahoo, Microsoft, and ICQ.[101] The R2D2 trojan horse also captured keystrokes from the leading internet web browsers and snapshots of computer screens of German citizen.[102] This action violates the EU data privacy laws and yet the German government officials that authorized the action were aware of the

---

[100] ABA Section of Antitrust Law, Data Security Handbook (2008), p.5

[101] http://www.securityweek.com/german-government-paid-€2m-r2d2-malware

[102] *Id*

consequences. But the citizens will have a way to find out if they were targeted and have their data erased by the authorities. Yet, if this information was transferred to the United States due to their national security concerns, these citizens would have a difficult if not impossible time to find out if their data is being used or not. The Supreme Court of the United States exempted foreign intelligence from procedural requirements applicable to national security matters affection US citizens in U.S. v U.S. District Court, 407 U.S. 297 (1972), so foreign citizens rights would not be a concern to the United States in privacy law.[103] The Patriot Act authorizes the government agencies of the United States to collect and use relevant data at it deems important to further the security of the country.

Another big development of data collection and technology comes in the form of biological data. The term DNA has become a mainstream term for population with common knowledge of what DNA is and entails being broadcast around the world on television shows and news programs. But in terms of counter terrorism and privacy rights, biometrics is the new technology that authorities will use in the present and future for security reasons. Biometrics can be described as the measurement of any physiological characteristic or personal trait that is distinctive to an individual or a behavioral characteristic.[104] In understanding biometrics, the data can be split in two different types of traits, physiological and behavioral characteristics.[105] Examples of physiological biometrics include fingerprints, iris scans, facial recognition, and hand geometry.[106] Examples of behavioral biometrics include voice recognition, keystroke

---

[103] The U.S. Intelligence Community Law Sourcebook: A compendium of National Security Related Laws and Policy Documents, 2011 Edition, ABA Standing Committee on Law and National Security, Andrew M. Borene, Editor

[104] The Practitioner's Guide to Biometrics, William Sloan Coats, editor; utilizes secondary source at http//www.ibgweb.com/reports/public_reports.html

[105] *Id* at p.3

recognition and signature recognition.[107] With this information of a person's biometric data, governmental authorities can use biometrics as a tool to fight terrorism since physiological characteristic (especially iris characteristic) are one of a kind that not even identical twins share the

identical biometric data.[108] With the knowledge of the science of biometrics being able to identify a person better than the current security measures, biometrics would seem to be the best system to fight terror in that terror suspects could be identified at a moments notice if there information is cataloged in a network of databases and if the biometric data is not taken without the person's knowledge. Biometrics and privacy of personal data can also come into play in corporate data protection in terms of health care and security. With more and more personal data detailing the health of a person being automated and transferred between hospitals, this data can have a positive or negative effect in terms of data privacy. For international students trying to get student visas, their biometric and healthcare data must be disclosed to U.S. authorities for their applications to be reviewed. In the United States, citizens health and biometric data is protected by the existing privacy laws in the country. One of these laws is the Health Insurance Portability and Accountability Act of 1996. [109] The Health Insurance Portability and Accountability Act or HIPAA major goal is to required health providers and related entities to implement privacy safeguards for the patient's privacy rights. [110] The provision

---

[106] *Id* at p.4

[107] *Id* at p.5

[108] *Id* at 2.

[109] 42 U.S. C. § 1306; ABA Section of Antitrust Law, Data Security Handbook (2008) p, 26

[110] *Id* at p. 26, 27

states that the entities must implement "appropriate administrative, technical, and physical safeguards" to protect the patient's health information. [111]The HIPAA and the revisions of the act main focus is to ensure protection of a patient's personal data. In the 2003 HIPAA Security Rule, the following safe guards of personal data were described:

- The confidentiality, integrity, and availability of all personal health information created, received, stored, or transmitted by the entity;
- Protection of personal health information from any reasonably anticipated threats or hazards;
- Protection of personal health information from disclosures prohibited by the HIPAA Privacy rule; and
- Ensuring the entity employees and agents comply with the Security Rule.[112]

Data privacy concerns are important as an issue in discussing and using biometrics as a tool in fighting terrorism. Currently, most countries use some form of biometrics as security measures at airports and passports currently have biometric chips with a person's information that can be checked against stored information about terror suspects.

In the European Union, Article 25 of the Data Directive permits transfers of "personal" data from European Union nations to countries not in the EU only if the outside country has adequate levels of protection of the personal data being transferred.[113] This rule can impair the fight on terror if the EU officials of a particular country feel that certain countries means of protecting data do not fall under the standards of the European Union and not permit the transfer of the personal data requested. This data could be used to update a country's biometric database

---

[111] *Id* at p.27

[112] *Id* at p. 27

[113] *Id* at 29; EU Data Directive, Article 25

to stop potential terror suspects. But with every law, there is always an exemption or loophole to the law or rule. The exemption in the case of Article 25 of the EU data directive is found in Article 26(1) with allows the transfer of the personal data if the nations have adequate levels of data protection and the transfers are necessary on important public interest grounds.[114] But in transferring personal data to United States law enforcement and intelligence agencies the Article 26(1) exemption will not allow transfer under the law. [115] This issue hampers the United States in its commitment to fight terror, yet the European Union must protect the data of its citizens.

The American Bar Association is suggesting that the European Union amend the Article 26's public interest exemption so that the transfers of personal information to U.S. agencies can take place and this information can be analyzed and stored by the appropriate authorities to assist in the fight on terror. Even though the European Union has set a priority to protect the privacy rights of its citizens, it is interesting to note that all asylum seekers to EU countries are required to give biometric data in the form of fingerprints to the proper authorities.[116] So who or what agency controls or monitors the use of the personal data collected to ensure privacy rights are being protected? In the United States, the Total Information Awareness program was created to address the development on new technologies to assist the security of the country and to protect privacy.[117] The TIA program was also supposed to elevate any concerns about U.S. government overreach, but politics within the U.S. government did not allow the TIA program to

---

[114] *Id* at 29; EU Data Directive, Article 26(1)

[115] *Id* at 29

[116] *Id* at 24

[117] Counterterrorism Technology and Privacy, Patrick McMahnon, Conference Rapporteur, McCormick Tribune Foundation, p. 40

succeed and thus concern their European partners in how other government agencies, (i.e. the CIA, DIA, and FBI) analyze and use the personal data collected on foreign individuals.

Other issues

The conflicts between the data protection rights of the European Union and the interest of the United States in its global fight on terror can be worked on. As I have shown in this paper, in terms of cooperation the road has been bumpy but the two powers have worked out their difference to achieve both of their goals. The United States government has shown when it feels that some information is needed, it will take measures to gain access of that information at all cost. Recently it was reported that Google Software gave the United States personal information and data on its European users. As reported by Lucian Constantin in softpedia.com, Google admits handing over European User data to US Intelligence agencies.[118] At the crux of the article is the issue of the Patriot Act and how it commands that all companies incorporated within the United States must hand over data administered by their foreign subsidiaries if requested the government.[119] Microsoft's UK's managing director also stated his company can be compelled to share data with the U.S. government regardless of where it is hosted in the world.[120] Especially in terms of the airline/PNR data, both sides have compromised on their positions so that they both can continue their working relationship. Taking a look at the cooperation of the U.S. /EU Safe Harbor Agreement shows how both parties can work together on important privacy issues. Due to the differences in how law and policies are enacted and carried out, the

---

[118] http://news.softpedia.com/news/Google-Admits-Handing-over-European-User-Data-to-US-Intelligence-Agencies-215740.shtml

[119] *Id*

[120] *Id*

U.S. Department of Commerce and European Commission were able to come up with this plan that would protect business in their international dealings and also provide the privacy protections to EU citizens.[121] With more bipartisan agreements, potential conflicts in new legislation can be discussed by all interested parties so that the legislation can be tailored to meet the demands of all parties without harming one side.

Conclusion

The United States of America was shaken to the core by the events of September 11, 2001. Even though the country had just dealt with a homegrown terror attack in Oklahoma City a few years ago that destroyed a federal building, it still didn't prepare the country for the site of two commercial airliners slamming into the twin towers in New York City. That event, plus a new administration in power in Washington cause a rush to enact a bevy of laws that had not been thought out for the issues and complications they may have on our international allies due to the fact that the United States is a world leader and when we make laws, not only do they have impact on domestic actions but they have a powerful impact internationally as well. In the United States of America's rush protect its shores and borders, the United States must not infringe on the civil and human rights European citizens in terms of personal privacy data. The EU has made their intentions known for years that they are moving towards an understanding of certain fundamental rights for all citizens. Also, the U.S. is in the best position of all countries to know how difficult and complicated EU member nations have in implementing laws from EU commissions. EU member states are all individual countries that must implement the policies in

[121] International Guide to Privacy, ABA Privacy & Computer Crime Committee Section of Science & Technology Law, by Jody R. Westby, p. 94, 95.

their existing national laws so it can be a long and difficult process to ensure that their individual national laws and the EU laws are similar and are not in conflict.

This is similar to the issue that individual states in the U.S. have to deal with when making new and ensuring they do not violate federal rights or laws. The EU Data Directive lets other countries know what is expected when dealing with citizens or business data of member states but they must also remember that it is just a standard per se, each country has its own specific laws. In closing, the initial question of can the EU still protect its citizen's data against the needs of the U.S. is tricky at best. As the United States has shown in the Google case and other examples is that they will find a way to get the information they need for the fight on terror regardless of the European's feelings or policies on privacy. But the United States has shown that it is willing to work with the EU to put in place policies that protect citizens data as well. With the Safe Harbor Acts, HIPAA, and other laws, the United States is showing the European Union that their concerns are taken serious and the matter of data privacy is important in the relationship of the two powers. The United States has shown that the civil rights of the international citizens are not violated in that the country does not discriminate on allowing EU citizens travel rights to the country based on health, biometric, or other personal data. The only time the United States wants the personal information is for national security purposes and the EU data directives has exemptions for data disclosure for this narrow need. Once the two communities work towards a more unified and detailed set of rules and data protection measures that can satisfy the rules and laws of both communities then the issue of data privacy in the fight on world wide terror can be resolved. But as of now, European Union countries need not to worry about their citizens data being misused but they cannot say for certain that their citizen's data is not in the hands of the United States. Working together, each country (including the

United States) can protect its homeland while not violating the civil rights of international citizens.